Mixing Matrix Recovery of Underdetermined Source Separation Based on Sparse Representation

Abstract
This paper presents a new algorithm for recovering of the mixing matrix A of underdetermined source separation. Most of the existing algorithms for SCA assume that source signals are strictly sparse, but the condition in this paper has been relaxed, i.e., there could be at most \( m - 1 \) nonzero elements of the source signals in each time. Firstly, we can find that all \( m - 1 \) linearly independent column vectors of observed signals \( X \), which can span different hyperplanes, and then cluster the normal vectors of the hyperplanes instead of the hyperplanes themselves. Secondly, we determine the hyperplanes by maximum analysis of the number of the observed signals, which are located the same hyperplane. Finally, the mixing matrix is identified from the intersection lines of the hyperplanes. The simulation results have shown the effectiveness of the proposed algorithm.

Region Assessment of Soil Erosion Based on Naive Bayes

Abstract
Since soil erosion is a serious environmental problem, regional-scale soil erosion assessment is important. However, it is limited by the development of soil erosion mode by far. This paper presents a region-scaled soil erosion qualitative evaluation model based on naive Bayes. Firstly, the model takes the E’Dong Mountain as case study area, chooses the four factor indexes affected erosion intensity, and then calculates the naive Bayes probability of each index of soil erosion based on the observed plot sample data. Secondly, the model abstracts affected factors parameters of soil erosion by RS (Remote Sensing) and GIS (Geography Information System) in study region. Finally, the erosion intensity of region is classified into six classes in terms of the naive Bayes probability: extreme, very high, high, moderate, low, very low. Therefore, the model provides a new method for assessing the soil erosion in regional scale.

A Bayesian Network based Approach for Root-cause-analysis in Manufacturing Process

Abstract
We describe an Early Warning System (EWS) which enables the root-cause-analysis for initiating quality improvements in the manufacturing shop floor and process-engineering departments, at product OEMs as well as their tiered suppliers. The EWS combines the use of custom-designed domain ontology of manufacturing processes and failure related knowledge, innovative application of domain knowledge in the form of probability constraints and a novel two-step constrained optimization approach to causal network construction. Probabilistic reasoning is the main vehicle for inference from the causal network. This inference engine provides the capability to do a root-cause analysis in manufacturing scenarios, and is thus a powerful weapon for an automotive EWS. This technique is widely applicable and can be used in various contexts in the broader manufacturing industry as well.

Step-size Optimization EASI Algorithm for Blind Source Separation

Abstract
Aiming at the problem of blind source separation of the communication signals, we propose a step size optimization equivariant adaptive source separation via independence (SO-EASI) algorithm basing on the EASI block based algorithm. This algorithm adjusts the step-size by the steepest descent method and thereby greatly increases its convergence speed whatever value the step-size is initialized. Simulation results show that SO-EASI algorithm can effectively blindly separate the communication signals and these results also support the expected improvement in convergence speed of the approach.
Variable Step-size Online Algorithm for Blind Separation Based on the Extended Infomax

Abstract A novel variable step-size online algorithm for mixed signals with sub- and super-Gaussian source distributions based on the extended infomax is present. The extended infomax algorithm usually separates the sources by batch processing and it requires adequate samples to estimate the kurtosis of the output signals so the algorithm will be invalid when the channel matrix is changed. An improved online estimation model of the kurtosis is introduced in this paper, we interpose a detection machine-made to judge whether the channel matrix is changed or not in separation process. In order to solve the ambivalent tradeoff between convergence rate and steady-state error, a variable step-size online algorithm is proposed. The step-size updating regulation is controlled by the kurtosis variance of the signals because the kurtosis fluctuation can describe the state of separation. This online algorithm accelerated the convergence rate and reduced the steady-state error efficiently.

A Novel Learning Method for ANFIS Using EM Algorithm and Emotional Learning

Abstract It is very difficult for the adaptive neuro-fuzzy interference system (ANFIS) using conventional training methods to converge while the samples space distribution is more complex, the desired results for that couldn’t be achieved. To change the situation and improve the learning behavior of ANFIS, in this paper we propose a new self-adaptive learning algorithm for ANFIS differently from conventional training methods. The method firstly adopts the EM algorithm to learning fuzzy parameters of the ANFIS, and then applies emotion learning to learn the Takagi-Sugeno-Kang (TSK) parameters of the linear TSK functions of the ANFIS. The relevant researches indicate that the proposed learning method possesses faster training speed and better adaptability, and is more ubiquitous. In the end, a simulation example shows the availability of the proposed method.

A Novel Method for Intelligence of Sensors Modeling

Abstract For the complexity of the automation system roll on, sensors should have to be more intelligent. Recently, Neural Network is widely used to intelligentize sensors for its well performance on capturing the information of the data. But due to its intrinsic linear character, it doesn’t perform well in nonlinear data processing. In this paper, RNN with Kernel Principal Component Analysis (KPCA) and Principal Component Analysis (PCA) as the feature extraction is introduced in an comparison. And then an experimental system is set up with pressure sensor. By examining the data of the example, it is shown that the proposed methods can both achieve good performance comparing with NN method. And the KPCA method performs better than the PCA method.

An Effective Feature-Weighting Model for Question Classification

Abstract Question classification is one of the most important subtasks in Question Answering systems. Now question taxonomy is getting larger and more fine-grained for better answer generation. Many approaches to question classification have been proposed and achieve reasonable results. However, all previous approaches use certain learning algorithm to learn a classifier from binary feature vectors, extracted from small size of labeled examples. In this paper we propose a feature-weighting model which assigns different weights to features instead of simple binary values. The main characteristic of this model is assigning more reasonable weight to features: these weights can be used to differentiate features each other according to their contribution to question classification. Furthermore, features are weighted depending on not only small labeled question collection but also large unlabeled question collection. Experimental results show
that with this new feature-weighting model the SVM-based classifier outperforms the one without it to some extent.

**Active P2P Traffic Identification Technique**

**Abstract**

Accurate traffic classification for different P2P applications is fundamental to numerous network activities, from security monitoring, capacity planning and provisioning to service differentiation. However, current P2P applications use dynamic port numbers, HTTP masquerading and inaccessible payload to prevent being identified. The paper proposed an accurate P2P identification system using Decision Tree algorithms (J48 and REPTree) on the basis of effective feature selection. The experimental results show that our scheme is of better accuracy, less computational complexity and it is robust enough to deal with unknown P2P traffic. With the merits, the scheme can suit the real-time active detection environment, such as monitoring network attacks camouflaged with P2P traffic and service differentiation.

**Study on PIGA Test Method on Centrifuge**

**Abstract**

The experiment design of PIGA test on centrifuge has been studied. Based on the identification method for high-order coefficients of PIGA (pendulous integrating gyro accelerometer) on precision centrifuge with counter-rotating platform, which can isolate the rotary movement caused by centrifuge arm so as to improve the environment of PIGA test on centrifuge, the method of the D-optimal designs is used in the data processing for separating the error model coefficients to optimize the test plans. The relation between the different values of the factors taken in the testing procedures and the estimated accuracy is discussed according to the D-criterion by way of simulation analysis. The results of the simulation analysis show that by optimizing the values of the factors in a test plan, the calibrating accuracy can be greatly improved.

**Parameters Selection for SVR based on the SCEM-UA Algorithm and Its Application on Monthly Runoff Prediction**

**Abstract**

Support Vector Machines (SVMs) have become one of the most popular methods in Machine Learning during the last few years, but its performance mainly depends on the selection of optimal parameters which is very complex. In this study, the SCEM-UA algorithm developed by Vrugt is employed for parameters selection of Support Vector Regression (SVR). The SCEM-UA algorithm, which operates by merging the strengths of the Metropolis algorithm, controlled random search, competitive evolution, and complex shuffling, can avoid the tendency of falling into local minima. The proposed method was tested on a complicated nonlinearly runoff forecasting. The results illustrated that SCEM-UA algorithm can successfully identify the optimal parameters of SVR than grid search method, and can achieve an accurate prediction. Keywords: Support Vector Machines; Optimization; SCEM-UA; Time series; Forecasting

**Estimate and Track the PN Sequence of Weak DS-SS Signals**

**Abstract**

This paper proposes a modified Sanger’s generalized Hebbian neural network method to estimate and track the pseudo noise sequence of weak direct sequence spread spectrum signals. The proposed method is based on eigen-analysis of received signals. The received signal is firstly sampled and divided into non-overlapping signal vectors according to a temporal window, which duration is a periods of PN sequence. Then an autocorrelation matrix is computed and accumulated by these signal vectors one by one.
The pseudo noise sequence can be estimated and tracked by the principal eigenvector of the matrix in the end. Because the eigen-analysis method becomes inefficiency when the estimated pseudo noise sequence becomes longer or the estimated pseudo noise sequence becomes time varying, we use a modified Sanger’s generalized Hebbian neural network to realize the pseudo noise sequence estimation and tracking from weak input signals adaptively and effectively.

A Smoothing Support Vector Machine Based on Quarter Penalty Function
Abstract
It is very important to find out a smoothing support vector machine. This paper studies a smoothing support vector machine (SVM) by using quarter penalty function. We introduce the optimization problem of SVM with an unconstrained and nonsmooth optimization problem via quarter penalty function. Then, we define a one-order differentiable function to approximately smooth the penalty function, and get an unconstrained and smooth optimization problem. By error analysis, we may obtain approximate solution of SVM by solving its approximately smooth penalty optimization problem without constraints. The numerical experiment shows that our smoothing SVM is efficient.

Fast Forecasting with Simplified Kernel Regression Machines
Abstract
Kernel machines, including support vector machines, regularized networks and Gaussian process etc, have been widely used in forecasting. However, standard algorithms are often time consuming. To this end, we propose a new method for imposing the sparsity of kernel regression machines. Different to previous methods, it incrementally finds a set of basis functions that minimizes the primal cost functions directly. The main advantage of our method lies in its ability to form very good approximations for kernel regression machines with a clear control on the computation complexity as well as the training time. Experiments on two real time series and benchmark Sunspot assess the feasibility of our method.

An Accelerated SMO-type Online Learning Algorithm
Abstract
In order to accelerate the learning speed for online learning algorithm, a fast support vector machine online learning algorithm is presented in this paper. In the proposed algorithm, the learning condition is relaxed and a novel learning strategy is presented while Sequential Minimal Optimization (SMO) training method which has been improved by Keerthi, is embedded. In order to verify the performance of the proposed algorithm, it has been applied to seven UCI datasets and a benchmark problem. Experimental results show that the novel algorithm is very faster than Online Support Vector Classifier (OSVC), SimpleSVM algorithms without losing generalized performance. Keywords: Support Vector Machine, Sequential Minimal Optimization, Online Learning

An Improved MRF based Unsupervised Change Detection Method
Abstract
Traditional unsupervised change detection algorithms based on simple MRF model assume that subimages applied to extracting features are homogeneous, but that is not always true and causes low accuracy. Based on the fields correlation Markov random field (CMRF) model, an adaptive algorithm is proposed in this paper. The labeling is obtained through solving a MAP (Maximum a posterior) problem by ICM (Iteration Condition Model). Features of each pixel are exacted by using only the pixels currently labeled as the same pattern. With the adapted features, the new labeling is obtained. The satisfied experimental confirm the effectiveness of proposed techniques. Although the proposed method has been presented in the specific context of the analysis of multitemporal remote-sensing images, it could be used in any change detection application requiring the technique based on the difference image.
Intrinsic Dimensionality Estimation with Neighborhood Convex Hull

Abstract
In this paper, a new method to estimate the intrinsic dimensionality of high dimensional dataset is proposed. Based on neighborhood graph, our method calculates the non-negative weight coefficients from its neighbors for each data point and the numbers of those dominant positive weights in reconstructing coefficients are regarded as a faithful guide to the intrinsic dimensionality of dataset. The proposed method requires no parametric assumption on data distribution and is easy to implement in the general framework of manifold learning. Experimental results on several synthesized datasets and real datasets have shown the facility of our method.

A Novel Evolutionary Algorithm for Function Optimization Using MEC

Abstract
This paper proposes a novel evolutionary algorithm that integrates Mind Evolutionary Computation (MEC) and non-uniform mutation. The algorithm greatly extends MEC to explore the tradeoff between exploration and exploitation for optimizing multimodal functions. Similartaxis mechanism drives the proposed algorithm to locate multiple local optima, while non-uniform method locates the global area cooperatively. Moreover, the 1/5 rule is adopted to guide the search direction based on information obtained from feedback. The proposed algorithm is experimentally testified with a test suits containing six complex multimodal function optimization problems. All experiments demonstrate that the proposed algorithm is competitive with other evolutionary algorithms published to date in both convergence velocity and solution quality.

A New Tree Encoding for the Degree-Constrained Spanning Tree Problem

Abstract
The degree-constrained minimum spanning tree (dc-MST) problem is of high practical importance. Up to now there are few effective algorithms to solve this problem because of its NP-hard complexity. More recently, a genetic algorithm (GA) approach for this problem was tried by using Pr"ufer number to encode a spanning tree. The Pr"ufer number is a skillful encoding for tree but not efficient enough to deal with the dc-MST problem. In this paper, a new tree encoding is developed directly based on the degree constraint on each vertex and the connectivity among vertices. We denote it as degree-based permutation encoding and apply it to the dc-MST problem by using the GA approach. Compared with the numerical results and CPU runtimes between two encodings, the new degree-based permutation is effective to deal with the dc-MST problem and even more efficient than the Pr"ufer number to evolve to the optimal or near-optimal solutions.

A novel hybrid real-valued genetic algorithm for optimization problems
Abstract
Since genetic algorithm lacks hill-climbing capacity, it easily falls in a trap and finds a local minimum not the true solution. In this paper, a novel hybrid real-valued genetic algorithm (NHRVGA) combined with harmony search that merits of genetic algorithm and harmony search (HS) is proposed. It provides a new architecture of hybrid algorithms, which organically merges the harmony search (HS) method into real-valued genetic algorithm (RVGA). During the course of evolvement, harmony search is used to improve the search performance and this makes NHRVGA algorithm have more powerful exploitation capabilities. Simulation and comparisons based on several well-studied benchmarks demonstrate the effectiveness, efficiency and robustness of the proposed NHRVGA.

Global Optimization Method Based on the Statistical Genetic Algorithm for Solving Nonlinear Bilevel Programming Problems

Abstract
This paper presents a global optimization method based on the statistical genetic algorithm for solving nonlinear bilevel programming problems. The bilevel programming problem is firstly transformed into a single level problem by applying Karush-Kuhn-Tucker conditions, and then an efficient method based on the statistical genetic algorithm has been proposed for solving the single level problem with the complementarity constraints. By certain handling technology, the simplified problem without the complementarity constraints can be gotten. If it is solvable then its optimal solution is a feasible solution of the original bilevel programming problem. At last, a global optimal solution of the original problem can be found among its feasible solutions. Numerical experiments on some benchmark problems show that the new algorithm can find global optimal solutions of the bilevel programming problems in a small number of fitness evaluations.

Prediction of MHC Class II Binding Peptides Using a Multi-Objective Evolutionary Algorithm

Abstract
The identification of T-cell epitopes is important for vaccine development. An epitope is a peptide segment that can bind to both a T-cell receptor and a major histocompatibility complex (MHC) molecule. The prediction of MHC binding peptides is a crucial part of the epitopes identification. This paper presents a novel Multi-Objective Evolutionary Algorithm (MOEA) to predict MHC class II binding peptides. The optimal search strategy of MOEA is used to find a position specific scoring matrix which can present MHC class II binding peptides quantitative motif. The performance of the new algorithm has been evaluated with benchmark datasets.

A New Evolutionary Algorithm for Constrained Optimization Problems

An improved genetic algorithm for optimal operation of cascaded reservoirs

Abstract
Based on the characteristics of optimal operation of cascaded hydropower stations, a mathematic model about the multistage optimization is established. In order to improve the capability of the traditional algorithm in optimal operation of cascaded reservoirs, Niche Genetic Algorithm (NGA) is suggested. This method could avoid the situation of GA convergence at a much earlier stage. The validity of improvement algorithm is testified by the solution of three classic functions. Finally it is successfully applied to the
cascaded hydropower stations of the Qing River. The results show that NGA has not only better optimization capability, but also better accuracy. It is a superior non-linear optimal method which could locally search the global solution with greater probability.

A Decision-tree-based Multi-objective Estimation of Distribution Algorithm

Abstract
A new decision-tree-based multi-objective estimation of distribution algorithm (DT-MEDA) for optimization problems with continuous variables is developed. Decision-tree-based probabilistic models are used to encode conditional dependencies among variables in DT-MEDA. By building and sampling the probabilistic models, the algorithm reproduces the genetic information of the next generation. Incorporating this reproduction mechanism together with the ranking method and the truncated selection, DT-MEDA can approximate the Pareto front. Polynomial mutation operator is used to enhance exploration and maintain diversities in the populations. Furthermore, DT-MEDA adopts a procedure to eliminate a solution with smallest crowding distance at a time in the truncated selection, so that it can obtain a well spread solution set. The performance of the proposed algorithm is evaluated on four biobjective test problems and metrics from literature. Simulation results show that the proposed approach is competitive with NSGA-II and DT-MEDA is a general and effective method for multi-objective optimization.

Performance Scalability of a Cooperative Coevolution Multiobjective Evolutionary Algorithm

Abstract
Recently, numerous Multiobjective Evolutionary Algorithms (MOEAs) have been presented to solve real life problems. However, a number of issues still remain with regards to MOEAs such as convergence to the true Pareto front as well as scalability to many objective problems rather than just bi-objective problems. The performance of these algorithms may be augmented by incorporating the coevolutionary concept. Hence, in this paper, a new algorithm for multiobjective optimization called SPEA2-CC is illustrated. SPEA2-CC combines an MOEA, Strength Pareto Evolutionary Algorithm 2 (SPEA2) with Cooperative Coevolution (CC). Scalability tests have been conducted to evaluate and compare the SPEA2-CC against the original SPEA2 for seven DTLZ test problems with a set of objectives (3 to 5 objectives). The results show clearly that the performance scalability of SPEA2-CC was significantly better compared to the original SPEA2 as the number of objectives becomes higher.

Comparison between Particle Swarm Optimization, Differential Evolution and Multi-parents Crossover

Abstract
Particle swarm optimization (PSO), differential evolution (DE) and multi-parents crossover (MPC) are the evolutionary computation paradigms, all of which have shown superior performance on complex non-linear function optimization problems. This paper detects the underlying relationship between them and then qualitatively proves that these heuristic approaches from different theoretical principles are consistent in form. Comparison experiments involving eight test functions well studied in the evolutionary optimization literature are used to highlight some performance differences between the techniques. The results from our study show that DE generally outperforms the other algorithms.
PSO Algorithm based Online Self-Tuning of PID Controller

Abstract
Proportional-Integral-Derivative (PID) controller is still widely used in control engineering, and tuning of PID is a crucial operation. We utilize particle swarm optimization algorithm to design an online self-tuning framework of PID controller. Our system is simulated in Matlab based on particle swarm optimization algorithm. Experiment focus on several problems application concerned. Our conclusions include that different fitness function can lead to different time response, and application system should initialize range of each particle as small as possible. Moreover, the conclusions also include that we should choose a modest generations for the online system with linearly inertia weight consume less times evolutionary generation, not a larger one. These conclusions can contribute mostly to application system concerning about calculation cost.

Keywords: PSO, PID controller, Matlab

A Self-adaptive Particle Swarm Optimization Algorithm with Individual Coefficients Adjustment

Abstract
This paper introduces a novel self-adaptive strategy of inertia weight and social acceleration coefficient adjustment in particle swarm optimization (PSOSAIC). In PSO-SAIC, each particle has its individual inertia weight and social acceleration coefficient, which will be adjusted dynamically and self-adaptively by the result of the passed evolutions, so the PSO-SAIC can retain the diversity of particles. The result of the compare to the time-varying inertia weight particle swarm optimization and the time-varying acceleration coefficient particle swarm optimization with 3 classical benchmark functions shows that the PSO-SAIC provides outstanding global and local convergence performances in optimization high dimensional objects.

A GA Based Combinatorial Auction Algorithm for Multi-robot Cooperative Hunting

Abstract
In order to improve the hunting efficiency of multirobot cooperative hunting in complicated environment: multi-target and dynamic continues surrounding, a combinatorial auction model based on genetic algorithm (GACA) was presented in this paper. The model adopted genetic algorithm to solve the winner determination problem in combinatorial auction. We also compared the combinatorial auction model based task allocation method with the traditional single item auction model in solving dynamic and complex task allocation problem in multi-robot cooperation. The simulation experiments were conducted in a selfdeveloped visible multi-robot simulation platform, OpenSim, and the results showed the whole process of hunting was very smooth, and the cost time cost by our algorithm was much shorter than the compared method.

An Adaptive Parameter Control Strategy for Ant Colony Optimization

Abstract: Ant Colony Optimization (ACO) has been proved to be one of the best performing algorithms for NP-hard combinational optimization problems like TSP. Many researchers have been attracted in research for ACO but fewer tuning methodologies have been done on its parameters which influence the algorithm directly. The setting of ACO’s parameters is studied in this paper. The Artificial Fish Swarm Algorithm (AFSA) is introduced to solve the parameter tuning problem, and an adaptive parameter setting strategy is proposed. It’s proved to be effective by the experiment based on TSPLIB test.

Keywords: Artificial Fish Swarm Algorithm, Ant Colony Optimization, parameters, TSP
A Multi-Focus Image Fusion Algorithm with DT-CWT

Abstract
A multi-focus image fusion algorithm with Dual-Tree Complex Wavelet Transform (DT-CWT) is proposed in the paper. There are some disadvantages in Discrete Wavelet Transform (DWT), such as shift variance and lack of directional selectivity. Therefore, to have better representation of the images, they are processed with DT-CWT. The low frequency coefficients and high frequency coefficients are fused separately with different methods because of their different characteristics. To the low frequency coefficients, neighborhood gradient maximum selectivity (NGMS) scheme is used, the ones having maximal neighborhood gradient are selected. To the high frequency coefficients, the absolute value maximum selectivity (AVMS) is used, the ones having maximal absolute values are selected. Experiment results show that the algorithm proposed in this paper not only solves the problems such as low contrast and blocking effects caused by fusion algorithms in space domain, but also avoids the artifacts and ringing artifacts exhibited by conventional wavelet based fusion algorithms.

Keywords: DT-CWT, image fusion, multi-focus, NGMS, AVMS

A Fuzzy Fusion in Multitarget Tracking With Multisensor

Abstract
In the system of the multi-sensors multitargets tracking, the data received from sensor measurements may be imprecise, incomplete and ambiguous because of the noise, which may cause the incorrect correlation. Here, according to the position error, velocity error and acceleration error between true value and estimation of the moving targets, a fuzzy track to track fusion algorithm for the multi-sensor multi-target tracking was proposed based on the fuzzy inference. The algorithm were tested by the real data from the different sonar sensor measurements. The results show that the approaches are good and valid, and well for the distributed multi-sensor multi-target tracking. The accuracy of tracking in clutter is high.

An Algorithm for Extracting Referential Integrity Relations using Similarity during RDB-to-XML Translation

Abstract
XML is rapidly becoming technologies for information exchange and representation. It causes many research issues such as semantic modeling methods, conversion for interoperability with other models, and so on. Especially, the most important issue in practical area is how to achieve the interoperability between XML model and relational database model. Until now, many methods have been proposed to achieve it. However, several problems still remain. Most of all, existing methods do not consider implicit referential integrity relations, so it causes loss of information. This paper proposes an algorithm for extracting referential integrity relations during RDB to XML translation. The key point of our method is how to find implicit referential integrity relations among columns which have different names to represent the same semantic. To resolve it, we define an enhanced extraction algorithm which based on a widely used ontology, WordNet. The proposed algorithm can reduce an extraction time among comparison columns in RDB tables and prevent loss of information.

Research on Algorithm of Web Classification Based on EP and FFSS

Abstract
In this paper, we present a new algorithm of web classification by combining extended pages (EP) and fair featuresubset selection (FFSS). As the importance of hyperlink, we extend web pages by anchor text. In extended pages, the proportion of the useful feature increases, so we can improve the solution of the web
classification. In view of using the structure of the web, we get extended pages by appending the sentence or the paragraph including anchor text to the original pages. Fair feature-subset selection not only gives fair treatment to each category but also has ability to identify useful features, including both positive and negative features, so it can address the issue of high dimensionality of vector space. Experiments show that the new algorithm enhances the precision and recall of the traditional method.

Discovery of Direct and Indirect Association Patterns in Large Transaction Databases

Abstract
Association rules mining is one of the important tasks in data mining research. While most of the existing discovery algorithms are dedicated to efficiently mining of frequent patterns, it has been noted recently that some of the infrequent patterns can provide useful insight view into the data. As a result, indirect association rules have been put forward, the traditional association rules are called direct association patterns. All the existing algorithms for mining indirect association rules need get all frequent itemsets using Apriori or other algorithms for mining association rules, then generate indirect association candidates using frequent itemsets. Instead of this method, we put forward an approach to discover both direct and indirect association patterns. Key words: Direct Association Pattern, Indirect Association Pattern, Data Mining

Associative Classification Using SVM-based Discretization

Abstract
Associative classification has been recently proposed which combines association rule mining and classification, and many studies have shown that associative classifiers have high prediction accuracies. In order to apply an association rule mining to classification problem, data transformation into the form of transaction data should be preceded before applying association rule mining. In this paper, we propose a discretization method based on Support vector machines, which is very effective for association classification. The proposed method finds optimal class boundaries by using SVM, and discretization utilizing distances to the boundaries is performed. Experimental results demonstrate that performing SVM-based discretization for continuous attributes makes associative classification more effective in that it reduces the number of association rules mined and also improves the prediction accuracies at the same time.

An Efficient Graph-based Multi-relational Data Mining Algorithm

Abstract
Multi-relational data mining can be categorized into graph-based and logic-based approaches. In this paper, we propose some optimizations for mining graph databases with Subdue, which is one of the earliest and most effective graph-based relational learning algorithms. The optimizations improve the subgraph isomorphism computation and reduce the numbers of subgraph isomorphism testing, which are the major source of complexity in Subdue. Experimental results indicate that the improved algorithm is much more efficient than the original one.

Analysis on Time-lagged Gene Clusters in Time Series Gene Expression Data

Abstract
There are a number of previous approaches for identifying time-lagged gene co-regulations. Popularly used cross-correlation method and edge detection method don't consider the direction of regulation of gene
pairs. And event method is proposed to deal with some of the above-mentioned limitations however its scoring system to identify promising time-lagged gene pairs is still questionable. This paper further analyses the time-lagged gene clusters mining process and some probably existing deduced direction of co-regulation’s contradictory phenomenon in these clusters/biclusters. Besides, the time-lagged value is proposed as a possible prevention mechanism.

A Novel Local Features-based Approach for Clustering Microarray Data

Abstract

DNA Microarray technology makes it possible to monitor simultaneously the dynamic expression levels of tens of thousands of genes during some important biological processes. A first step to comprehend and interpret the resulting mass of data is via clustering techniques. However, most existing methods are based on clustering genes by comparing their expression levels on all experiment conditions although genes in a functional cluster more often than not correlate only under a subset of conditions. Besides, most clustering algorithms depend on some critical user parameters in determining the number of resulting clusters. Unfortunately, correct parameter values are rarely known in real datasets. In this paper, we propose a novel clustering algorithm that (1) goes beyond global approaches to discovery gene clusters based on local features, and (2) automatically determines the number of resulting clusters. Furthermore, we introduce the norm-based method to improve it, as is proved reasonable. Extensive experiments are conducted on both synthetic and real data sets. Experiments prove that our method is efficiency and efficient.

Improved Variable Precision Rough Set Model and Its Application to Distance Learning

Abstract

Improved Variable Precision Rough Set (VPRS) is proposed to extract the significant decision rules from a Student Information Table (SIT) in the distance learning environment. Moreover, two approaches are proposed. The first approach, VPRS based on Bayesian Confirmation Measures (BCM) is presented in order to handle totally ambiguous and enhance the precision of Rough set, and to deal with multi decision classes. The second approach, the VPRS parameters are refined, especially with multi decision classes. These concepts have been demonstrated by an example. The simulated result gives good accuracy and precise information with few computational steps.

A New Attribute Reduction Algorithm in Continuous Information Systems

Abstract

This paper puts forward a new method of discretizing continuous attributes. Compared with the traditional approach, the method, proposed in this paper, can make the number of the obtained classes be more moderate, as well as the lost information be fewer. And then a simple attribute reduction algorithm is developed in continuous information systems. Finally, a real example is used to illustrate its feasibility and effectiveness, respectively.

Realization of a New Association Rule Mining Algorithm

Abstract

Based on fully analyzing the PF_growth, an association rule mining algorithm, this paper presents a new association rule mining algorithm called MFP. The MFP algorithm can convert a transaction database into an MFP_tree through scanning the database only once, and then do the mining of the tree. Because the MFP algorithm scans a transaction database one time less than the FP_growth algorithm, the MFP...
A Study on the Method of Attribute Reduction Based on Rough Set under Fuzzy Equivalent Relation

Abstract
In this paper, first we proposed a method of attribute reduction based on rough set under fuzzy equivalent relation. We computed the similarity of cases with the fuzzy equivalent relation, reduced the attributes by the same fuzzy equivalent partitions based on rough set, and then gave a method of computing the weights of the attributes. Comparing with the traditional method of attribute reduction based on rough set, more information of the primary data is held, and more accuracy of the attribute reduction is enhanced by our method.

Mining Maximally Common Substructures from XML Trees with Lists-Based Pattern-Growth Method

Abstract
With the continuous growth in XML data sources over the Internet, the discovery of useful information from a collection of XML documents is currently one of the main research areas occupying the data mining community. The mostly used approach to this task is to extract frequently occurred subtrees in XML trees. But, because the number of frequent subtrees grows exponentially with the size of trees, a more practical and scalable alternative is required, which is the discovery of maximal frequent subtrees. In this paper, we present the first algorithm that directly discovers maximal frequent subtrees from a concise data structure, without any candidate subtree generation.

The Algorithm of Objective Association Rules Mining Based on Binary

Abstract
This paper proposes an algorithm of objective association rules used in data mining, which is suitable for mining some potential rules related to the given object from large data warehouse. The basic principle of algorithm is that the association rules were formed according to this special information, which is mined with binary logic “and” operation from many attribute-values of database, where data have been expressed by binary. The theory of algorithm is quite simple. It is feasible and efficient to execute the algorithm. It is a practical significance to apply to the algorithm in some applicable domains to search special objective association rules.

Fuzzy Factor in Switching Regression Models

Abstract
Switching regression models is a kind of special mixture regression models, and the clustering method of it can be classified as hard partitioning and fuzzy partitioning. The former is simple in coding and fast in execution, but its partitioning is too pure since it overlooks the fuzziness; whereas the latter, taking the fuzziness into account, is more reasonable for partitioning, but the algorithm complexity and cost will increase. Based on the research of hard partitioning and fuzzy partitioning, the idea of fuzzy factor is proposed. By adjusting fuzzy factor, hard partitioning and fuzzy partitioning are unified, and the clustering analysis of switching regression models becomes more flexible. It is demonstrated by simulation experiment that it is feasible to find the optimal combination of speed and fuzziness according to the practical application.

Personalized Web Search Using User Profile

Abstract
Current Web search engines are built to serve all users, regardless of special needs of any individual user. So personalization of Web search is to carry out retrieval for each user incorporating his/her interests. A novel query expansion algorithm is proposed in this paper. It is based on a model of personalized web search system, which can learn a user’s preference implicitly and then generate the user profile automatically. When the user inputs query keywords, more personalized expansion words are generated by the proposed algorithm, and then these words together with the query keywords are submitted to a popular search engine such as Baidu or Google. These expansion words can help search engines retrieval information for a user according to his/her implicit search intentions, and return different search results to different users who input the same keywords.

Mining Temporal Web Interesting Patterns

Abstract

Previous work on mining web associations focus primarily on finding frequent access patterns in the data. However, they ignore an important relationship that web frequent access patterns have the dynamic characteristic of time varying. It is also important that in database, some items which are infrequent in whole dataset but those depend on the present of a mediator itemset may be frequent in a particular time period, which induce some interesting patterns may not be discover. In this study, our focus is to apply a new mining technique called indirect association onto temporal web data and propose the TIFP-mine algorithm based on a new model WM-graph, which are both capable of extracting all temporal indirect frequent patterns and its temporal extended patterns. Experimental results confirm that TIFP-mine algorithm is efficient and effective. Our analysis shows very promising results, especially in terms of identifying Web users with distinct interests.
Trusted Computing Enabled Access Control for Virtual Organizations

Jing Zhan Wuhan University School of Computer Science Wuhan, 430079, China Huanguo Zhang Wuhan University State Key Lab of Software Engineering Wuhan, 430072, China

Abstract

Grid computing is becoming the prominent paradigm for resource exchange and collaboration, which are supported by dynamic, multi-institutional virtual organizations (VOs) overcoming limitations of time or space. As the de-facto standard for Grid security, Grid Security Infrastructure provides no effective mechanism to protect both resource providers and users from access of malicious entities. The Trusted Computing (TC) technology adopted by the Trusted Computing Group (TCG) defines that an entity can be trusted as long as it always behaves in the expected manner. Specifically, the TC uses a hardware module called Trusted Platform Module (TPM) to ensure the tamper-proof attestative behavior by integrity measurement, logging and report. In this paper, we propose and design a TC enabled system based on Linux and TPM hardware to enforce access control policy for the VO.

A Protecting protocol of Mobile Agent Integrity

Huanmei Guan1,2,3, Huanguo Zhang2,3, Ping Chen1, and Yajie Zhou1
1. Computer Center, Wuhan University, Wuhan 430072 China
hmguan-wh@163.com
2. Computer School, Wuhan University, Wuhan 430072 China
liss@whu.edu.cn
3 The State Key Laboraty of Software Engineering, Wuhan University, Wuhan 430072 China

Abstract

The integrity of mobile agent means that its state and partial results can not be modified by a malicious host or such modifications could be found. The paper proposes an integrity protocol. It provides strong identity authentication and strong integrity protection. It can detect most attacks.

The semantic model based on BSCM for the information security

Liu zhong
The Center of technology of modern education, Guiling University of Technology, Guilin, Guangxi, P.R.China: 541004
Abstract
Semanteme identifying is very difficult problem in the information security. But if the semantic models have been set up for the mechanism of the information security, that’s the easy way to identify the semanteme. A few semantic models have been set up based on the BSCM. These models should be defined the basic semanteme unit and be defined the models of the semantic relativity. The content of information could be judged by these models. The most basic semantic unit should be defined as BSCM. Basing on the BSCM, the model of the relativity of semanteme for the relativity of semanteme has been set up.

A Proactive Defense Scheme Based on the Cooperation of Intrusion Deception and Traceback
Junfeng Tian, Ning Li, Zhiqiang Wang1
1Institute of Computer Network Technology, Hebei University, Baoding 071002, China
2The Administrative Center for China’s Agenda 21, Beijing 100038, China
E-mail: donnyli@163.com

Abstract
This paper presents a proactive defense scheme based on the cooperation of Intrusion Deception and Traceback. A new model of PDDT (Proactive Defense Model based on Intrusion Deception and Traceback) is established to protect the network resources. We propose an improved approach APPM based on the PPM (Probabilistic Packet Marking) in the traceback module of PDDT. This approach enhances the efficiency in real-time capability and flexibility which are deficient in the PPM. The simulation result indicates the performance and efficiency of this scheme.

A New Information Measurement Scheme Based on TPM for Trusted Network Access
Lu Chen School of Computer, State Key Lab of Software Engineering, Wuhan University, Wuhan, Chinaieuc1@163.com
Huanguo Zhang School of Computer, State Key Lab of Software Engineering, Wuhan University, Wuhan, China liss@whu.edu.cn
Liqiang Zhang School of Computer, State Key Lab of Software Engineering, Wuhan University, Wuhan, China whujking@126.com
Liang Cai Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou, China ieucl@sohu.com

Abstract
The information measurement of the NAR (network access requester) is the key element for trusted network access. The only issues TNC (trusted network connection) proposed the conception of integrity measurement and pointed out that only if the measurements passed can the NAS (network access server) let the endpoint enter. But no concrete techniques are expatiated in TNC, and the related
specification IMM (integrity measurement model) is too complex to implement. Virtually, the measurement cannot be localized to the integrity. In this paper, a new information measurement architecture is proposed, in which not only the integrity information of the platform, but also the identity of user and platform, and the information of system availability are considered. The related techniques (information collection and verification etc.) are illustrated, and the trust chain transfer is analyzed at the end.

Keywords: trusted platform model (TPM), trusted network access, trusted information measurement, trust chain transfer

An Improved Trust Negotiation Protocol with Hidden Credentials
Guoming Cai, Yadi Wang, Zhiqiang Zhu, Kaiyong Xu
Zhengzhou Information Science and Technology Institute
Zhengzhou, Henan 450004, China
E-mail: cgmcai817@sohu.com

Abstract
Hidden credentials are widely used for strangers in open environments to establish mutual trust without actually disclosing credentials and policies. With these schemes, sensitive resource and policies are protected against being leaked to unqualified recipients. However, an adversary is able to tamper negotiation messages or flood error messages to the recipient. Because the traditional protocol with hidden credentials omits integrity and authentication protection, the recipient still tries each of his credentials to decrypt the message. These will add the recipient’s computational overhead and result in potential threats to the protocol. In this paper, we develop an improved trust negotiation protocol to prevent such attack. Compared with previously proposed trust negotiation protocol, our protocol uses cryptographic authentication mechanisms which can help the recipient to detect any modification and identify hostile sender. We also discuss the security and performance of the improved protocol.

An Improvement on Precision in DDoS Source-end Detection with Multi-stream Combined HMM
Jian Kang, Qiang Li, Yuan Zhang, Zhuo Li
Department of Computer Science & Technology
Jilin University, Changchun, China
kj885788@gmail.com

Abstract
DDoS (Distributed Denial-of-Service) attacks detection system deployed in source-end network is superior in perceiving and throttling attacks before data flows enter Internet, comparing with that in victim network. However, the current existed works in source-end network are so fragile, lead to a high false-positive rate and false-negative rate. This paper proposes a novel approach using Multi-stream combined Hidden Markov Model (MC-HMM) on source-end DdoS detection for integrating multi-features simultaneously.
The multi-features include the S-D-P three-tuple, TCP header Flags, and IP header ID field. Through experiments, we compared our original approach based on multiple detection features with other algorithms (such as CUSUM and HMM). The results present that our approach effectively reduces false-positive rate and false-negative rate, and improves the precision of detection.

A High-efficiency Intrusion Prediction Technology Based on Markov Chain
Cao Lai-Cheng
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China, caolch@lut.cn

Abstract
Intrusion detection is only able to detect intrusions after the attacks occurred. In this paper, an intrusion prediction technology based on Markov chain is pointed out, a dynamic load-balancing algorithm is adopted in its predicting model, which can avoid packet loss and false negatives in high-performance network with handling heavy traffic loads in real-time. Experiments show that this technology have good performance on real-time prediction, false alarm rate is lower than 0.6% and false negative rate is tend to 1%, so this prediction technology can contain or stop the attack in real time, it can also enhance the efficiency of finding intrusion.

Ad hoc Networks Security Mechanism based on CPK
Lei Feng-Yu College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan, China 430074 superbluecrystal@163.com
Cui Guo-Hua College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan, China 430074 ever_cs@163.com
Liao Xiao-Ding Institute of Communication Engineering, PLA. University of Science and Technology, Nanjing, China 210007 goldenyears86@163.com

Abstract
The existing security schemes are not applicable to ad hoc networks perfectly because ad hoc networks have some inherent security vulnerabilities and stringent resource constraints. This paper suggests using CPK as the security mechanisms of ad hoc networks with the purpose of high-level security as well as excellent performance. This paper investigates several security schemes, and evaluates the scalability, the availability and the robustness of the schemes by extensive simulations. The simulation results show the advantages of CPK contrasting with PKI, peer-to-peer authentication scheme, and the localized scheme.

Group oriented Secure Routing Protocol of Mobile Agents
Weidong Qiu, Haibin Guan, Xinghao Jiang, Zheng Huang
School of Information Security Engineering
Shanghai Jiaotong University
800 Dongchuan Road, Minhang
Shanghai 200240, P.R.China
qiuwd, hbguan, Xinghaojiang, Huang-zheng@sjtu.edu.cn

Abstract
Security is an important issue for the widespread deployment of applications based on software agent technology. Group signature is integrated into secure routing protocol for mobile agents in this paper. The hosts visited by mobile agent are in different groups. The structure of group oriented routing protocol is more clear and nature. Besides, by building trust policies, the risk and loss of DoS attack will be minimized. Furthermore, if DoS attack happens unfortunately, the protocol can identify the malicious host launching the DoS attack. According to the behavior of hosts in past, we can either define an appropriate order in which selected hosts should be visited, or decide which hosts we do not want to contact again.

Improvement of Temporal-replication Mechanism in Mobile Agent System
Fault-tolerant Model
Wang-Xiao Yun
Hang Zhou DianZi University
Institute of Management School, Hang Zhou, Zhejiang, P.R.China, 310018
wangxy_zj@126.com
Ye-Jian Nan, Huang-Guo Jin, Yu-Mei He
Hang Zhou DianZi University Institute of Management School, Hang Zhou, Zhejiang, P.R.China, 310018 yejiannan@126.com

Abstract
Fault-tolerant is one of the most important content of mobile-agent system. After studying the existing mobile-agent system fault-tolerant mechanisms both in domestic and overseas, this paper is concerned with Temporal-replication methodology. On the basis of witness agent approach, which was proposed by Michael R.Lyu etc, in this paper a progressed mechanism was introduced. There are two aspects of improvement, the one is to keep address and timestamp of the nodes that agent has traveled; the other is to employ the agent creation node as a fixed backup. This approach can handle server failures, place failures, and failures in message passing. It is capable of detecting and recovering most failure scenarios in mobile agent systems. We describe the design of our fault-tolerant approach to mobile agent systems, and conduct reliability evaluation for our approach by using simulation tools of C-Sim and Matlab. The evaluation results show our approach is a promising

Anonymous Agent with Anonymous Itinerary
Fatemeh Raji
Department of Computer Engineering University of Isfahan, Iran
raji@eng.ui.ac.ir
Behrouz Tork Ladani Department of Computer Engineering, University of Isfahan, Iran ladani@eng.ui.ac.ir
Mehdi Brenjkoub Department of Computer Engineering, Isfahan University of Technology, Iran
Abstract
The mobile agent is desired to be able to roam autonomously and anonymously from one agent platform to another one. To achieve this aim, a novel secure protocol is proposed to provide anonymity of the agent owner as well as the agent itinerary. In the presented method, a set of trusted auxiliary hosts named as Mixers are employed to insert a transient fictitious owner in each step of the agent itinerary. The ability of the proposed protocol is analyzed and its resistance against traffic analysis attacks is illustrated.

Characteristic Analysis of Virus Spreading in Ad hoc Networks
Peng Li, Zeming Wang, Xuezhi Tan
Communication Research Center, Harbin Institute of Technology
P.O.Box 3043, HIT Science Park, YiKuang Street No.2, Harbin, 150080
hitlip@gmail.com, wangzeming@gmail.com, tanxuezhi@public.hr.hl.cn

Abstract
The security of Ad hoc networks has received more and more attention recently with the widely use of Ad hoc in many areas. Virus spreading over the network can cause significant damage and the loss of network security. On the other hand, the anti-virus process also plays an important part affecting the virus spreading.
Considering the characteristic of dynamic topology of Ad hoc networks, the virus spreading is different from wired networks. In this paper we present four virus spreading models and analyze the effect of node mobility, multi-hop and anti-virus function on virus spreading. The simulation result indicates that multihop and mobility can accelerate virus spreading. However, increasing transmission range will reduce the effect of mobility and enhance the effect of multihop. The anti-virus function can decelerate the virus spreading and reduce the infection rate. With the increase of transmission range, the anti-virus function can keep the infection rate at a lower degree which will prevent the virus from spreading.

Secure Vault: an Intrusion Prevention Model for Ender-users
Lijun Dong Min Du College of Computer Sci., Huazhong Univ. of Sci. & Tech., Wuhan, China
Leo.DLJ@gmail.com
722 Institute, Shipbuilding Industry Corporation, Wuhan, China
jie112991@sina.com.cn
Shengsheng Yu Rongtao Liao College of Computer Sci., Huazhong Univ. of Sci. & Tech., Wuhan, China
College of Computer Sci., Huazhong Univ. of Sci. & Tech., Wuhan, China

Abstract
In order to provide sufficient protection against increasingly sophisticated cyber-attacks, Intrusion Prevention System (IPS) is explored. But in some cases, common IPS can not provide timely protection...
Towards Survivable Sensor Networks using Self-Regenerative Rejuvenation and Reconfiguration

Sazia Parvin
Network Security Laboratory
Korea Aerospace University
South Korea saziap@kau.ac.kr
Dong Seong Kim Network Security Laboratory
Korea Aerospace University South Korea dskim@kau.ac.kr
Jong Sou Park
Network Security Laboratory Korea Aerospace University
South Korea jspark@kau.ac.kr

Abstract
The previous works in sensor networks security have focused on the aspect of confidentiality, authentication and integrity based on cryptographic primitives. There has been no prior work to assess the survivability in systematic way. In this paper, we propose a framework for enhancing the survivability of sensor networks using self-regenerative software rejuvenation and reconfiguration. We utilize selfregenerative capabilities for detecting misbehaving in node level and apply software rejuvenation and reconfiguration methodology or both in order to extend the availability of sensor networks. The security analysis shows the feasibility of our approach.

The Communication Protocol for Wireless Sensor Network about LEACH

FAN Yiming Department of Information and Electronic Engineering of West branch of Zhejiang University of Technology, Zhejiang,China fyim@qzc.cn
YU Jianjun Department of Information and Electronic Engineering of West branch of Zhejiang University of Technology, Zhejiang,China yjj@qzc.cn

Abstract
This paper talk about the communication protocol named LEACH. The protocol focuses on reducing the power consumption of wireless sensor networks, which can have significant impact on the overall energy dissipation of these networks. LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporate data fusion into the routing protocol to reduce the amount of
information that must be transmitted to the base station. Simulations show that LEACH can achieve as much as a factor of 8 reductions in energy dissipation compared with conventional routing protocols. In addition, LEACH is able to distribute energy dissipation evenly throughout the sensors, doubling the useful system lifetime for the networks we simulated. We extend LEACH’s stochastic cluster head selection algorithm by a deterministic component. Depending on the network configuration an increase of network lifetime by about 30% can be accomplished.

PSMR: Publish/Subscribe Multi-cast Routing for Wireless Ad hoc Networks
Lidong Zhai, Xiaolei Ma, Jinchun Gao and Yuan’an Liu
Wireless Communication Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
Tel: +86-10-62283228, Fax: +86-10-62283228
E-mail: nakusakula@gmail.com

Abstract
With the widespread deployment and use of wireless data communications in the mobile computing domain, middleware as a mobile connector applied in distributed and potentially heterogeneous environments is in great need. Pub/Sub scheme with the strength of asynchronously, loosely coupled form of interaction between multi-points, so the middleware based on Pub/Sub scheme is well adapted to the dynamic, distributed interaction in large-scale mobile computing applications. In this paper, we describe the integration of the middleware based on Pub/Sub scheme and the multicast routing protocol of mobile Ad-hoc network, and present a multi-hop routing subscription (Publish / Subscribe Multi-hop Routing) protocol, named PSMR. PSMR helps to distribute the publisher’s data to subscribers and establish a Pub/Sub multi-hops network at the same time, and cooperate the layer of Pub/Sub scheme and the layer of routing work to distribute the data to make the transmission more reliable.

A Formulation for Ideal Signature Functionality and Its Realization*
*Research supported by the Key Technologies R&D Program of Henan Province of China (No. 0524220044, 0624260017, 072102210029); the S&R Found of HAUT of China (No. 050211,050215, 06XJC017,06XJC022)
Haojun Zhang
Henan University of Technology, ZhengZhou, Henan 450001, China zhj@haut.edu.cn
Huibin Wang Information Engineering University, ZhengZhou, Henan 450002, China wanghuibin8@163.com
Li Chen Information Engineering University, ZhengZhou, Henan 450002, China cl@hnife.edu.cn

Abstract
Universal Composition framework, UC, provides a methodology for designing and analyzing protocols. A secure protocol/task can be formulated to an ideal functionality, translate some realistic schemes into an ideal protocol so that it can securely emulate the ideal functionality. UC theory ensures the security of protocols is maintained under a general protocol composition operation. Signature is a primary cryptographic task. The present formulation of ideal signature functionality is introduced and some flaws are pointed out, and then an improved signature functionality is presented and proven that it is securely
realized by precisely those signature scheme that is equivalent to existential unforgey against chosen message attacks, EU-CMA.

**A Method on Detecting Unpredictability of Chaotic Signal**

Jianxiu Jin, Shuisheng Qiu, Liying Xie School of Electronic and Information, South China University of Technology, Guangzhou 510640, Guangdong, China
jxjin@scut.edu.cn
Mingku Feng
Dep. of Electronic Information Engineering, Guangdong Polytechnical Normal University, Guangzhou 510665, Guangdong, China fengmk@163.com

**Abstract**

A method on detecting unpredictability of chaotic signal is put forward, which is based on periodic orbit statistics. Chaotic time sequences come from analog circuit and numerical simulation respectively. Hot saddle periodic orbits (SPO) are found and its regression spectrum and regression frequency are investigated. The results show that the method is fit for detecting the unpredictability of chaotic system.

**AAA Architecture for Unified Configuration Management in Large-scale Network**

Wang Jinsong1,2, Lou Jia1, Wu Shaoying1, Wang Zhengxu1, Wu Gongyi2
1School of Computer Science and Technology, Tianjin Univ. of Technology, Tianjin, China
2Dept. of Computer Science, Nankai Univ., Tianjin, China

**Abstract**

Unified configuration management of network devices in large-scale environment is an important issue. As a traditional method, password authentication by router can not verify the administrators’ identities. In other words, someone who actually is not an administrator, can also access the router if he knows password. In this paper, we present a new policy-based AAA architecture that uses VPN and certificate-based authentication. By implementing the architecture, administrators can access authorized routers only and execute authorized commands. Single Sign-On mechanism is used to simplify authentication process. Moreover, the actions of administrators can be logged for accounting. Finally, we implement the architecture in Tianjin Education Metropolitan Area Network.

**Multi-agents Artificial Immune System (MAAIS) Inspired by Danger Theory for Anomaly Detection**

Haidong Fu Wuhan University of science & technology, China
Xiguo Yuan Wuhan University of science & technology, yuanxiguo21@sohu.com
Na Wang science & technology,

**Abstract**

Inspired by the potential interesting ideas of the danger theory (DT), the research into artificial immune system (AIS) has been developing faster then ever. The basic role of DT embedded in AIS is to provide what T-cells should respond through the professional antigen-presenting cells when there are some cells undergoing injury, or stress or ‘bad cell
death’.

However, in the context of AIS-based network security systems, how to minimize damage by mitigating virus infection is a key step to solve real-world problems. In this paper we present the blueprint of a DT inspired multi-agents AIS for anomaly detection, it is called MAAIS, which can dynamically adapt to various types of immune responses by configuring parameters during the course of evaluating the degree of danger signals received. Additionally, a suitable mechanism of communication between agents is employed to stipulate the better performance of the novel system.

A New Mechanism for Trusted Code Remote Execution
Liqiang Zhang Computer School, State Key Lab of Software Engineer, Wuhan University, Hubei, China whujking@126.com
Huanguo Zhang Computer School, State Key Lab of Software Engineer, Wuhan University, Hubei, China liss@whu.edu.cn
Xiantao Zhang Computer School, State Key Lab of Software Engineer, Wuhan University, Hubei, China xiantao@mail.whu.cn
Lu Chen Computer School, State Key Lab of Software Engineer, Wuhan University, Hubei, China ieucl@163.com

Abstract
Current authentication model in collaboration computing use entity’s identity to establish trust relationship, this kind of security mechanism is at great risk. The identity authentication only can guarantee that the interactive entity’s identities are real, but know nothing about the entities’ security status and behaviors. Therefore it also needs to carry on the authentication to the entity’s platform status, simultaneously needs to introduce a dynamic method which can carry on the authentication to the entity’s behavior. This paper integrates the identity authentication, platform authentication and behavior authentication based on Trusted Computing technology, remote attestation and trusted behavior, proposes a new mechanism for trusted code remote execution. This mechanism can solve the problem of codes executing remotely effectively.

AOP-Based J2EE Source Code Protection
Xiufeng Zhang Qiaoyan Wen† School of Science Beijing University of Posts and Telecommunications 100876, Beijing, China zhangxiufeng@tyut.edu.cn †wqy@bupt.edu.cn

Abstract
Encryption has become the mainstream to protect Java source code. However, there are defects, one of which is it cannot protect J2EE applications efficiently. This paper firstly analyses the problems encountered when applying this technology to protect J2EE applications, then resolves these problems using AOP technology, and thereby enlarges the range of encryption to protect Java source code.
Fair E-Cash System without Trustees for Multiple Banks
Jingliang Zhang
State Key Lab. of Integrated Service Networks, Xidian
Univ., Xi’an 710071, China; Department of Mathematics,
Ocean Univ. of China, Qingdao 266071, China zjlmlz@yahoo.com.cn
Lizhen Ma Department of Physics, Ocean Univ. of China,
Qingdao 266100, China zjlmlz@ouc.edu.cn
Yumin Wang State Key Lab. of Integrated Service Networks, Xidian
Univ., Xi’an710071, China ymwang@mail.xidian.edu.cn

Abstract
A new fair electronic cash system is proposed based on ACJT group blind signature and secret sharing
scheme. We use a novel method to trace the e-coin: under normal situation, the bank issues ordinary ecoin,
while under abnormal situation such as blackmailing, kidnapping etc., the bank issues marked
e-coin, and at the step of deposit, any bank in the group can recognize the marked e-coin. Furthermore,
our proposed scheme does not need a special trusted third party besides the Central Bank to trace users: a
shop owning suspicious e-coin and the bank having issued the coin can collaborate to find the user using
secret sharing scheme, however, any one of them can’t trace the user alone. Also, our scheme is
constructed
for multiple banks as in the real life, thus it is more practical..

Security in E-Commerce and the Economics of Immediate Satisfaction
Min Zhang Lecturer Social Physical Department Xi’an Institute of Physical
Education (XAIPE) NO.65 Han-guang Road Xi’an Shannxi China 710068
catclin@yahoo.com.cn
Renguoj Jiang PH.D Candidate Box 1203, Qu-Jiang Campus
Xi’an University of Technology (XAUT) NO.58 Yan-xiang Road Xi’an Shannxi China
710048
jiangrenguo@sina.com.cn
Haiqing Hu Professor Box 1203, Qu-Jiang Campus Xi’an University of Technology
(XAUT)
NO.58 Yan-xiang Road Xi’an Shannxi China 710048

Abstract
This paper apply lessons from the investigation on behavioral economics to understand the decision
making process with regard to safety in electronic business. This paper shows that it is unreasonable to
expect individual rationality in this context. Models of self-decision problems and satisfaction offer more
descriptions of the decision process and are more consistent with available data. In particular, this paper
shows why who may genuinely want to protect their safety might not do so because of psychological
tortuosity well documented in the behavioral literature; we show that these tortuosity may affect not
only ‘naive’ people but also ‘sophisticated’ ones; and we testify that this may occur also when people
become
aware of the risks from not protecting their safety as significant.

A Modified GJR-GARCH Model with Information Disseminating
Speed
Guo Qing Zhao and Jun Wei
School of Economics, Renmin University of China
A Dynamic Pricing Model for Postponement Supply Chain: the Bi-Level Programming Approach

Gui Shouping South China University of Technology  
E-business School Higher Education Mega Center, Guangzhou, P. R. China  
Niu Baozhuang* South China University of Technology E-business School  
Higher Education Mega Center, Guangzhou, P. R. China  

Abstract
The paper proposes a dynamic pricing model based on bi-level programming approach: firstly, we establish a two-stage distributed control model for postponement supply chain, which is the basis of the pricing model. Then, according to the pricing mechanism, we find that there is Stackelberg game feature in the process. Aimed at the feature, we propose a dynamic bi-level programming model, taking the centered warehousing & manufacturing point (CWMP) as the leader, and hence, the model is calculated and verified using the investigation data. We take chaos coverage hunting algorithm to solve the model, based on its features. Research shows: the dynamic pricing model is helpful to obtain the maximum profit of the whole supply chain, which is under the assumption of a twostage distributed control system; we obtain steady Equilibrium Prices (EP), which verify the efficiency of the decision-making model. The pricing model is proved to be useful to give reasonable prices of goods traded on postponement supply chain, and it is also an effective decision-making tool of supply chain coordination.

The Test and Calculation of the Underwriting Cycle in Property-Liability Insurance of China

Manying Bai School of Economics and Management ,  
Beihang University, Beijing, China. No.37, Xueyuan Load, Haidian district, Beijing, China  
Rui Zhao School of Economics and Management ,  
Beihang University, Beijing, China. No.37, Xueyuan Load, Haidian district, Beijing, China  

Abstract
The supply and demand of insurance interact with each other. Generally speaking, the result of this interaction is the appearance of underwriting cycle with cyclical fluctuation of insurance premium and the supply and demand of insurance as its main characteristic. Based on the ratios of premiums-to-claims data, the research of this paper sets up a recession model to test the existence of the underwriting cycle in
property-liability insurance of China and calculate its length. We found that, first, the underwriting cycle does not follow second order auto regression process. Second, according to the result, the length of underwriting cycle in property-liability insurance of China is 1.83 year. It plays an important role for the development of insurance of china to study internationally the actual situation of the underwriting cycle and take corresponding measures to stabilize and mitigate the cyclical fluctuation of insurance supply and demand.

A Fast Algorithm based on Tabled SAE Reuse
Hong-jun Wang1,2, Hua Li2, Yan-fei Li1, Hui He1, Shan Fan1, Li-li Wang1 1School of Information Science and Engineering, Shandong University, Ji’nan, China, 250100
2School of Electronic Information Engineering, Tianjin University, Tianjin, China, 300072

Abstract
H.264 can provide both objective and subjective image quality superior to existing standards by adopting new technical developments. But these developments increase the complexity and computation load of motion estimation greatly and make the encoder too complex to be applied in real-time applications. Although many fast algorithms are proposed, most of them would easily be trapped into local minimum. In this paper, we proposed a fast algorithm based on SAE reuse that can efficiently reduce the computational cost and quicken the matching speed while keeping the same quality.

A Novel Conditional Access Architecture for TV Service Protection
Jianbo Liu Communication University of China ljib@cuc.edu.cn
Cheng Yang Communication University of China cafeeyang@163.com
Jiayin Tian Communication University of China 34tianjiayin@163.com

Abstract
In broad TV network, the broadcasting will coexist with interactive services in a single Set-Top-Box (STB) device and the traditional unidirectional Conditional Access System (CAS) in DVB can’t be adapted to the variation. The dual-CAS is designed based on a double layer security scheme proposed in this paper to implement the authentication and access control, key updates between servers and STBs. In the dual-CAS, on the one hand, the layering user agent mechanism is established in STBs to provide transparent streaming security service to upper applications. On the other hand, the dual layer security scheme is designed to protect the ECM transmission, and master key management scheme is used to enhance the security and the system flexibility. In addition, two types of watermark are also involved in the dual-CAS, fingerprint watermark for piracy tracing, legality watermark for conditional playing. Contrast with the traditional DVB CAS, the dual-CAS architecture proposed in this paper is more flexibility and secure.

Trust-Contexts Modeling, Organization and Trust Estimation on the Web
Changli Zhang Department of Computer Science and Engineering, NWPU, Xi’an 710072, China charlieii@163.com
Abstract

Trust-contexts, computational models of the situational factors of trust behaviors, play important roles in trust decisions, but their researches are still in infancy. In this paper, based on earlier studies, trust-contexts are modeled and organized globally on the Web. Then, the basic ideas and an extension of trust estimation, which is the core step of trust decision, are focused. At last, more extensional topics are presented.

Detecting Malicious Witness Reports in Multi-agent Systems

This paper is supported by the National Grand Fundamental Research 973 Program of China under Grant No.2002CB312002, the Natural Science Foundation of the Education Department of Jiangsu Province of China under Grant No. 06KJB520132 and the Natural Science Foundation of Jiangsu Province of China under Grant No. BK2007074.

Maolin, Xing
1. Information engineering college of Yangzhou University, Yangzhou, China xingmlyz@163.com
2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China lb@yzu.edu.cn
Xingshen, Wu
1. Information engineering college of Yangzhou University, Yangzhou, China Wuxingshen@yahoo.com

Abstract

In open Multi-agent Systems, trust plays the central role in facilitating interactions. Most of trust models need to collect the witness reports, and they may suffer due to existence of malicious witness. To detect the malicious witness reports, this paper presents an approach, OSM (Opinion Similarity Measure). Evaluator calculates the opinion similarity state (OSS) between evaluator and witness according to their reports, and evaluates the witness credibility according to the OSS between them. Experiment and analysis show that OSM is more robust than existing approaches.

Trust Management and Service Selection in Pervasive Computing Environments

Shangyuan Guan, Xiaoshe Dong, Weigu Wu, Yiduo Mei, Shihua Liao
School of Electronic and Information Engineering Xi'an Jiaotong University, Xi'an, China
{guansy, meiyiduo}@gmail.com, {xsdong, wgwu}@mail.xjtu.edu.cn

Abstract
Trust is an important aspect of decision making for pervasive applications and it is important to choose and use service efficiently in pervasive computing environments. This paper presents trust force to specify trust among interactive entities in a pervasive computing environment utilizing experience and knowledge in a social network and the coulomb's law in real word. Based on trust force, we present a Trust Management and Service Selection model, named TMSS. TMSS was tested and the experimental results show that our method for selecting service is not only more efficient than traditional and heuristic methods, but also can isolate malicious services.

Searching for the Classification Concept in WCO
Zhu Hongning, Hu Xianwei, Wang Yu, Zhang Bin
School of Information Science and Engineering
Northeastern University, Shenyang, 110004, P. R. China

Abstract
Aiming at the web information heterogeneous problems, we use the structure and the semantic characteristics of ontology, on the basis of the web information classification glossary, to construct the web classification ontology (WCO) suitable for the web applications, provide the searching algorithms for the concept node of the web information classification in WCO, and supply the experimental result, in order to research on the standardization and combination of the web information classification architecture (CA).

A Research on the Steganography Capacity of the Reed-Solomon Codes
LIU Cui-Qing, PING Xi-Jian
Zhengzhou Information Science and Technology Institute Zhengzhou 450002, China
liu-cuiqing@163.com
WANG Yun-He
Chinese People’s Public Security University Beijing 100038, China crane23@163.com

Abstract
With the right length of the shared key the steganography method based on the error-correcting codes is perfectly secure. By modifying the part of the codeword of the Reed-Solomon codes according to the error map we can embed the secret information into the RS codeword as there is a mapping code between secret information and codeword error map. The steganography capacity of the RS codes is dependent upon its parameter of the codeword and the codeword error map that attend to the information hiding. In this paper we would present some algorithms that calculate the steganography capacity of RS codes.

Text Information Hiding Based on Part of Speech Grammar
Dai zuxu
Huazhong university of science and Technology School of computer science and technology
430074 Wuhan, P.R.China
zuxudai@china.com
Hong fan, Yang muxiang and Cui guohua
Huazhong university of science and technology School of computer science and technology
430074 Wuhan, P.R.China
Abstract
Method for text information hiding based on Part of Speech (PoS) Grammar is proposed. A context free PoS grammar generates PoS strings, which are patterns of natural language sentences. Taking PoS strings as a transform domain of natural language, the method maps both secret message and cover text to the domain, then maps each PoS string to a number where sentence appears in the cover text by string matching, and sequence of the numbers is the secret key. Using the secret key, receiver extracts the secret message by syntactic analysis. Further more, a formula computing the capacity of hidden information is given. This method does not require any modification of text, meanwhile, it is a sound solution of the problem cover text is syntactic but not semantic that Wayner’s scheme encountered.

Key words: Text information hiding, Part of Speech grammar, Sentence pattern, Mimic function

Reversible Image Authentication Based on Combination of Reversible and LSB Algorithm*
* This work was supported by Key Program of Natural Science Fund of Tianjin (07JCZDJC06600), China
Tiegang Gao College of Software, Nankai University Tianjin ,Chian, 300071
gaoftiegang@nankai.edu.cn Qiaolun Gu Antai School of Management, Shanghai Jiaotong University. Shanghai 200052, P.R. China tiguqiaolun@sohu.com

Abstract
Nowadays, digital watermarking algorithms are widely applied to ownership protection and tampering detection of digital images. In this paper, a new image ownership and tampering authentication scheme based on combination of reversible algorithm and LSB replacement is proposed. In the scheme, the original image is split into many non-overlapping blocks. Feature data of image is extracted according the attribute of the block, for some blocks, feature data is embedded into the differences of some pixels, and for the other blocks, the data is embedded in the lease significant bit of some pixels. the interesting point and usefulness of the algorithm lies in that watermarked image can be exactly restored into the same as the original image. The experimental results show that the quality of the embedded image is very high, and the positions of the tampered parts are located correctly.

Watermarking 3D Meshes Based on Fixed Spectral Basis
Tao Xu, Yanning Zhang, Jinqiu Sun, Zenggang Lin School of Computer Northwestern Polytechnical University Xi’an, P.R.China

Abstract Watermarking 3D meshes in transformed domain by using traditional Laplacian matrix decomposing may become unstable, since the valence of meshes may be different. To solve this problem, the proposed watermarking algorithm produced fixed spectral basis by using the dual graph derived from the mesh topology and projected geometric features of the dual graph onto fixed spectral basis. In order to resist similar transforming, a geometric invariant vector was chose as watermark covering data. Watermarking signal was hided into low frequency coefficients by their linear relations. Original mesh data were not needed when extracting watermark. The proposed algorithm can resist translating, rotating, uniformed scaling, and also have robustness against mesh geometry compressing, adding noise with low intensity.master_xutao@163.com, ynzhang@nwpu.edu.cn
Perceptual Steganography Based on Adaptive Quantization-Embedder
Guangjie Liu, Yuewei Dai, Zhiquan Wang Automation School Nanjing University of Sci.& Tech. Nanjing, 210094, China guangj liu@yahoo.com.cn Shiguo Lian France Telecom R&D Beijing Beijing, 10080, China sg lian@163.com

Abstract
A steganographic scheme based on adaptive quantization-embedder is proposed in this paper. The scheme uses the new constructed contrast-correlation distortion metric to optimally choose quantization steps for image blocks to guarantee more data being embedded in busy areas. Different form existing methods, our scheme embeds the AQE parameters together with message bits into the cover image. Simulation experiments show the proposed scheme can provide a good trade-off between the perceptibility and the capacity.

DCT-Based Video Watermarking Transcoding Technique
DU Yao-gang Beijing Electronic Science and Technology Institute No.7,Fufeng Road,Fengtai district, Beijing P.R.China(100070) duyaoanga@besti.edu.cn ZHANG Yan-Shuo,Wang Li-Feng Beijing Electronic Science and Technology Institute No.7,Fufeng Road,Fengtai district, Beijing P.R.China(100070)

Abstract
This paper presents a new technique of how to insert additively imperceptual watermarking to resist downsampling attack according to Watson's model based DCT domain and the block classification. Firstly, we obtain subimages through quasi-convoluted downsampling technique; Secondly, downsampling video block is classified as five categories by computing the luminance block variance; Finally, the region and strength of optimizing watermark complied with standard normal distribution(zero mean and unit variance) is additively embedded into the unmarked original downsampling characteristic and a perceptual distortion constraint, which greatly improves robustness of upsampling watermarked video. The original video is not required for watermark detection. Simulation results in video quality degrading averagely with PNSR 3.4dB but subjective quality remaining. The proposed scheme is not only robust to downsampling attack, but also achieves a low computational complexity.

Keywords : video watermarking transcoding, DCT domain downsampling, correlation detection.

Passphrase with Semantic Noises and a Proof on Its Higher Information Rate
Kok-Wah Lee Faculty of Engineering & Technology Multimedia University 75450 Bukit Beruang, Malaysia kwlee@mmu.edu.my Hong-Tat Ewe Faculty of Information Technology Multimedia University 63100 Cyberjaya, Malaysia htewe@mmu.edu.my

Abstract
Key size becomes very important to a cryptographic algorithm according to Kerckhoff's law where a civilian cryptosystem shall depend fully on key secrecy. Currently, there are four passphrase generation methods: Sentence, acronym, diceware, and coinware. Unicity distance is the minimum size of ciphertext for unique decipherability of ciphertext when number of spurious keys is zero. A key with size less than unicity distance is good where there are spurious keys which allow a protection method using limited unsuccessful
logins. Here, stronger forms of passphrases using textual semantic noises like punctuation marks, mnemonic substitution, misspelling, and associative morphing, which improve the key entropy, are proposed. An ASCII mutual substitution table is presented together with its proof on information rate increment. Higher information rate has lower encrypted keys the short cryptogram in a key vault, like Password Safe, cannot be cryptanalyzed within certain limited login attempts.

Keywords: Key security, passphrase, semantic noises, unicity distance, ASCII mutual substitution table.

Forward-Secure Public-Key Encryption Scheme with Tamper Evidence

Jiang Han, Xu QiuLiang, Hou MengBo

School of computer science and technology, Shan Dong University

jianghan@sdu.edu.cn, xql@sdu.edu.cn, houmb@sdu.edu.cn

Abstract

Forward Secure is an effective way to solve the key exposure problem, but how to find out the period when the key was exposed and give out the evidence have not be studied. Based on the Tamper Evidence, we define a new notion of Forward-Secure Public-Key Encryption Scheme with Tamper Evidence (TE-FEnc) and propose a general method to build a TE-FEnc scheme. We also give out a concrete instance at last. In the standard model, we prove that our scheme is Forward secure, strong Forward Tamper-Evidence secure, and achieve security against chosen ciphertext attacks.

Content Dependent Image Watermarking using Chaos and Robust Hash

Wei Lu 1,2 and Hongtao Lu 2

1 Department of Computer Science, Sun Yat-sen University, Guangzhou 510275, China
2 Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China E-mail: luwei3@mail.sysu.edu.cn, lu-ht@cs.sjtu.edu.cn

Abstract

Most of the present watermarking schemes focused on achieving the robustness to common signal processing and geometrical distortions. However, there are many special attacks to watermarking introduced in recent years, such as collusion attacks, copy attacks, denoising and so on. So, how to design robust watermarking scheme against these attacks is a key step for watermarking application in practice. This paper presents a novel content dependent image watermarking using robust media hash and chaotic map. Through constructing a content dependent watermark, the proposed scheme achieves good robustness against some special attacks, which is also demonstrated in the experiments.

A Novel Watermark Algorithm for Blind Extraction

Li Yu
University of Electronic Science and Technology of China School of Automation Engineering
No.4 Section 2, North Jianshe Road, Chengdu, P.R.China lyu@uestc.edu.cn

Fen Chen
University of Electronic Science and Technology of China School of Automation Engineering
No.4 Section 2, North Jianshe Road, Chengdu, P.R.China chenfen@uestc.edu.cn

Abstract
A novel blind watermark algorithm based on DCT is proposed to embed several same watermarks into
digital images in this paper. The watermark is designed to be decoded without the original image.
Experimental results show that embedded watermarks quality and are robust in varying degree to JPEG
compression, low-pass filtering, noise contamination, and cropping attacks.

A Robust Dual Digital-Image Watermarking Technique
Kai-xing WU School of information & Electronic Engineering Hebei
University of Engineering, Handan, Hebei
Wei-wei YAN School of information & Electronic Engineering Hebei
University of Engineering, Handan, Hebei vivi821014@163.com
Jing DU School of information & Electronic Engineering Hebei
University of Engineering, Handan, Hebei

Abstract
In this paper a robust dual watermarking technique is suggested that incorporates two
watermarks in a host image for improved protection and robustness. To embed the watermark robustly
and imperceptibly, watermark bits are added to the significant coefficients of each subband selected by
considering the human visual system (HVS) characteristics. A watermark, named Boat (will be
called the secondary watermark), is embedded in the wavelet domain of a primary watermark before
being embedded in the host image. From the experimental results it can be observed that
proposed method is robust to wide variety of attacks.

Steganalysis Based on Lifting Wavelet Transform for Palette Images
Jiaohua Qin1,2, Xingming Sun1, Xuyu Xiang1,2
1School of Computer & Communication, Hunan University, Changsha, Hunan, China, 410082
2Department of mathematics & computer, Hunan City University, Yiyang, Hunan, China, 413000
{qinjiaohua, sunnudt, xyuxiang}@163.com

Abstract
Based on the statistical analysis of the correlation between the low frequency sub-band coefficients and the
high frequency sub-band coefficients in wavelet domain, a novel steganalytic algorithm with the ability of
reliable detecting modifications in palette images is proposed in this paper. Firstly, we divide the image into
non-overlapping 8 × 8 blocks and perform Integer Wavelet Transform based on lifting scheme to each
block. Then, the average correlation, which is used to determine whether the secret message exists or not in
palette images, is calculated according to the correlation between low frequency coefficients and high
frequency coefficients. Experimental results show that the new algorithm can achieve better performance
than the Pairs Analysis. Moreover, it is easy to be implemented and well-suited for real-time detection.

A Joint Biometrics and Watermarking Based Framework for
Fingerprinting,
Copyright Protection, Proof of Ownership, and Security Applications
Shiraz Ahmad 1
1 Dept. of Electronic & Information Engg., Harbin Institute of Technology
Shenzhen Graduate School (HITSGS), Shenzhen 518055, P. R. China.
shiraz_shiraz@yahoo.com
Zhe-Ming Lu 1, 2 Media Processing & Communication Lab., School of Information
Science and
Technology, Sun Yat-Sen University, Guangzhou 510275, P. R. China.
luzhem@mail.sysu.edu.cn

Abstract
In this paper we present a novel framework employing biometric recognition and robust watermarking
technique to achieve a number of media privacy and security objectives. Scheme description
and presented test results support and prove the claims of practicability and effectiveness of the model for a
number of privacy and security related applications.

An image steganographic method with noise visibility function and
dynamic
programming strategy on partitioned pixels
Ying-hua Lu 1 Jun Kong 1, 2, *
{ Computer school, Northeast Normal University, Changchun, Jilin Province,
China { luyh, kongjun } @nenu.edu.cn Si-hui Li 1, 2 Jing Qin 1, 2 Key Laboratory for
Applied Statistics
of MOE, China { lish448, qinj549 } @nenu.edu.cn

Abstract
In this paper, we proposed a novel image steganographic method. Considering the visual quality
of the stego-image, the pixels of host image are classified into three groups according to the noise
visibility function values of the pixels. For each group of pixels, the corresponding secret pixel values go
through an optimal substitution process and are transformed into other pixel values. Then the optimal
substitution is obtained by dynamic programming strategy. To get the good image quality of the
stegoimage,
the modulus function is employed to hide the secret bits into host pixels. According to our
experimental results, this method can provide better stego-image quality than some traditional schemes.

Selection on Wavelet Base for The Detection of ship pitching
Movement Disturbances
Sun Li-hong 1, 2
1 Automation College Harbin Engineering University
2 College of Foundation Science Harbin University of Commerce.
Email: honghong9942@yahoo.com.cn

Abstract
wavelet analysis is becoming a useful tool because it allows the decomposition of data functions into different
frequency or scale components. Accordingly wavelet transforms are to be suited to analyze short-timed
high-frequency phenomena. The remarkable ability of wavelets to highlight the singularities associated with
shocks present in the ship pitch field is explored. In the detection of ship pitch disturbance, It was observed in the
singularity signal the sharp points were located at the position responding to the end or the start of disturbances. Singularity theory of detecting signal based on wavelet transform was applied to the local detection of these sharp points, the mother wavelet option method is studied. Simulations verify the detecting validity and accuracy of the selected mother wavelet.

**Keywords:** wavelet transform; mother wavelet; singularity signal; wavelet scale

### Moving Targets Detection and Tracking Based on Nonlinear Adaptive Filtering

Wang Ying-li
Department of Automation Measurement and Control Engineering, P.O.Box 308, Harbin Institute of Technology, Harbin 150001, China wyl10411@163.com
Dai Jing-min Tutor Department of Automation Measurement and Control Engineering, P.O.Box 308, Harbin Institute of Technology, Harbin 150001, China

**Abstract**

To resolve the problem of the missile detection in the space early-warning process, an efficient method based on nonlinear adaptive filtering is proposed to detect the small IR target of low SNR under the complex background in this paper. The method can eliminate the influence of the unbalance background to the image segmentation, select the small moving target and the noise points and then eliminate wrong point targets to obtain the satisfactory detection result. The effectiveness of the method is proved by the experimental results for several infrared image sequences.

### The Detection Arithmetic Of Soft Decision Based On Non-ideal Channel In Distributed Detection

Ying-kun Liu
Air Force Engineering University
No.1 Feng Hao Road, Xi’an, China
ms.liu@56.com
Xin-xi Feng
Air Force Engineering University
No.1 Feng Hao Road, Xi’an, China

**Abstract**

In this paper we expand the arithmetic of the distributed detection in two aspects. In order to improve the detection performance and use communicated resource rationally, the local decision is extended from hard decision to soft decision. According tonon-ideal independent channels, the local decision and reliability information are transmitted to the fusion center. The non-ideal channel is extended from binary symmetry channel to memorial channel. Then we derive the optimal decision form of the local detectors and fusion center by NP(Neyman-pearson) rule. At last stimulation of two detectors shows that using soft decision improves the detection performance and worsen channel depress the detection performance surely

### A New Blind Signature and Threshold Blind Signature Scheme from Pairings

Wei Cui, Yang Xin, Yixian Yang, Xinxin Niu
Information Security Center, State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
Email: dacui635@163.com

Abstract
An efficient provably secure identity-based blind signature (IBBS) scheme based on bilinear pairings is proposed. Assuming the intractability of the q-Strong Diffie-Hellman problem, our IBBS is unforgeable under adaptive chosen-message and ID attack. Because of avoiding using the inefficient MapToPoint function, our IBBS can offer advantages in runtime over the schemes available. Based on this ID-based blind signature scheme, we describe the first ID-based threshold blind signature (TBS) and show that it has security properties of unforgeability and robustness.

Audio Digital Watermarking Algorithm Based on Wavelet Analysis
Jie-Chang Wen Faculty of Applied Mathematics
Guangdong University of Technology Guangzhou, China wjcpi@126.com

Abstract
This article mainly researches on the principle of digital audio signal embedded watermarking and the usage of wavelet transform to realize the audio digital watermark embedding and extracting algorithm. This algorithm has good stealth and robustness. The influence of embedded watermarking on the original audio signal can not be found by human perceptual system and can resist the general signal attack.

Double Secret Keys and Double Random Numbers Authentication Scheme
Tian-Junfeng, Jiao-Hongqiang, Li Ning, Liu Tao
Institute of Computer Network Technology Hebei University

Abstract
This paper presents the mutual authentication scheme based on Bilinear pairings with the deployment of smart card. We propose a novel technique of using double secret keys and double random numbers for preventing forgery attack in authentication process. It enhances the security of the authentication system and accomplishes the mutual authentication safely between user and remote system. Finally, we provide the validity and compute complexity.

Efficient Identity Authentication Protocol and Its Formal Analysis
Li Chen¹,² and Guixiang Zhang¹ and Xiangdong Li²
1. Computer Center,
Henan University of Finance and Economics
2. Department of Network Engineering,
Information Engineering University,
Zhengzhou, Henan 450002, China
cl@hnufe.edu.cn

Abstract
The paper proposes an efficient identity authentication protocol for mobile commerce based on token. The proposed protocol needs fewer messages to authenticate identities of mobile users called as important entities in the foremost time, as well as session keys used for transaction are negotiated efficiently. To analyze the proposed protocol, the paper also proposes an extension of BAN logic. Using the extended BAN logic, the objective and security of the protocol are proved by the formal analytical process.
Improving the C-Scheme by Allocating Unique Secret Parameters for Different Users
Jin Jiang 1, 2, Zhihong Huang 2, Lei Li 2
1 South China University of Technology, GuangZhou, 510640, China
2 HydeInfo Technology Ltd, GuangZhou, 510095, China
joyfulson.jiang, lhdhzh, pubertllg@gmail.com

Abstract
Different from conventional authentication approaches, an authentication scheme using n-dimensional construction method based on circle property (henceforth called C-Scheme) is proposed in paper[17]. Then the scheme is analyzed in improved respectively in paper[5] and paper[16]. However, this paper shows a weakness of the C-Scheme and proposes an improvement to the weakness by allocating unique secret parameters for different users in the C-Scheme. After analysis, the improved C-Scheme achieves a higher security level.

A TPM Authentication Scheme for Mobile IP
Liu Jing-sen
College of Automation Northwestern Polytechnical University
Xi'an, Shaanxi, 710072, China ljs@henu.edu.cn
Dai Guan-zhong
College of Automation Northwestern Polytechnical University Xi'an, Shaanxi, 710072, China daigz@nwpu.edu.cn
Li Yu
Research Lab of Management Science and Engineering Henan University Kaifeng, Henan, 475004, China leey@henu.edu.cn

Abstract
In Mobile IP scheme, if mobility agents and mobile nodes are trusted computing platforms (TCPs), the combination of Mobile IP registration authentication and trusted platform module (TPM) authentication is expected. But neither the Privacy CA scheme nor the direct anonymous attestation (DAA) scheme provides the authentication between TMs that belong to different authenticating domains. This paper proposes an improved scheme based on the existing DAA scheme. The improved scheme adds a CA layer on the authenticating domains that could share the trusted relationship. It could achieve the authentication between TMs that belong to different authenticating domains. This scheme has the security and anonymity identical to the DAA, and it can therefore satisfy the requirement of Mobile IP authentication.

ID-Based Authenticated Blind Signature Scheme from Bilinear Pairings
Zemao Zhao
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, P.R.China
Email: zhaozm@hdu.edu.cn

Abstract: An ID-based authenticated blind signature scheme was proposed using the bilinear paring based on elliptic. The proposed scheme combines the authenticated functions for user with blind signature, which implements effectively user’s identity authenticated function and blind signature, makes user not need exceed certified system to verify legal, and improves system work efficiency.
Key words: Identity-based cryptosystem, blind signature, Authorized blind signature, bilinear pairings

Cryptanalysis and Improvement on An Threshold Key Issuing Protocol
Zhang Bo1, Xu QiuLiang2, Liu Xin3
School of computer science and technology, Shan Dong University1,2,3
zbsdu@126.com1, xql@sdu.edu.cn2, lxonsin_cn@sina.com3

Abstract
Key issuing protocols deal with overcoming the two inherent problems: key escrow and secure channel requirement of the identity based cryptosystems. An efficient and secure key issuing protocol enables the identity-based cryptosystems to be applicable in the world. We analyze an threshold key issuing protocol due to Gangishetti et al. and show that the protocol suffers from the attacks of the malicious KGC and the users can deny that they have never received the key. Furthermore, we present an improved protocol, which is undeniable and secure against KGC’s attacks.

A Schema of Automated Design Security Protocols
Haifeng Xue, Huanguo Zhang
School of Computer, Wuhan University; The State Key Laboratory of Software, Wuhan University; Wuhan 430072, Hubei, China
liss@whu.edu.cn
Sihan Qing Institute of Software, Chinese Academy of Sciences, Beijing 100080, China
qsihan@ercist.icas.ac.cn

Abstract
This paper proposes a novel approach to automated design of security protocols using artificial immune algorithm based on cord calculus. Designing security protocol is notoriously difficult and errorprone. Artificial immune algorithm is a powerfully intelligent algorithm. The cord calculus is applied to the artificial immune algorithm to instruct the search and compose of security protocols. Automated design of security protocols using artificial immune algorithm can alleviate people’s burden of manually design security protocols and get more security and reliable protocols.

An Efficient Group Key Agreement Protocol from Bilinear Pairings
Chengyu Hu
Institute of Network Security Shandong University, Jinan, P.R.China
hc@mail.sdu.edu.cn
Pengtao Liu Shandong Political-Legality Institute
Jinan, P.R.China lpt@mail.sdu.edu.cn
Daxing Li Institute of Network Security Shandong University, Jinan, P.R.China
lidaxing@vip.sina.com

Abstract
A group key agreement protocol is designed to efficiently implement secure multicast channels for a group of parties communicating over an distrustful, open network by allowing them to agree on a common secret key. Recently some constant-round protocols have been proposed. However, some of them are too expensive with computational complexity $O(n)$, others with lower computational complexity doesn’t ensure the participants to get the same session key.
In this paper we propose a new constant-round protocol suited for groups consisting of many hosts with limited computational capability and a host with more computational power. Then we prove its security.

Security Analysis on a Blind Signature Scheme Based on Elgamal Signature Equation
Yu Baozheng, Xu Congwei
School of Management
Hefei University of Technology Hefei, Anhui 230009
Email: chinaybz@126.com

Abstract
Universal forgery attacks and selected forgery attacks on both weak and strong blind signature schemes based on Elgamal signature equation proposed by Wang et al. are developed. Without using any secret key, anyone can forge a valid signature through selecting some random parameters. The possibility of forging the blind schemes is analyzed and moreover, an improved weak blind signature scheme and an improved strong blind signature scheme are designed. Also, the securities of the improved blind signatures are analyzed.

An Improvement of Authentication Test for Security Protocol Analysis
Xiangdong Li Qingxian Wang
Dept. of Network Engineering
Information Engineering University
No.7, Jianxue Street, Zhengzhou, China 450002
Lixiangdong2510@126.com wqx2008@vip.sina.com

Abstract
Authentication Test (AT), based on strand spaces, is a method used to verify cryptographic protocols. This paper identifies an inaccuracy existing in AT and presents an improvement called Authenticated Authentication Test (AAT). An analysis of Denning-Sacco and other protocols using AAT shows that the improved method is effective.

A verifiable multi-secret sharing scheme (VMSS)
Pang Liaojun
Institute of Intelligent Info. Proc., Xidian Univ., Xi’an 710071
Mini. of Edu. Key Lab. of Comp. Netw. & Info. Secu., Xidian Univ., Xi'an 710071 ljipang@mail.xidian.edu.cn Li Huixian School of Compt. Sci. & Eng., Northwestern Polytechnical Univ., Xi'an 710072, Chinalihuixian@nwpu.edu.cn Jiao LichengInstitute of Intelligent Info. Proc., Xidian Univ., Xi’an 710071 lchjiao@mail.xidian.edu.cn Wang Yumin
Mini. of Edu. Key Lab. of Comp. Netw. & Info. Mini. Secu., Xidian Univ., Xi'an 710071 ymwang@xidian.edu.cn

Abstract
Chien et al. proposed a new type of multi-secret sharing scheme based on the systematic block codes, in which multiple secrets instead of only one secret can be shared in each sharing session. Their scheme is very useful especially in sharing a large secret. But, there are still some problems in their scheme: the secret shadows are generated by the dealer and must be redistributed to each participant over a secure channel; the scheme does not provide any mechanism to check whether the dealer or every participant is honest. In order to overcome the problems, this paper proposes a modified multi-secret sharing scheme
with verification added. At the same time, no secure channel is needed in the proposed scheme. Compared with Chien et al.’s scheme, the proposed scheme is more practical and efficient.

**Unambiguous Measurements Based Quantum Cryptography**
Wei Yang Liusheng Huang Yonglong Luo
Department of Computer Science and Technology
National High Performance Computing Center at Hefei
University of Science and Technology of China, Hefei, 230027, P. R. China
smartyw@mail.ustc.edu.cn lshuang@ustc.edu.cn vlluo@ustc.edu.cn

**Abstract**
A new quantum cryptography (quantum key distribution) scheme based on unambiguous measurements is presented, which is secure against any individual attack allowed by quantum physics. By carefully constructing the unambiguous measurements elements a higher efficiency than previous protocols is achieved. Furthermore, an equality for the probability of the participant's reliable measurement outcome and the polarization angle that he chooses when distinguishing between two non-orthogonal states is also derived in this paper.

**SPUC: Security Protocol for Ubiquitous Computing**
Fan Yang, Qingcong Lv, Qiying Cao
Department of Computer Science & Technology,
Donghua University, Shanghai, China, 201620
Yangfanon19@mail.dhu.edu.cn

**Abstract**
We present a security protocol for ubiquitous computing. It provides data authentication, and data freshness besides inobtrusiveness that is the essential property of ubiquitous computing. We creatively use both asymmetric-key and symmetric-key algorithms to make the protocol more security and suffice severe resource constraints, limited computation, memory, and communication capacities.

**A Proxy Blind Signature Scheme with Proxy Revocation**
Ji-Hye Park
Department of Computer Science and Engineering
Sogang University jhpark@alglab.sogang.ac.kr
Young-Seol Kim Department of Computer Science and Engineering
Sogang University yskim@alglab.sogang.ac.kr
Jik Hyun Chang Department of Computer Science and Engineering
Sogang University jchang@alglab.sogang.ac.kr

**Abstract**
A proxy blind signature allows the designated proxy signer using the proxy private key to generate a blind signature on behalf of the original signer. In previous proxy blind signature schemes, there was no revocation protocol wherein the original signer could delegate his signing capability to a proxy signer. In this paper, we propose a proxy blind signature scheme with the proxy revocation, where the original signer can revoke his delegation to a proxy signer whenever he wants. Moreover, the proposed scheme satisfies all security properties for the proxy blind signature.

**New Simple Matrix Representation Method of the BM Algorithm Using in Flowing Cipher Field**
Abstract
In this paper, a new simple representation of the Berlekamp-Massey algorithm was proposed, which resolves the problem of the length of the shortest linear recurrence in the flowing cipher study. In the process of investigating the Berlekamp-Massey algorithm, using matrix-method can help to simplify the representation of the Berlekamp-Massey algorithm and easily calculate the distributing regulation of the shortest linear recurrence length compared to the traditional method.

Logical Mistakes in NTRU Compensation Algorithm and Improvement of Encryption Verification Algorithm
Supported by National Natural Science Foundation of China (60673072)
Yining Quan, Xinshe Li, Yupu Hu
Key Laboratory of Computer Networks & Information Security, Ministry of Education,
XiDian Univ., Xi’an 710071, China
ynquan@mail.xidian.edu.cn

Abstract
The basic security of NTRU is based on the hardness of the shortest vector problem (SVP) of some lattice, named as CS lattice. Dealing with the decryption failure problem of NTRU is an important topic. The logical mistakes and defects of NTRU compensation algorithm [1] which is used for dealing with the decryption failure problem of NTRU are analyzed. The compensation algorithm is proven to be incorrect in this paper. It seems that NTRU encryption verification algorithm [2] can cope with the decryption failure problem of NTRU. But in fact, it is hard to get a satisfying result. An improvement scheme on NTRU encryption verification algorithm [2] is also put forward and discussed, which can correctly resume the plaintext in high probability while the security is the same with NTRU.

Block Sampling Algorithm of Image Encryption Based on Chaotic Scrambling
Ren Hong-e
Northeast Forestry University
Information and Computer Engineering
College Harbin, 150040, China
Abstract
Base on the randomness and initial value sensitivity of Lu chaotic sequence, dividing the original image into blocks, carrying out the gray scrambling and location scrambling on each team of the pixel points, making their location and grey distribute evenly at the same time, it can accomplish the encryption of a image. Using Matlab to simulate, the result indicates that this algorithm has great secret key’s space, and it also has the ability of resisting statistic attack and damage. For 256 × 256 BMP image which data size is 192k, encryption cost approximately 0.152s and decryption cost approximately 0.161s.

New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography
Dang Hoai Bac 1 2; Nguyen Binh 1; Nguyen Xuan Quynh 1
1: Electronics Faculty, Posts & Telecommunications Institute of Technology (PTIT), Vietnam.
2: Mobile Telecommunication Division, Electronics & Telecommunications Research Institute (ETRI), Korea.
bac@etri.re.kr

Abstract
Currently, there are many methods for constructing cryptosystems based on various algebraic structures. This paper presents a proposed cryptosystem that based on a new algebraic structure with simple and flexible properties. This cryptosystem is constructed from Cyclic Geometric Progressions over polynomial ring in finite field, in which it is considered as a polyalphabetic cipher. Simple scheme for cryptosystem using the cyclic geometric progression over polynomial ring is described. The new structure of multiplicative group and Cyclic over polynomial ring is also mentioned in this paper.

Key words: Multiplicative group, Cyclic Geometric Progressions (CGPs), quadratic residue, cyclotomic coset

Cryptanalysis of Liao et al.’s Blind Signature Scheme from CIS’05
Yongjian Liao
School of Computer Science Engineering,
Univ. of Electronic Science and Technology of China. Chengdu,610054,China
sc lyj@sina.com.cn
Qihang Wang
Department of Business Administration,
Chongqing Electronics Engineering Vocational College. Chongqing, 401331, China
Abstract
Liao et al. proposed first blind signature schemes without random oracles from pairings and provided security proofs in CIS’05. However, we show that their blind scheme is neither blind, nor unforgeable, anyone not to query the signing oracle can forge signature of any message.

Key Words: Cryptography; Blind signature; Without random oracles; Pairings.

Cryptanalysis of MAJE4
Mohammad Ali Orumiehchi ha
Zaeim electronic industries company
P.O. BOX 14155-1434, Tehran, Iran
orumiehchi@zaeim.co.ir
Elham Shakour
Zaeim electronic industries company
P.O. BOX 14155-1434, Tehran, Iran
shakour@zaeim.co.ir

Abstract
In this paper, some weak points in design of MAJE4 algorithm are probed and by exploiting them, two cryptographic attacks are proposed for both versions (128-bit, 256-bit). It is proved that MAJE4 is vulnerable against key recovery attack with complexity less than exhaustive search. We show the security of MAJE4-128, -256 are not greater than $2^{96}$ and $2^{106}$ respectively. And also, a distinguish attack is examined that can recognize the output running keys from a truly random stream with data complexity of $2^{78.8}$ and $2^{84.8}$ output words for MAJE4-128 and MAJE4-256 respectively.

Efficient Secure Group Signature Scheme with Revocation
Rongbo Zhu
College of Computer Science
South-Central University for Nationalities
Minyuan Road 708, Wuhan 430074, China
rongbozhu@gmail.com
Xiaozhu Liu
School of Automation
Wuhan University of Technology
Luoshi Road 122, Wuhan 430070, China
lxz_h@163.com

Abstract
Because group signature schemes allow us to anonymously verify user’s ownership of some privileges, it is applied to various security protocols such as anonymous e-cashes, biddings and so on. But, in order for the whole group signature concepts to become really practical, the problems of secure and efficient group member revocation must be treated nicely. In this paper, we construct a novel efficient and secure revocation method for group signature schemes. The length of the group public key and the size of signatures are independent of the number of the group members. Furthermore, the proposed scheme is very convenient for members to join to or to leave from the group.

One-way Hash function construction based on iterating a chaotic map
Yong Wang1,2
1School of Computer Science and Engineering, Chongqing University,
Chongqing, 400044, PRChina wangyong_cqu@163.com
Degang Yang1,3
1School of Mathematics and Computer Science, Chongqing Normal University, 40047, PR China ydg42@163.com
Maokang Du2 School of Economy and Management, Chongqing University of Posts and Telecommunications, 400065, China excel@126.com Huaqian Yang1,4 4Department of Computer and Modern Education, Chongqing Education College, Chongqing 400067, PR China yhq_cq@163.com

Abstract
An algorithm for one-way Hash function construction based on iterating a chaotic map is proposed. The total chaotic space is divided into some subspace based on the density distribution function of the chaotic map. Each subspace is associated with a unique bit in a bit sequence. The value of the chaotic map is dynamically decided by the last-time value and the corresponding message bit in different positions. When the chaotic value is in one subspace, changes the corresponding bit. Finally, the bit sequence is used as the Hash value. Theoretical analysis and computer simulation indicate that the algorithm can resist statistical attack, birthday attack and meet-in-the-middle attack and satisfy all performance requirement of Hash function in an efficient and flexible manner. It is practicable and reliable, with high potential to be adopted for E-commerce.

Normalization towards Instruction Substitution Metamorphism Based on Standard Instruction Set
Ran Jin , Qiang Wei, Pei Yang and Qingxian Wang
Institute of Information Engineering
University of Information Engineering
Zhengzhou, 450002, China
{jinran17, funnywei, aberlan, ranosk}@163.com

Abstract
Metamorphic malware is able to change its signature which is a fixed sequence of bytes or code from generation to generation. This makes the traditional scanner based on the signature difficult to detect it. Combing normalization with traditional scanner is a promising direction to solve the problem. The idea is: firstly transform the code into canonical form then pass it into scanner to check. This paper proposes a novel normalization method towards instruction substitution which is a commonly used metamorphism approach. The method mainly involves two steps. Firstly, the input code is rewritten with standard instructions. Secondly, the order of standard instructions is adjusted based on the data dependence graph of each basic block. A case study of normalizing Win32.Evol has been carried out. The results demonstrate the feasibility of our method to make variants, including the original code, tend to be uniform.

Design Principles for Public key Cryptography System Protected with Power Analysis
Xu Rui
School of Aerospace Science and Engineering
Beijing Institute of Technology (BIT)
xurui@bit.edu.cn Jiang Huiping
School of Computer Science and Technology
Abstract
Side channel information could be used to analysis the key information according to leakage information depending on the operation of cryptography algorithm and its hardware. And power analysis is the chief method. In this paper, an improved architecture for RSA system against power analysis was proposed based on its basic theory. A DPA attack for RSA specially, is discussed in details, and the shadow technology was proposed based on it. In order to maximize the capability/cost, Shadow technique and removing intermediate value technique are introduced into RSA system, which only cost more than 30% timing to realizing secure RSA algorithm. Contemporary the effectiveness of advanced RSA cryptography system was illuminate briefly.

Cryptanalysis and Improvement of a Constant-size Identity Based Ring Signature Scheme
Huaqun Wang School of Information Engineering Dalian Fisheries University whq@dlfu.edu.cn
Xianju Guo School of Information Engineering Dalian Fisheries University gxj@dlfu.edu.cn
Abstract
Ring signature is of vital importance to secure electronic voting. Many ID-based ring signature schemes have been put forward, but most of them are not constant-size. Au etc proposed a constant-size ID-based ring signature without random oracles. The size of the signature is independent of the size of the ring. In stronger security model, the constant-size ID-based ring signature scheme can be forged. A forged method was presented in this paper. In order to resist this attack, we improve the original ring signature scheme. The improved scheme is secure even in the stronger security model.

An Efficient Group Signature Scheme Without Random Oracles
Wang Shaohui Wang Meiqin
Key Laboratory of Cryptologic Technology and Information Security Ministry of Education, Shandong University Jinan 250100, China wangshaohui@mail.sdu.edu.cn
Abstract
In this paper, we give an efficient short constant-size group signature scheme that is secure in standard model based on Strong Diffie-Hellman Assumpiton. We achieve this result by combining a variant signature scheme of the one presented by Okamoto and Non-Interactive Zero Knowledge proof used by Boyen and Waters. Compared with the most efficient group signature scheme without random oracle, our scheme has a much shorter public key length and signature length, and needs less computation.

A Novel Hybrid Encryption Scheme against Adaptive Chosen Ciphertext
Attack
Zhifeng Qi, Sihan Qing, Yixian Yang, Guanghui Cheng
Information Security Center, State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, 100876, China

Abstract
Many efficient CCA2-Secure hybrid encryption schemes have been proposed, but their securities are based on too strong assumptions. It would be preferable to base a security proof on a weaker assumption, so we describe a practical hybrid encryption scheme based on the weaker LDDH assumption, and in the standard model prove to be CCA2-Secure if the LDDH assumption is true.

Multi-secret Sharing Threshold Visual Cryptography Scheme
Bin Yu, Xiaohui Xu, Liguo Fang
Institute of Electronic Technology, the PLA Information Engineering University, P. R. China
Binyu2001@21cn.com

Abstract
Original VCS can only share a secret image at a time. When we want to share more secret images, we need to preserve a number of shares which increase our burden. Based on \((k, n)\)-VCS and \((k-1, k-1)\)-VCS, we propose a multi-secret sharing threshold VCS that a participant only preserves a share to share more than one secret and expands the scope of application.

Restricted-Verifier Precise Bounded-Concurrent Zero-Knowledge
Ning Ding, Dawu Gu
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, 200240, China
{dingning, dwgu}@sjtu.edu.cn

Abstract
We present a stronger notion of precise bounded-concurrent zero-knowledge. Our notion captures the idea that view of any verifier in a bounded-concurrent interaction can be reconstructed in the almost same time. Precise zero-knowledge in stand-alone setting was introduced by Micali and Pass in STOC’06 and they constructed some precise stand-alone zero-knowledge protocols for NP using at least \(\omega(1)\) rounds. Via providing a precise simulator for the known \(O(1)\)-round bounded-concurrent non-black-box zero-knowledge argument, we show the existence of \(O(1)\)-round bounded-concurrent zero-knowledge arguments with polynomial precision for NP. Our result assumes that the ratio of running-time of any adversarial verifier on any two different views in bounded-concurrent execution of the protocol is bounded by \(na\), where \(a\) is any predeterminate constant. Such verifiers are called restricted verifiers.

An Improved Quick Algorithm for Aligning DNA/RNA Sequences
Quan Zou, Maozu Guo, Yang Liu, Taotao Zhang
School of Computer Science and Technology, 
Harbin Institute of Technology, 
Harbin 150001, PRC 
{guoer713108@163.com, maozuguo@hit.edu.cn, yliu@jdl.ac.cn, ztt317@126.com}

Abstract 
Biology sequence database search is an important problem for bioinformatics research. The main search software BLAST is based on the BYP algorithm[1]. In BYP, if the length of hit region is set long, it may lose similar appearance. Otherwise, there may be too many r-length regions from Aho-Corasik algorithm. Checking where exists any approximate alignments for the DNA or RNA sequence always spends much time, although the expected running time of BYP is linear. A new algorithm is proposed from the viewpoint of shorting the length and increasing the number of the regions, which can make most of the false r-length regions excluded. Thus the algorithm can align the DNA or RNA sequences quickly since the rate of real r-length regions is increased. Experimental results show that the proposed algorithm is computational efficient and achieves good performance.

Traffic forecasting based on chaos analysis in GSM communication network 
Xianhua Hu 
Electric Power College, South China University of Technology, Guangzhou 
Guangdong, China, 510640 
1392220077@139.com 
Jie Wu 
Electric Power College, South China University of Technology, Guangzhou 
Guangdong, China, 510640 
epjiewu@scut.edu.cn

Abstract 
In this paper, some chaotic characteristics of the traffic time series in the GSM network are studied. Following a low-pass filtering, the traffic time series is reconstructed as a phase trajectory by properly choosing some parameters. Through the reconstructed trajectory and corresponding data analysis, it can be found that the traffic time series in the GSM network reveals some chaotic characteristics. Experimental results show the chaotic characteristics are obvious for short term. Moreover, the results supply some hints for the prediction algorithm design and data selection.

Platform Technology of Web Services-Oriented DCS Data Exchanging 
Qibing JIN 
College of Information 
Beijing University of Chemical Technology 
15 BeiSanhuan East Road, Beijing 
jinqb@mail.buct.edu.cn 
Weilong SHAO 
College of Information
Abstract
To solve the problem of information interdiction among various kinds of DCS and systems of MIS and ERP, through using a kind of universal Web Services object’s encapsulation technique, a Web Services oriented DCS data exchanging platform is constructed, and the functional architecture and Key Enabling Technologies of the platform are introduced in detail. Accordingly, the enterprise information integration across different platforms and languages is realized, and an open, unified application integration environment is provided for the heterogeneous control systems and management systems.

Deployment and Application of ERP Service on Grid
Gao Zhongwen
College of Automation, Harbin Univ. Sci. Tech., Harbin 150080, China
xinyun0920@163.com
Duan Ruizhen
College of Automation, Harbin Univ. Sci. Tech., Harbin 150080, China
d_zhen_05@126.com

Abstract
This paper presents an implemental plan to deploy and apply ERP on Vega GOS platform, in which the stability of Vega GOS is guaranteed by dint of the Linux better security. The ERP application can be transplanted into Grid environment by compiling service program and sealing, and then it is realized that the ERP service registered to grid router is transferred by compiling program for client terminal. Additionally, the grid resources are real-time monitored and rationally dispatched by the performance evaluation module in Vega GOS. Finally, the superiority of this application is analyzed over traditional way, including interoperability, expandability, Sharing and the cooperation, High effect, Secure and the reliability and so on.

Model-based Fault Diagnosis for the Spacecraft Power System
Shao Jiye Wang Rixin Xu Minqiang Gao Jingbo
Harbin Institute of Technology, Harbin, China
Shaojiye@hit.edu.cn Wangrx@hit.edu.cn Xumq@hit.edu.cn Gaojb@hit.edu.cn

Abstract
Model-based diagnosis has a great advantage compared to other diagnostic methods. This paper develops a fault diagnosis system for the power system of spacecraft using model-based consistent diagnostic theory. Designing the nominal and faulty modes of each component, the qualitative model of the power system is built in a component-based manner using JMPL language. The fault diagnostic engine is constructed using conflict-A* algorithm. Experiments on the spacecraft power system verify that the model of the power system is correct and the diagnosis system developed is very effectively.

A Method of Radar Signal Separation
Feng Youqian1 Zhang Shanwen2 Li Zhengchao3
1. Air Force Engineering University, Xi’an, P. R. China, 710051
Abstract

Radar signal separation is an important link in the chain of information processing for air-defense, which is the process of extracting unknown independent radar signals from unknown sensor measurements. Sometimes, the source signals and the method of combination are unknown, and hence the problem is related to the problems of blind deconvolution and blind equalization. Blind signal separation is sometimes referred to as independent component analysis, as it generalizes principal component analysis to produce independent signals rather than simply uncorrelated signals. Based on the frequency localization of Morlet wavelet and genetic algorithm, this paper presents a method of radar signal separation. Some examples are given. The results of separation demonstrated this method is effective and low sensitivity to noise.

Keywords: Morlet wavelet, Radar signal separation, Genetic Algorithm

Grey SVM with Simulated Annealing Algorithms in Patent Application Filings Forecasting

Abstract

The patent applications filings (PAF) are complex to conduct due to its nonlinearity of influenced factors. In this study, a grey support vector machines with simulated annealing algorithms (GSVMS) is proposed to forecast PAF. In addition, GM (1, N) model of grey system is used to add a grey layer before neural input layer and white layer after SVM layer. Simulated annealing algorithms (SA) are used to determine free parameters of support vector machines. Evaluation method has been used for comparing the performance of forecasting techniques. The experiments show that the GSVMS model is outperformed GM (1, N) model and SVM with simulated annealing algorithms (SVMS) model, and PAF forecasting based on GSVMS is of validity and feasibility.

A Novel RED Scheme with Preferential Dynamic Threshold Deployment

Lijun Sun
Institute of Complexity Science, Qingdao University, Qingdao 266071, China
msxkhv@hotmail.com

Lihong Wang
Department of Computer Science & Technology, Yantai University, Yantai 264005, China
wanglh@ytu.edu.cn

Abstract

Congestion control mechanisms in Internet have attracted more attention in network studies. To the high loss rate and synchronization resulted from Drop Tail policy, Random Early Detection (RED) and its variations were reported. In this paper, a novel algorithm named Preferential Dynamic Threshold – RED (PDT-RED) and its optimized scheme OPDTRED are proposed. They can adjust dynamically average queue length thresholds basing on packets’ priority and unused buffer space, and accordingly realizes differentiated service. Compared with RED, OPDT-RED algorithm has three features: 1) it reduces greatly the loss rate of packets with higher priority and the average loss rate of all packets; 2) it is simple for
New Temporal Error Concealment Method for H.264 Based on Motion Strength
Congdao Han
Dept. of Information Science and Electronic Engineering,
Zhejiang University, Hangzhou, China hancongdao@163.com
Jilin Liu
Dept. of Information Science and Electronic Engineering,
Zhejiang University, Hangzhou, China liuji@zju.edu.cn

Abstract
In this paper, an effective error concealment algorithm for H.264-coded video is proposed. Firstly, motion vector relative strength of neighboring macroblocks (MVRS) is obtained by calculating a ratio involving the motion vectors of adjacent macroblocks. Then, according to the magnitude of MVRS, the way of generating the motion vector of the lost macroblock is determined. Finally, each lost macroblock is concealed on the basis of the selected algorithm. Satisfying simulation results are achieved, which illustrate the proposed method yields better performance than the methods in literatures for most video sequences.

Suppliers' Innovative Capabilities and Their Relationship with Customers:
An Evidence from Packaging Machinery Industry in China
He Mao
School of Management & Economics, Kunming University of Science and Technology, Kunming, 650093, P.R.China ynhemao@yahoo.com.cn

Abstract
In order to compete successfully in the marketplace, suppliers have to develop certain innovative capabilities that, in turn, depend on the type of relationship that is established with customers. Based on a study of 197 suppliers operating in the packaging machinery industry in China, structural equation modeling and multiple hierarchical regression are used to reveal the relationship between suppliers’ innovation capability and their different roles in the supply chain. The research findings lend support to the hypothesis that the level of investment in technology and the acquisition of specific managerial capabilities are to a large extent, a determinant of supplier–customer interdependence.

Stereoscopic Video Coding Based on H.264 Standard
Shigang Wang
College of Communication Engineering of Jilin University, P.R.China, 130012 wangshigang@vip.sina.com
Xuejun Wang
College of Communication Engineering of

Abstract
H.264 is an advanced video compression standard, absorbing the advantages of the previous standard. In this paper, block-based stereoscopic video coding is presented. The main view of the sequences is encoded
as a H.264 bitstream and the auxiliary views are encoded by joint motion and disparity compensation, so that both temporal and spatial redundancy are reduced and high compression is achieved. Investigating the effectiveness of the joint motion and disparity vectors estimation as well as the employing of the H.264 encoder optimizes the whole framework.

**Research on Supplier Selection Tactic Model and Algorithm of Special Steel Enterprise for Strategic purchasing**

Liu Xiaobing  
Dalian University of Technology  
CIMS Center  
Dalian, Liaoning, 116024 China  
xbliu@dlut.edu.cn  
Lv Qiang  
Dalian University of Technology  
CIMS Center  
Dalian, Liaoning, 116024 China  
Lvq1970@163.com

**Abstract**  
By the analyzing and study on the problem about JIT procurement and supplier selection of Special Steel enterprise group, a supplier selection tactic model structure of enterprise group was firstly constructed. The constructing process of the model is basically based on the procurement cost and the delivery time. On the basis of adaptive genetic algorithm, an original algorithm for multi-constraint supplier selection tactic mathematical model was then proposed. The procurement cost and the delivery time was chose as the optimization objective in the proposed mathematical mode. The model and the algorithm is applied to solve a given practical problem of Special Steel enterprise group, the validity and efficiency of the model and the algorithm is then verified by the solving results. Finally some lacking place of the multi-constraint supplier selection tactic mathematical model was discussed.

**Speech Quality of IEEE 802.11b and 802.11g Wireless LANs**

Yuanfeng Liu  
School of Electronic and Information Engineering, South China University of Technology, Guangzhou, 510641, China  
Lyf16@163.com  
Minghui Du  
School of Electronic and Information Engineering, South China University of Technology, Guangzhou, 510641, China  
Ecmhdu@scut.edu.cn

**Abstract**  
As 802.11g devices develop, it is possible for WLANs to support heavy voice communications. In this paper, an improved evaluation model which presents more detail on voice communications is introduced. The best and acceptable speech quality speech quality of 802.11b and 802.11g WLANs are obtained and compared to the theoretical results. The effect of playout algorithms are compared which come to conclusion that the playout algorithms play a more important role as the network condition getting worse.
Sparseness Points Cloud Data Surface Reconstruction based on Radial Basis Function Neural Network (RBFNN) and Simulated Annealing Arithmetic *
Xue-mei Wu 1, Gui-xian Li 1
1. School of Mechanical and Electrical Engineering Harbin Institute of Technology Harbin, Heilongjiang Province, 150001 China wxm@hit.edu.cn
Wei-min Zhao 2
2. Department of Mechanical Engineering Daqing Petroleum University Daqing, Heilongjiang Province, 163318 China biyelunwen_2005 @126.com

Abstract
A novel neural network arithmetic was employed in sparseness points cloud data surface interpolation and reconstruction. Radial basis function neural network and simulated annealing arithmetic was combined. The new arithmetic can approach any nonlinear function by arbitrary precision, and also keep the network from getting into local minimum. Global optimization feature of simulated annealing was employed to adjust the network weights. MATLAB program was compiled, experiments on sparseness points cloud data have been done employing this arithmetic, the result shows that this arithmetic can efficiently approach the surface with 10^-4 mm error precision, and also the learning speed is quick and reconstruction surface is smooth. Different methods have been employed to do surface reconstruction in comparison, the sum squared error is 6.7×10^-8 mm employing the algorithmic proposed in the paper, the one is 1.34×10^-6 mm with same parameters employing radial basis function neural network. Backpropagation learning algorithm network does not converge until 3500 iterative procedure.

Automatic Generating Test Cases for Testing Web Applications*
Shengbo Chen, Huaikou Miao, Zhongsheng Qian
School of Computer Engineering and Science, Shanghai University, Shanghai 200072, China
csb_hust@163.com, hkmiao@shu.edu.cn, changesme@163.com

Abstract
In order to ensure the security and reliability of Web application, the testing of Web application is one of the most effective methods. This work regards a Web application as the composition of different interactive Logical Components (LCs). We combine LCs with agent to assist to automatic generate test cases for testing Web applications. From Pages-Flow-Diagram (PFD) of Web application under test, this research successively partitions Web applications into LCs, at different levels of abstraction, each of which is composed of Web pages and other LCs. We use an automaton to model each LC, and use compositions of automata
to model interaction of LCs. Our approach supports concurrent access and interaction between LCs. It avoids the state space explosion problem effectively. It also enhances the reuse of component interactions and overcomes differences in actions between LCs by using an agent as a coordinator.

Tool Wear Monitoring and Failure Prediction Based on Hybrid SOM-DHMM Architecture

Abstract
A method of pattern recognition of tool wear based on Discrete Hidden Markov Models (DHMM) is proposed to monitor tool wear and to predict tool failure. At the first FFT features are extracted from the vibration signal and cutting force in cutting process, then FFT vectors are presorted and coded into code book of integer numbers by SOM, and these code books are introduced to DHMM for machine learning to build up 3-HMMs for different tool wear stage. And then, pattern of HMM is recognised by using maximum probability. Finally the results of tool wear recognition and failure prediction experiments are presented and show that the method proposed is effective. Index Terms- Discrete Hidden Markov Model (DHMM); Tool wear; Pattern Recognition; Prediction; Self-Organizing Feature Map(SOM).

Research on Mission Hot-Swapping and Dynamic Replacement Mechanism of Mission Component
YE Haizhi College of Computer Science and Technology, Harbin Engineering University yhz87@163.com
WANG Huiqiang College of Computer Science and Technology, Harbin Engineering University Whqiang@163.com
LIANG Ying
College of Computer Science and Technology, Harbin Engineering University liang223@126.com

Abstract
It’s urgently necessary for many mission-critical systems with high availability to implement online updating, fault recovery and environmental adaptability of software. Therefore, the idea of mission hot-swapping is proposed, in which, related problems and key technologies of mission component’s dynamic replacement is analyzed. A dynamic replacement mechanism of mission component based on interceptor and component container is put forward. The research results show that the dynamic replacement of mission component is feasible and the idea of mission hotswapping is correct.

The Post-processing for Mathematical Expressions Oriented on Integrative Rectification
Wen-jiao Wang1, Lei Han2, Tian-yu Chen3, Xue-dong Tian1
1Faculty of Mathematics and Computer, Hebei University, Baoding, Hebei, China
2Hebei Provincial Meteorological Technology Equipment Center, Shijiazhuang, Hebei, China
3Zhongshan People’s Hospital, Zhongshan, Guangdong, China
E-mail: wwjwwj1113@163.com

Abstract
At present, inaccurate results still exist in the output of the printed mathematical expressions recognition
system. After the results were analyzed, one kind of method was introduced which unified the printed mathematical formula structure analysis and semantics knowledge. Suitable post-processing for recognition result based on integrative rectification was carried on. Thus printed mathematical formula recognition system gets consummate. The experiment indicates that this method may enhance the accuracy of the system effectively.

A Metadata Configuration Model for Component-based Software Integration Testing
Guo Fuliang Department of Computer Engineering, Naval University of Engineering, Wuhan, Hubei, China, 430033
Ma Liangli Department of Computer Engineering, Naval University of Engineering, Wuhan, Hubei, China, 430033

Abstract
Component-based software develop has become the main develop method. Meanwhile how to assure its quality is an important research content, including component-based software integration testing. This paper introduces a metadata configuration model describing interior information of component to increase testability. The metadata configuration model (MCM) includes three parts: basic attributes, additive attributes and integrated attributes. And a general framework of the model is further given, which is consisted of several classes. Each class includes several attributes, and their meanings are described. Finally the case study based on previous model is done, and the corresponding results are given. All these show effectively that the models we presented are valid and helpful for component-based software integration testing.

A Novel Data Acquisition Algorithm for the Reverse Analysis of Encrypted Synchronous PLDs
Qing-bao Li Ping Zhang Rong-cai Zhao
Zhengzhou institute of Information Science and Technique, Zhengzhou, Henan, CHINA, 450002

Abstract
The key problem in the reverse analysis of encrypted programmable logic devices (PLDs) using logic analysis techniques is how to acquire effective and self-contained data set, especially for sequential PLDs. An efficient data acquisition algorithm is presented which suits for large scale and multi-state synchronous PLDs. The algorithm builds non-complete state graph and finds the shortest path for state migration from initial state to each active state. The algorithm has ideal time and space cost and has been used in our PLD reverse analysis system.
Online Measurement of Transformer Partial Discharge

Wang Baobao
Network security and computing institute of Xidian university
South taibai road NO.2, Xi’an, Shaanxi province, China
bbwang@xidian.edu.cn
Yang Yang
College of computer science, Xidian university
South taibai road NO.2, Xi’an, Shaanxi province, China
yyyang911@163.com

Abstract
In ultrasonic locating of transformer partial discharge (PD), the key technologies are time-delay (TD) estimation and PD point calculating, which directly determine the correctness and the precision of the results. The TD correlation algorithm has traits of convenient implementation and high precision. Based on the TD estimation, the hybrid unconstrained optimum method for solving the PD point locating equations realizes the specialties of fast iterative speed, wide convergence field and stable outcomes. Satisfying results are received while the algorithms are applied in the transformer PD point online detecting system.

Keywords: partial discharge, time-delay estimation, ultrasonic locating, the steepest method, newton method.

The Research of Broken Filaments Detection Device on Viscose Filament yarn
Li De Jun
College of Electronics Information Engineering of Wuhan university and engineering
ldj@wuse.edu.cn

Abstract
In this paper, on the basis of researching several methods for broken filaments detecting in-depth, we have designed a real-time broken filaments detection device in the process of viscose filament yarn winding.

The detection device is used for detecting broken filaments by illuminating broken filaments on viscose filament yarn. The broken filaments will become an enlargement image on the sensitive surface of the photoelectric sensor. The image will cause luminous flux of photoelectric cell to weaken, by monitoring the signal, and the system can detect and count the broken filaments. The accuracy of the viscose filament measurement system is reliable and low cost.

Keywords: viscose filament yarn; broken filaments; detection device; photoelectric sensor;

Research on an Overprinting Accuracy Analysis Algorithm without Color Marks of Multi-color Printings
Jun Gao1,2 Bing-heng Lu
1. School of Mechanical Engineering School of Mechanical Engineering
Xi’an Jiaotong University Xi’an Jiaotong University
Xi’an, 710049, P. R. China Xi’an, 710049, P. R. China
2. School of Mechanical Engineering
Shandong University of Technology
Zibo, 255091, P. R. China
gaojun71@sina.com
Abstract
A new algorithm of overprinting accuracy analysis of multi-color printings with no color marks required is presented in the paper by applying image processing technology and color separation technology to quality inspection of multi-color printings. Firstly the standard image and the images collected from printings waiting for inspection are color-separated, consequently they are registered; then the image registration data can be gotten; finally overprinting error can be obtained by applying the inherent information embodied in inspected images and image registration data. Obviously other than traditional overprinting error analysis methods, with the new algorithm no color marks are necessary to print on the margin of printing media. So printing media can be saved and additional operations such as cutting color marks out can be left out. The experiment shows that accuracy and efficiency of overprinting inspection can completely satisfy the requirement of precise printings with little additional calculation or measurement required.

Platoon Dispersion Prediction Under the Condition of Adjacent Cycle Traffic Flow Overlapping Based on Support Vector Regression
This work was supported by National Natural Science Foundation of China(Grant No. 70701006), National Basic Research Program of China (Grant No.2006CB705500), Talent Recruitment Foundation of Changsha University of Science and Technology (Grant No.1004140)
Lu Shoufeng
Changsha University of Science & Technology
Traffic and Transportation College
Changsha, Hunan, China
itslu@126.com

Liu Ximin
Changsha University of Science & Technology
Traffic and Transportation College
Changsha, Hunan, China
liuximin1980@163.com

Abstract
Coordinated signal control can improve the continuity of vehicular traffic flow movement and reduce delay. Cycle Flow Profile is the base for calculating coordinated signal control parameters. Platoon dispersion characteristic determines the Cycle Flow Profile. So, improving platoon dispersion prediction accuracy can obtain significant benefit for signal coordination. When the velocities of the vehicles vary greatly, faster vehicles of next cycle can catch up the slower vehicles of the current cycle. Traffic flow overlapping of adjacent cycle is an important characteristic. The paper adopts Support Vector Regression to predict platoon dispersion and compares prediction accuracy with Robertson formula. The results are encouraging, support vector regression has higher prediction accuracy.

Building Optimal Bidding Strategies for Generation Companies in Electricity Market
Abstract
In a competitive electricity market with sealed auction, building the optimal bidding strategies for generation companies (Gencos) could be based on many uncertain information including rival’s bidding behaviors, forecasted load and other market parameters. All the uncertain parameters to be considered in the procedure of bidding strategies have the random and fuzzy character. As a result, two main approaches to build optimal bidding strategies for Gencos were based on probability theory and possibility theory. However, as a limit of mathematical theory, there could not simultaneously deal with both random variable and fuzzy variable in a model developed in the past work. Based on credibility theory that was recently founded, a new framework of random-fuzzy programming was proposed for building optimal bidding strategies with risk management in this paper, and a hybrid intelligent algorithm by integrating simulation, artificial neural network and genetic algorithm were presented to find optimal bidding strategies. A numerical example of a simulated electricity market with six participating Gencos is served to demonstrate the feasibility of the developed model and solution method.

Research of Campus Grid Construction

Xia Zhang1, 2
1 Department of Information Technology, Central China Normal University, Wuhan, Hubei, China
2 Physics and Information Science Department, Yulin Normal College, Yulin, Guangxi, China
49749769@qq.com

Abstract
The extensive distribution and heterogeneity of distance education resources causes great difficulty to share them, forms numerous isolated information islands. The appearance of grid technology provides an excellent opportunity to solve the problem, who aims to integrate, virtualize, and manage resources and services within distributed, heterogeneous, dynamic “virtual organizations”[1], so as to eliminate isolated information islands, therefore, grid technology has a vast prospect of development and application in campus grid construction and distance education field. This paper first analyzes problems that distance education is now facing, and then gives a brief introduction to grid and OGSA, in the end designs a general structural framework of campus network according to OGSA's philosophy of eliminating isolated information islands with grid service.

Appraisal Research of the Government Achievements
Based on Electronic Government Affairs Angle

Xia Bin Pan Bin
Northwestern Polytechnical University
Faculty of Business Administration, Xi’an University of Technology, P.R.China , 710054
E—mail: xb611@sohu.com

Abstract:
This paper through analysis to research condition of the electron government affairs of the information society, has proven the feasibility and the necessity of the government achievements appraisal based on the
Study on Wuhan Railway Transit Project Information System
Zhou Ying, Ding Lie-yun, Zeng Guang
School of Civil Engineering & Mechanics, Huazhong University of Science & Technology., Wuhan, Hubei, China.
Hubei Key Laboratory of Control Structure, Huazhong University of Science & Technology., Wuhan, Hubei, China.
hello_grace@163.com

Abstract
With the continuous development of the construction management, traditional manners can not satisfy the project managers’ requirement. This article applies information technology in construction to enhance the management efficiency. Based on the practice of Wuhan railway transit project, the system design goals, system structure and functionality are explained. Also, it gives the suggestions of improving the system.

Application of Three-Dimensional Visualization in Landscape Planning
Chen Shenghao
School of Art & Design, Wuhan University of Technology, Wuhan, China
E-mail: Sammychen1201@sina.com

Abstract
This paper presents the findings of an investigation into the role and use of landscape visualization software, for landscape and environmental planning. It examines the challenges and requirements of 3D visualization technology and its potential for application in landscape and environmental planning. Relevant literature and comparable surveys are reviewed in order to determine the current state of affairs, and the general and international relevance of the results is assessed.

Network Forensic Computing Based on ANN-PCA
This paper is supported by the 863 important project, China (Grant Number 2006AA12A106), and the Academic Natural Science Research Project of Education Department of Jiangsu Province, China (Grant Number 06KJD520019)
Youdong Zhang, Yongjun Ren
2 Department of Computer Engineering
Huaiyin Institute of Technology Jiangsu Huaiian 223001, China
z.yd@163.com Jiangdong Wang, Liming Fang
1 College of Information Science and Technology Nanjing University of Aeronautics and Astronautics Jiangsu Nan Jing 210016, China

Abstract
The network forensic computing is faced with the question of the massive information stream analyses. Two solutions including feature extracting and classification mining were proposed. The main work includes features extracting with ANN-PCA, classification mining after features extracting in FAAR algorithm which we proposed to mine association rules based on PCA and Fuzzy classification technology. The experiment indicates that the classification accuracy raise distinctly after feature extracting, and the feature quantity decrease especially U2R attack. Further more, the number of generating rules also reduces clearly.
Time Bounding Event Reasoning in Computer Forensic
Liu Zhi jun Wuhan University Computer School
Hubei Police University Department of Information Technology
86 Jiefang Road, Wuhan, China
Zhang Huan guo Wuhan University Computer School Luojia Hill, Wuhan, China
Liss@whu.edu.cn seraphtear@163.com

widely used in computing and offer an easy way to determine the time of events in digital investigations. Unfortunately, the ability of users to change clock settings, the difficult to recover the multi-level overwriting data in a disk, etc. can not provide the efficient timestamp for event reasoning. In this paper, we present techniques to use lay technique to deal with the time of a file on local machine, even its data block of a file had been re-written many times or deleted long ago, and adopt the time offset mechanism to deal with the deviation time of the file at time t. Use a logging mechanism to record the time of modifications to each disk block and its deviation time at time t to calculate the real time of a file for reasoning the order of the events and obtaining a timeline of activities on a file.

Competitive Stock Replenishment Problem in a Two-echelon Supply Chain with Competing Retailers
Qing Liu
Research Institute of Automation East China University of Science and Technology, Shanghai 200237
Dao Huang
Research Institute of Automation East China University of Science and Technology, Shanghai 200237
He Liu Research Institute of Automation East China University of Science and Technology, Shanghai 200237
Yu Tian
Research Institute of East China University of Science and Technology, Shanghai 200237

Abstract
This paper studies a two-echelon supply chain, with a warehouse and n retailers. The entire supply chain is characterized by several parameters including demand variance, inventory holding cost and backorder penalty cost. We investigate replenishment strategies of this system under decentralized and centralized control. We consider horizontal information sharing between these retailers when the shared information is valuable for stabilization of the system. It is shown that unique Nash equilibrium of the competitive retailers system exists. We also propose demand-dependent and equational coordination schemes. These three coordination schemes are compared numerically; the result of the simulation show that penalty cost and holding cost effect replenishment in Nash equilibrium greatly, and although the set of strategies under profit oriented Nash equilibrium balance the supply chain system, it increases system cost.

Research on the Problem of Contact Characteristic Finite Strip and its Characteristic Agent
Guo-chang Li De-bin Zhang Chun-e Zhang Cai Liu
Abstract
The deformation mechanism of cold-formed steel is very complex, the relation between the deforming forces exerted and the deformation of steel strap can not be described by simple function. In order to reduce data redundancy, adopt the characteristic finite strip method which can solve primary illogicality. The characteristic finite strip can be divided into 3 kinds, thereinto, “the characteristic finite strip contacted with roller” can parse the effect roller energy to steel strap deform and the influence steel strap and roller friction to deformation. So, research on this kind of finite strip looks very important. Making this kind of characteristic of finite strip has informatization and intelligentize have instructed effect to the intelligence of pass design. Adopt characteristic Agent is the relative good method of making the characteristic finite strip has intelligence.

Emotional Agent Based on Rough Set
Jun Hu Yu-hai Chen Chun Guan
Institute of software Dep. of Computer Science Dep. of Computer Science
Nanchang University Nanchang University Nanchang University
Nanchang 330047, China Nanchang 330047, China Nanchang 330047, China
hujun@ncu.edu.cn guanchun@ncu.edu.cn

Abstract
To improve the ability of agent for handling emotions, a new architecture for emotion agent is presented, based on the traditional BDI agent model and the rough set theory. By a new emotional reasoning algorithm based on rough set, the architecture performs emotion reasoning and implements the emotion treatment. An emotional agent grid based on this architecture has been realized, experiment results show that it is efficient to transact simple emotions by emotional agents.

Constructing Adaptive Individual Learning Environment Based on Multi-agent System
Peng Chen
College of Electrical Engineering & Information Technology, China Three Gorges University, 443002 Yichang, Hubei, China
E-mail: niumanlov@126.com Anbo Meng Faculty of Automation, Guangdong University of Technology, 510090 Guangzhou, China
E-mail: febirdhust@163.com
Abstract
A multi-agent system (MAS) based integrate framework in support of adaptive and active learning in individual learning spaces is proposed in this paper. In the adaptive individual learning space, the key issue is how to dynamically generate personalized learning path consisting of domain concepts and present associated learning objects catering for a learner’s knowledge state and learning preference. As to this, a novel domain model with ontology layer, metadata layer and learning objects layer is proposed, and an efficient searching algorithm for the presentation generation base on the proposed domain ontology model is put forward.

Agent-based Distributed Conceptual Design of Virtual Prototyping for Complex Products
Chen Xi
Management School, Nanjing University
doctor_chan@163.com

Abstract
Integrating and sharing multidisciplinary model data and improving robusticity and validity of product conceptual design system in distributed environment is one of the key technical problems in Virtual Prototype design and simulation of complex products. After long time research on multi-agent systems, an agent-based product conceptual design system combining XML and Web Service technology was proposed, system architecture, communication style and system workflow were illustrated. Further more it discussed product conceptual design development process, decision arithmetic and gave a unified intelligent agent group form for electronic, software and control systems involved in virtual prototyping product conceptual design, realized a service-oriented, supporting distributed, heterogeneous and multi-field collaborative product conceptual design supporting platform.

Research on Multi-Agents Systems Model for E-commerce under Distributed and Heterogeneous Environments
Meng Hao School of Information and Computer Anhui Agricultural University Hefei Anhui P.R.China 230036 Mh2005@ahau.edu.cn
Gu Lichuan School of Information and Computer Anhui Agricultural University Hefei Anhui P.R.China 230036 Gulichuan@ahau.edu.cn

Abstract
Commercial activities have been distributed all over the world. To query and access the commercial databases under this distributed and heterogeneous environment becomes very important. Combined the advantages of XML with CORBA technology, a model for e-commerce under this environment is proposed. With the well designed fuzzy neural network in information mining, a corresponding example is presented and proved primarily feasibility and validity.
Key words—Multi-agent System, Communication, Interaction, XML
Association Rules Mining of Traditional Chinese Medical Syndrome Differentiation Oriented
Shen Xiaoyan
Information Center Shenyang Medical College
Shenyang, 110034, P.R.China
Qian Xiaotang School of Information Science and Engineering, Northeastern University
Shenyang, 110004, P. R. China

Abstract
The paper expounds the association rules mining procedure on Traditional Chinese Medical Syndrome Differentiation (TCMSD), comes down to a method - Apriori algorithm which creates the frequent item sets. In the process of creating the frequent item sets, the efficiency of execution becomes lower rapidly as dimensions increasing, so DFP-growth algorithm is provided on the FP-growth algorithm. DFP-growth has the same structure as FP-tree, and makes use of a top-down increment strategy to obtain the frequent item sets.

Research on Multi-Mode Fusion Tracking of OTHR based on Auction Algorithm
Kong Min
Research Institute of Information Fusion, Naval Aeronautic Engineering Institute, Yantai, China.
kongmin2000@sohu.com
Wang Guohong
Research Institute of Information Fusion, Naval Aeronautic Engineering Institute, Yantai, China.
wangguohong@vip.sina.com

Abstract
In OTHR's tracking system, we will estimate the state of a discrete-time, linear stochastic system whose observation process consists of a finite set of known, non-linear measurement models. MPDA is capable of exploiting multipath target signatures arising from discrete propagation modes that are resolvable by the radar, but it is very time-consuming and will bring multipath tracks. In this paper, a Multi-Mode Fusion Tracking of OTHR based on Auction algorithm (A-MFT) is proposed, which effectively solve the problem of multi-mode measurements. When tracking a single and non-maneuvering target with four possible measurements, simulations in clutter environment show that the computing speed of the algorithm proposed in this paper is greatly higher than that of MPDA, and the tracking precision just a little lower than that of MPDA, further more, A-MFT will not bring multipath tracks and do not need consequent track association.

An Improved Information Fusion Algorithm Based on SVM
Jun Ma Harbin Engineering University
College of Computer Science and Technology Harbin, 150001, China majun@hrbeu.edu.cn
Jianpei Zhang Harbin Engineering University
College of Computer Science and Technology Harbin, 150001, China zhangjianpei@hrbeu.edu.cn
Jing Yang
Abstract
The support vector machine (SVM) is an algorithm based on structure risk minimizing principle and has high generalization ability. The model offers a kind of effective way for the information fusion problem of little sample, non-linear and high dimension. In this paper, mobile agent is applied to information fusion system. The model of OODA and the study method of information fusion system are improved. The model and an algorithm of information fusion based on the support vector machine are proposed. The experiment results show that this hierarchical and parallel SVM training algorithm is efficient to deal with large-scale classification problems and has more satisfying accuracy in classification precision.

Forecasting Method on Pear Scab Based on Fusion Reasoning
Gu Lichuan1, 2; Ni Zhiwei 1; Li Shaowen2; Zhang Youhua2
1. School of Management HeFei University of technology HeFei Anhui, P.R.China 230009
2 School of Computer Anhui Agricultural University

Abstract
At present, the Forecasting methods on fruit diseases have the problems of inefficient reasoning and poor effects of forecasting. In this paper, a integrated reasoning method based on CBR and RBR is studied. A fusion reasoning frame based on CBR and RBR is put forward, a forecasting system on pear scab is designed and developed based on the frame as well. Statistical analysis is conducted between the real data and the forecasting data of Dangshansu pear scab, which shows the new method is better than the current methods in efficiency and precision for forecasting the occurrence tendency of Dangshansu pear scab.

Association Rules Mining Using Multi-objective Coevolutionary Algorithm
Jian Hu Research Center of Technology, Policy and Management School of Management, Harbin Institute of Technology, Harbin 150001 jianhu-hit @163.com
Xiang Yang-Li Research Center of Technology, Policy and Management School of Management, Harbin Institute of Technology, Harbin 150001 xiangyangli@hit.edu.cn

Abstract
Association rule mining can be considered as a multi-objective problem, rather than as a single objective one. To enhance the correlation degree and comprehensibility of association rule, two new measures, including statistical correlation and comprehensibility, as objection functions are proposed in this paper. Their calculating formulas and primary characteristics are given. Association rule mining is generally solved by lexicographic order method. On the basis of discussing the weakness of above method, a new coevolutionary algorithm is put forward in this paper to solve multi-objective optimization problem of
association rule. Three coevolutionary operators are designed and the mining algorithm is realized in this paper. According to experimentation, the algorithm has been found suitable for association rule mining of large databases.

A Cache-based Attribute Granular Computing System
Xiaoxia Huang
Department of Computer Science and Engineering, Shanghai Maritime University
Shanghai 200135, P.R. China
lhuangxiaoxia@163.com Lun Cheng Department of Control Science and Engineering, Tongji University Shanghai 200092, P.R. China
yunccll@163.com

Abstract
This paper presents a multilayer cache-based attribute granular computing system. After defining an attribute granule, it brings forward an AHP based attribute granules combination algorithm which can be used for dimensionality reduction in the preprocess stage of data mining. A cache-based operation and storage model is presented then. The storage management of the attribute granules is discussed mainly. Finally a hierarchy cache-based attribute granular computing system is presented. It can be used to implement the AHP based attribute granules combination algorithm and other algorithms based on attribute granular computing.

Research and Realization of Text Mining Algorithm on Web1
1 Corresponding author: Yuhui Qiu yhqiu@swu.edu.cn
Shiqun Yin Yuhui Qiu Jike Ge
Faculty of Computer and Information Science Southwest University
Chongqing, China 400715
E-mail: qiong-yin@126.com

Abstract
It is recognized that text information on Web is growing at an astounding pace. Research and application of text mining on Web is an important branch in the data mining. Now people mainly use information retrieval (IR) or the search engine to look up Web information. But IR focuses on searching for information that is explicitly present but not latent knowledge in some document. the search engine can hardly according to different need of different customers and provide individual service, and it is very difficult to mine data further. However, text mining on Web aims to resolve this problem. This paper discusses an Algorithm of how to follow the appointed website or Web page according to the user’s request by using the text mining technique, how to extract and express text characteristic, how to classify the data information with feedback judgement combined with the Web page text contents for later use. We present experiments on different data set that demonstrate more effectiveness of our algorithm than traditional algorithm. The process of Web text mining, information extraction method, mining algorithm and realization technique are discussed in details. Keywords: Web Text mining, Information extraction, mode discovery, Text Classification, feedback judgement.

An Active Data Integration Model Based on P2P Routing Service1
1 Foundation item: Project supported by the Science & Technology Plan of Zhejiang Province, China (No.2005C11034)
Wuling Ren
Abstract
To provide more efficient and active data integration service in network manufacturing environment for cooperated enterprises, a 5-layered active data integration model was proposed. Core of the model are layer 2, 3 and 4, which separately defines the description of data resources, data routing service and active data exchange service. Data router which provides data routing service uses P2P technique to locate application nodes which possess resources required and select the optimal path to download the resources among original resource provider and the nodes having the designated resources. The data pump that provides active data exchange service uses XML-based and remote controlled data exchange technique to perform data syntax analysis and semantic check, and then draws data from local applications or loads data into the applications with data exchange specifications. With this model, the shared data resources may have more adaptability and activeness, resource transmission delay will be shortened, and the effect of data integration will be enhanced.

Towards Improving Ant-based Clustering-An Chaotic Ant Clustering Algorithm
Xiaofang Huang, a, b, Yixian Yang, a, Xinxin Niu, a
a Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, b Department of Computer Science, Southwest University of Science and Technology

tinahxf@gmail.com

Abstract
Ant-based clustering as a nature-inspired heuristic algorithm has been applied in a data-mining context to perform both clustering and topographic mapping. It is derived from a basic model of behavior observed in real ant colonies. Early works demonstrated some promising characteristics of the ant-based clustering, but they did not extend to improve its performance, stability, convergence, and other key features. In this paper, we describe an improved version, called CACAS, adopting an important strategy of using chaotic perturbation to improve individual quality and utilized chaos perturbation to avoid the search being trapped in local optimum. We compare its performance with the K-means approach and ant-based clustering by evaluation functions and topographic mapping using a set of analytical data. Our results demonstrate CACAS is a robust and viable approach.
An Effective Algorithm for Mining Weighted Association Rules in Telecommunication Networks
Tongyan Li
Key Laboratory of Broadband Optical Fiber Transmission and Communication Networks of Ministry of Education, UESTC, Chengdu 610054 Email：sunny60138800@yahoo.com.cn
Xingming Li, Hailin Xiao Key Laboratory of Broadband Optical Fiber Transmission and Communication Networks of Ministry of Education, UESTC, Chengdu 610054 Email：xingmingL@uestc.edu.cn

Abstract
The algorithms of weighted association rules mining and weights confirming were studied in alarm correlation analysis. A novel method named Neural Network based WFP-Tree (NNWFP) for mining association rules was proposed. NNWFP differs from the classical weighted association rules mining algorithm MINWAL (O). It is an efficient algorithm based on weighted frequent pattern tree, and the weights of the items are confirmed by the neural network. Experiments on a large alarm data set show that the approach is efficient and practical for finding frequent patterns in the alarm correlation analysis of telecommunication networks, and the performance of NNWFP is better than MINWAL (O)

The Correlation between the Wavelet Base Properties and Image Compression
Li Ke
Department of Biomedical Engineering Shenyang University of Technology
College of Information Science & Engineering Northeastern University
Shenyang, Liaoning, P.R.CHINA amykeli@hotmail.com
Qiang Du
Faculty of Science, ChangChun University of Science and Technology, Changchun, Jilin 130022, P.R.CHINA leonarddu@sina.com
Zhe Su
Department of Biomedical Engineering Shenyang University of Technology
Shenyang, Liaoning, P.R.CHINA zhes_0622@hotmail.com

Abstract
When wavelet transform is applied to image compression, the chosen wavelet base affects the efficiency of coding and the quality of the reconstructed image, because the property parameters of different wavelet bases are varied, it is very important to research the correlation between the wavelet base properties and image compression. Chosen wavelet bases of one family for the experiments are convenient for analyzing contrastively, and the results have high reliability, and Daubechies wavelet bases with the properties of compactly supported, orthogonality, regularity, vanishing moment are widely used, then the paper chooses Daubechies wavelet bases as the research object, analyzes the correlation between the wavelet base properties and the image compression. The experiment results present the principles of wavelet base choice in image compression.

Probabilistic Document Correlation Model
Xiping Jia  
South China University of Technology  
School of Computer Science and Engineering  
Guangzhou 510640, China  
jiaxp@126.com  
Hong Peng  
South China University of Technology  
School of Computer Science and Engineering  
Guangzhou 510640, China

Abstract
Vector Space Model (VSM) and related models are popular in document relationship analysis in text mining recently. However, they are failed to discover the document correlation from topic level. This paper proposes a probabilistic document correlation model (PDC) to capture the document correlation based on topics. The PDC model defines the document correlation by the posterior probability of documents. And the posterior probability of each document is resolved through introducing the posterior probability of topics and topic similarity. Latent Dirichlet Allocation (LDA), a generative topic model, is used for topic retrieval in this paper. Experiments on correlated document search show that the PDC model outperforms the VSM in average retrieval precision document compressing.

An improved clustering algorithm based on ant colony approach
Zhang Tao Lv Xiaodong Zhang Zaixu
(College of Economic Administration of China University of Petroleum (East China), Shandong Dongying, P.R. China, 257061)
Email: zht2129@126.com

Abstract
Ant colony algorithm is a kind of evolutionary algorithm with global optimization quality to deal with discrete problem. Clustering analysis is an important part in data mining community. Traditional clustering algorithm is slow of the convergence and sensitive to the initial value and preset classed in large scale data set. The ant colony algorithm was applied in aggregation analysis for the first time in this paper. A new clustering algorithm was presented based on the ant colony algorithm. This algorithm has quality of essential parallel, quick convergence and high effectiveness. The experimental result shows that it is about 10% higher than the C-means method in effectiveness.

Keywords: ant colony algorithm, clustering analysis, essential parallel

An Automatic kernel of Graph Clustering Method in Conforming Clustering
Hua-Fu Ding Harbin Institute of Technology  
Harbin University of Science and Technolgy No.92,west Da-Zhi Street,Harbin,Heilongjiang,China  
No.52 Xuefu Road Nangang District,Harbin,Heilongjiang,China Dinghuafu1107@sina.com

Abstract
Based on analyzing graph theory knowledge and kernel function theory, every data sample is considered as top point V in graph, so all data samples consist of nondirectional weighted graph $G=(V,E^*)$, which takes similarity as weighted value. In the perspective of graph theory, this article defines connected modulus,
which can fully reflect the best clustering number. This modulus categorizes similar text into a connected graph, and keeps the clearance of physical meaning. In this paper, a Kernel of Graph Clustering method based on clustering was proposed, this arithmetic is compared with kernel C-equal value arithmetic. The test justifies that this arithmetic not only has less complexity in time and space, but also good robustness. Key word: Kernel function, graph theory, connected graph, kernel clustering, kernel of Graph Clustering

An Algorithm for Classifying Incomplete Data With Selective Bayes Classifiers
Jingnian Chen, Xiaoping Xue, Fengzhan Tian and Houkuan Huang
School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China
Dept. of Information and computing Science, Shandong University of Finance, Jinan, Shandong, 250014, China
School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
E-mail: jnchen06@163.com

Abstract
Actual data sets are often incomplete because of various kinds of reason. Although many algorithms for classification have been proposed, most of them deal with complete data. So methods of constructing classifiers for incomplete data deserve more attention. By analyzing main methods of processing incomplete data for classification, this paper presents a selective Bayes classifier for classifying incomplete data. The proposed algorithm needs no assumption about data sets that are necessary for previous methods of processing incomplete data. Experiments on twelve benchmark incomplete data sets show that this algorithm can greatly improve the accuracy of classification. Furthermore, it can also sharply reduce the number of attributes and so can greatly simplify the data sets and classifiers.

Synchronization of Uncertain Lorenz Chaotic Systems Based on a Novel Active Pining Control
Qu Shao-cheng, Gong Mei-jing
Department of Information and Technology, Huazhong Normal University, Wuhan, Hubei, 430079, China
E-mail: qushaocheng@mail.ccnu.edu.cn

Abstract
This paper discusses the synchronization of two Lorenz chaotic systems with parameters perturbation. Based on active control strategy, a novel active pining control synchronization approach is presented. The design of the whole controller only uses a system state. According to Lyapunov stability theory, the synchronization conditions of active pining control method for the two uncertain chaotic systems are given. And robust stability of uncertain chaotic systems synchronization is guaranteed. Numerical simulations are used to show the robustness and effectiveness of the proposed control strategy.
The Implementation Architecture of Content Protection in P2P Network
Cheng Yang Communication University of China cafeeyang@163.com Jianbo Liu Communication University of China ljb@cuc.edu.cn Yichun Zhang, Aina Sui Communication University of China zhangyichun@cuc.edu.cn

Abstract
P2P content sharing is often blamed for copyright infringement, making the establishment of content security technologies an urgent need. A PCP(P2P-based Content Protection) system is proposed in this paper. The system is based on a trust model that focuses on content security, rights management and access control in P2P network. Encryption, digital watermarking, and packaging technologies are adopted to protect the confidentiality and integrity of contents, and support copyrights verifying and piracy tracing. The structure of rights management integrates the distributed and centralized modes, which not only reduces the burdens of networks and rights server, but also provides controllability. For the access control, the authentication is divided into three aspects of certificate, identity, and credit. The PCP system is implemented to prove that it can provide a more robust intellectual property protection solution for P2P content delivery.

Transductive Support Vector Machine for Personal Inboxes Spam Categorization
Chao Xu, Yiming Zhou School of Computer Science and Engineer, Beihang University, Beijing 100083, China chaoxu@263.net

Abstract
A method based on transductive support vector machine for personalized spam filtering is proposed. Both labeled emails from the public available source and unlabeled emails in individual inbox are used as the input of the classifier. The problem of the generalizing the training data to the test data in SVM is solved. It provides a way to combine the ability of generalization and adaptation for the spam categorization. The model and parameter selection is stated in order to improve the performance of TSVM. The experiments show that the results of filtering with TSVM are better than the SVM.

Random Jump Index: A Trustworthy Index for Random Insertion
He Huang College of Software Beijing University of Aeronautics and Astronautics huanghe@buaa.edu.cn Fengchen Liu College of Software Beijing University of Aeronautics and Astronautics aric101@hotmail.com Qingwen Liu College of Computer Science Beijing University of Science and Technology netperson_ustb@126.com

Abstract
This paper presents an improved structure of Jump Index for trustworthy key search retention, called Random Jump Index. Unlike Jump Index, in which sequences must be strictly monotonically increased, this new jump index supports inserting of random sequences. This property enhances the efficiency of building index largely compared with Jump Index. Random Jump Index has the similar query efficiency of Jump Index. The structure of Random Jump ensure that every element has the unique and fixed path in this index, the index is fossilized. Therefore, Random Jump Index is a trustworthy index.
Study of Lyapunov Exponent Spectra for Axial-flow Compression System
Jiangming Yu
Northwestern Polytechnical University
Xi’an, China
Dingwei8011@126.com
Jiang Zhang, Wei Ding, Youli Wu
Engineering College, Air Force Engineering University
Xi’an, China
Wu_youli@126.com

Abstract
The Lyapunov exponent spectra of the axial-flow compression system’s Moore-Greitzer model were researched with chaos theory. When the parameter B of the MG model is greater (surge) or smaller (stall), the system’s Lyapunov exponent spectra are all (0, -). So the compressor’s working points are all on a limit circle, when the compressor is in the state of surge or stall. When the compressor is surge, it can come into a full limit circle, but in the stall, it can not. The conclusion was applied to detect the stall of the compressor. The numerical experimentation results demonstrate that the method can exactly detect the stage of the first stall before the start of deep rotating stall.

Specification of Access Control Policies for Web Services
Miao Liu, Wei Zhang, Huai-Liang Liu
School of Information and Mechanical & Electrical Engineering, Guangzhou University, China
E-Mail: gzliumiao@yahoo.com.cn

Abstract
In this paper we design an access control policy language WSACPL for web services. The WSACPL language is comprised of the WSACPL policy ontology, and includes a mechanism to induce SWRL language to express access control rules. The paper also brings up the method to compute authorization results of composite processes in OWL-S. On the analysis of cause and kinds of policy conflicts, the paper represents the method to resolve conflicts among WSACPL policies.

RBTN: a Role-Based Trust Negotiation Model
Yizhu Zhao
School of Computer
Huazhong University of Science and Technology
Wuhan, China
missbamboofirst@163.com
Hongwei Lu
School of Computer
Huazhong University of Science and Technology
Wuhan, China  hwlu@mail.hust.edu.cn

new approach for establishing trust between strangers through the exchange of digital credentials and the use of access control policies. However, in TN/ATN, a user has to negotiate with the server each time he
requests several resources or services from it and disclose credentials even if he had disclosed it before. In this paper, a Role-Based Trust Negotiation model (called RBTN) is proposed. RBTN introduces the role concept to trust negotiation, and assigns roles to users according to their credentials, which are disclosed during the previous negotiations. Thus RBTN can reduce the rounds of negotiation when one visits several resources or services one time. In the paper, we have a detailed description of RBTN. Thereto, a use case is given to show how the model works, which illustrates that RBTN is sound and reasonable.

μCLinux Security Enhancement Technology Based on MAC
Gaozu Wang*, Weihua Li*, Yangling Xu+, Jianfeng Yan*
*School of Computer Science
Northwestern Polytechnical University
Xi’an, Shanxi Province, China
wanggz@nwpu.edu.cn
+School of Automation
Northwestern Polytechnical University
Xi’an, Shanxi Province, China
flightxu@163.com

Abstract
μCLinux is an embedded operating system with high performance. Security of μCLinux is of great importance for embedded system based on it. To solve security problems of μCLinux system, the author adopts Linux Security Module (LSM) framework and puts forth a multi-policy mandatory access control (MAC) mechanism based on both Domain and Type Enforcement (DTE) model and improved Bell-La Padula (BLP) model. The mechanism enhances security protection of μCLinux kernel and implements access control in fine-grain level to ensure confidentiality and integrity of the system. The scheme proves to be applied in most embedded system with properties of Level B1 security standard, which ensures security of all application softwares.

UCGS: A Usage Control Approach for Grid Services
Yiduo Mei, Xiaoshe Dong, Weiguo Wu, Shangyuan Guan, Jing Xu
School of Electronic and Information Engineering, Xi’an Jiaotong University
Xi’an, 710049, China
meiyiduo@gmail.com, xsdong@mail.xjtu.edu.cn

Abstract
The dynamic and multi-institutional nature of the grid environments introduces challenging security issues that demand new technical approaches. But traditional access control models consider static authorization decisions based on subjects’ pre-assigned permissions on target objects and focus on a closed system, therefore, they are not suitable for the dynamic grid environments. To address the above problems, we propose UCGS, a novel usage control approach for grid services. Our approach is inspired by the Usage Control Model (UCON). UCGS improves the security of the grid services by employing a continuous usage
control of the grid services, monitoring the behavior of the subjects. It enables richer and finer-grained control
over authorization and usage of grid services and resources than that of traditional access control
models. "Blacklist", "unilateral contract" and "arbitrator" are introduced in UCGS to guarantee that
a subject can not deny its obligations after service is complete, which contributes to maintain the normal
order of the grid environments and the security and interests of the service providers.

Discussion about Similarity Measures in Pattern Recognition of Fuzzy Information
Zhang-lin Guo
School of Economics and Management Hebei University of Engineering
Handan 056038, China  gg_zz_ll@163.com
Jing Tian School of Economics and Management
Hebei University of Engineering Handan 056038, China
tianjingle27@163.com

Abstract
As one of the important indicators to describe the degree of similarity of two fuzzy sets, the similarity
measure is the basic theoretical foundation in pattern recognition of fuzzy information. Based on the
Concept Principle, each concept should be compatible, independent and complete. Following the Concept
Principle and meanwhile using counterexamples in Cantor sets with finite elements, the similarity
measures in fuzzy mathematics are questioned. Firstly, the definition of the similarity measure between
Cantor sets and Clear sets both with finite elements are given based on Concept Principle. Then, the
incompleteness of existing similarity measures between two fuzzy sets is proved by some counterexamples in Cantor sets
with finite elements. Two useful conclusions are presented as follows: Lattice-similarity and
Hamming-similarity are questionable. The properties in the axiom definition of similarity measures are necessary but not
sufficient conditions in fuzzy mathematics. Finally, we propose to use a new mathematic tool, the similarity
measures of clear sets to solve the pattern recognition of fuzzy information.

Reconstruction of Partially Occluded Face by Fast Recursive PCA
Zhi-Ming Wang1,2, Jian-Hua Tao2
1: School of Information Engineering,
University of Science and Technology Beijing, Beijing, China, 100083
2: National Laboratory of Pattern Recognition, Institute of Automation,
Chinese Academy of Sciences, Beijing, China, 100080
wangzhiming@tsinghua.org.cn

Abstract
This paper proposes a fast recursive PCA (Principal Component Analysis) algorithm to remove
face occlusions. In training phase, all faces are normalized by two eye centers and two mouth corners,
and eigenvectors (eigenfaces) were obtained by PCA analysis. In test phase, face occlusion is removed by iteratively perform two steps of analysis and synthesis. New damaged face is first normalized by clicking
An Improved PCA Face Recognition Algorithm Based on the Discrete Wavelet Transform and the Support Vector Machines
Hong Wang, Su Yang, Wei Liao
School of Information Engineering, Wuhan University of Technology, China
whong2002@vip.sina.com, suyang815@163.com, liaowei120@163.com

Abstract
In this paper, an improved PCA face recognition algorithm based on the Discrete Wavelet Transform and the Support Vector Machines is presented. The 2-D Discrete Wavelet Transform has been used to process the ORL standard face images to form the low frequency sub images by extracting the low frequency component. Then the PCA method is used to obtain the characterizations of these sub images. At last, the extracted eigenvectors are put into the SVM classifier for training and recognition. The experimental results indicate that this algorithm reduces the computational quantity because the dimension of the total population scatter matrix of the source images has deduced a lot and the performance of the SVM classifier is superior to many other classifiers. Compared with the traditional PCA face recognition algorithm, the calculation speed and the recognition efficiency here increase a lot.

DT-CWT Feature based Face Recognition using Supervised Kernel ONPP
Yuehui Sun
College of Information Engineering, Guangdong University of Technology, Guangzhou (510006), China
Yuehui_sun@126.com

Abstract
A novel DT-CWT feature-Kernel face recognition method is proposed in this paper. This involves transforming a face image with DT-CWT on feature extraction stage, and supervised kernel Orthogonal Neighborhood Preserving Projections (ONPP) being then automatically applied to the feature vectors. Numerical experiments are reported to illustrate the performance of our algorithm and to compare it with a few competing methods.

Automatic Fire smoke Detection Based on Image Visual Features
Zhengguang Xu, Jialin Xu
Information Engineering School, University of Science and Technology Beijing
Abstract
For open spaces, this paper proposes a novel method for automatic fire smoke detection based on image visual features. The greatest characteristic of the method is that both static and dynamic features of fire smoke are investigated. And the basic strategy is that we extract features of the moving target including growth, disorder, frequent flicker in boundaries, selfsimilarity and local wavelet energy as a joint feature vector which will be normalized, and then a BP artificial neural network is trained to recognize fire smoke. Experimental results show that this method can achieve early detection of fire accident with high accuracy and stronger anti-jamming ability.

A Novel 3D Model Retrieval Method Based on the Object Outline of Image
Tianyang Lv1, 2, Qian Song1, Shaobin Huang2, Zhengxuan Wang1
1 College of Computer Science and Technology, Jilin University, Changchun, China
2 College of Computer Science and Technology, Harbin Engineering University, Harbin, China
raynor1979@163.com

Abstract
To compensate the drawbacks of traditional 3D model retrieval methods which adopt several keywords or a sample model, the paper proposes a novel retrieval method based on the image which contains user’s desired object. Since object’s outline can efficiently describe its content especially its shape, we first extract the object outline from image and then obtain the set of shape points from the outline. Through comparing the shape feature of the outlines of 3D model’s multiple 2D projections with that of the desired object’s outline, the related 3D models are returned. The experiments conducted on a classical 3D model database, Princeton Shape Benchmark, show that our method can efficiently retrieve the desired models according to the images obtained from web and digital camera.

A Robust Algorithm for Iris Localization Based on Radial Symmetry
Wencong Zhang, Bin Li, Xueyi Ye, Zhenquan Zhuang
MOE-Microsoft Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, 230027 Hefei, China
binli@ustc.edu.cn

Abstract
Previous algorithms have good localization performance for iris images captured in the ideal condition. However, in practice, the quality of iris image is greatly influenced by luminance, eyelashes, hair or glasses frame, which is easy to cause mislocalization. In order to improve the robustness of iris localization, this paper proposes a new localization algorithm based on the radial symmetry transform, in which the radial symmetry characteristic of the pupil is fully used to realize iris localization. Experimental results show that the proposed algorithm can efficiently avoid the interference of luminance and other bad conditions, and realize robust precise localization in a real-time system.

Using Nonlinear Features in Automatic English Lexical Stress Detection
Nan Chen School of Electronic and Information Engineering, South China University of Technology, Guangzhou, 510641, China
n.ch@mail.scut.edu.cn
Qianhua He School of Electronic and Information Engineering, South China University of Technology, Guangzhou, 510641, China
eeqhhe@scut.edu.cn
**Abstract**

Lexical stress is an important prosodic feature, especially for stress-timed language such as English. This paper proposes three novel features, based on the nonlinear Bark scale and the Teager Energy Operator (TEO), for automatic English lexical stress detection. The proposed features are Bark Scale Cepstrum (BSC), Time Domain TEO-Bark Scale Cepstrum (TDT-BSC) and Frequency Domain TEO-Bark Scale Cepstrum (FDT-BSC). Their contributions, along with traditional features and their combinations, to English lexical stress detection are evaluated by single word pairs and continue sentences. Evaluation results showed that these new features gave significant improvement over traditional ones.

**Dissymmetrical P2P Topology and Resource locating Algorithm**
Yang Jing He Liang*
Department of Computer Science, East China Normal University, Shanghai, China
lhe@cs.ecnu.edu.cn

**Abstract**

The paper proposes a dissymmetrical and pure P2P topology based on K-ary-tree architecture named DSKTree topology, with the view of “node symmetrical characteristic”, it can solve the unstable and linearly increasing scale problem in existing resource sharing application using pure P2P topology. We also design Resource locating Algorithm in DSKTree topology. The performance analysis shows that it can optimize the cost of locating and lower the impact to performance of pure P2P topology while the scale of the system increases.

Keywords: P2P, Peer-to-Peer, Dissymmetrical, Resource locating

---

**A Multi-Constraint QoS Routing Protocol with Route-Request Selection Based on Mobile Predicting in MANET**
Jin LIAN1,2, Layuan L1; Xiaoyan ZHU2 1.School of Computer Science & Technology Wuhan University of Technology Wuhan, P.R.China lj_jhun@163.com 2.School of Mathematics & Computer Science JiangHan University Wuhan , P.R.China zxy_jhun@163.com

**Abstract**

Due to the dynamic nature of the network topology and restricted resources, the stable routing based on quality of service (QoS) in mobile ad hoc network (MANET) is a challenging task. QoS requirement with uncertain parameters has become a very important research issue in MANET. The paper presents a multiconstraint QoS Routing protocol with Route-Request Selection based on Mobile Predicting (QRRSMP). The QRRSMP is the scalable routing algorithm whose control overhead should be under control to keep up with increasing offered load. In this algorithm, the goal is to construct a stable QoS routing path and reduce the number of Route-Request (RREQ) packet by forwarding or discarding RREQ packets. Simulation results show that the proposed approach reduces the control overhead and provides the QoS routing stability in dynamic mobile networks.

---

**Research on the Instrument on Network(ION) and its Key Technologies**
Huang Fei
National University of Defense Technology
Measure & Control Technology Lab.
410073, Changsha Hunan, China icemarshal@163.com

Ming Dexiang
Abstract
The instrument on network is intended to bridge the “gap” between information highway and nature and solve the problem of “connection of tracks” between the test instrument and information highway, with “The Measure and Control Network” plus “Sensors” as its basic model. The paper puts forward an open architecture of ION based on network interconnection, expounds basic definitions and connotations of ION in depth, and provides a tentative analysis of such key technology issues as unified time, time determinability transmission, etc.

Stability Analysis for Grid Services Dynamic Scheduling System
Supported by the National Natural Science Foundation of China No. 90412012, No.60673160
Yang Yang Information Engineering School, University of Science and Technology Beijing Beijing 100083,China yyang@ustb.edu.cn
Weidong Hao Information Engineering School, University of Science and Technology Beijing Beijing 100083,China wed@ustb.edu.cn
Ming Zeng Information Engineering School, University of Science and Technology Beijing Beijing 100083,China

Abstract
Grid services and Agents are increasingly walking to convergence. In this paper, an autonomy-oriented state space model based on the discrete events is given to describe the grid services dynamic scheduling system which processes a number of heterogeneous jobs concurrently. The stability condition of the Grid Services Dynamic Scheduling System is given and proved, then the suitable scheduling policy is found and the stability of the policy is proved. Simulation shows that the mathematical model and its scheduling policy can make the system within a controlled and stable state..
Keywords: distributed system, Service Grid, stability analysis, scheduling policy, QoS(Quality of Services)

Routing Algorithm of Network Coding on Multicast
Shaoguo Tao, Wenbo Qiao, Zongkai Yang, Wenqing Cheng
Dept. of Electronics and Information Engineering, Huazhong University of Science and Technology, China
{taoshaoguo,qiaowb}@gmail.com {yangzk,wqcheng}@mail.hust.edu.cn

Abstract
As a novel transmission mechanism to enhance the performance of multicast network, network coding (NC) has received much researcher concern recently. Due to its inherent characteristic, the process of constructing the routing paths in network coding is different from the traditional IP multicast based on replicating and forwarding. In this paper, we analyze the algebraic model of network coding and conclude that the goal of the routing problem in network coding is to build edge-disjoin paths from the source to each receiver. Using the idea of tree packing, we present a detailed routing algorithm for network coding based multicast. Simulations based on the
algorithm show that, for network coding based multicast, performance in terms of achievable throughput and bandwidth consumption has been improved significantly with respect to the traditional IP multicast.

A Parallel Data Processing Middleware Based on Clusters
Nianbin Wang Department of Computer Science and Technology, Harbin Engineering University Harbin, 150001, P.R China wangnianbin@hrbeu.edu.cn
Xiangzhong Jiao Department of Computer Science and Technology, Harbin Engineering University Harbin, 150001, P.R China jiaoxiangzhong@163.com
Hui Cheng Department of Computer Science and Technology, Harbin Engineering University Harbin, 150001, P.R China giselleching@163.com

Abstract
HPDPM is a middleware system applying in share nothing clusters architecture to support parallel and distributed computing. Presenting a new method to use parallel data processing middleware instead of parallel database system provides the ability for high performance computing. A framework is given for realizing parallel data manipulation. The primary modules of the middleware are described. Key techniques used to improve system performance, include data placement and semantic caching are discussed in detail. Then, the work principles and work steps of the middleware are presented.

Implementation
and experiments of this study showed that this approach can improve system performance efficiently. At present, the middleware system has been applied to some large engineering projects which capacity of data is a little more than 1000 Gigabytes.

DRM interoperability
Ton Kalker
IEEE Fellow, Hewlett-Packard Labs, Multimedia Communications & Networking Department, CA, US

Abstract
The use of Digital Rights Management (DRM) technologies for the enforcement of digital media usage models is currently subject of a heated debate. Consumer organizations and national governments claim that DRM technology interferes with basic personal rights, such as the right to make copies for personal use or the right to use content on any platform of choice. This issue has lately gained increased attention by a trend in some European countries to force DRM vendors and online media stores to open up their respective DRM technologies, i.e. make them interoperable. In the first part of this talk we discuss the many obstacles to DRM interoperability, both technological, legal and business wise. In the second part we discuss discuss some potential solutions to the DRM interoperability problem. In particular, we present the Coral DRM interoperability framework that allows multiple DRM systems to seamlessly work together while at the same time requiring minimal modification to existing DRMs.

Towards an Understanding of the Brain via Microscopic and Macroscopic Studies
(Keynote Address at the International Conference on Computational Intelligence and Security, CIS 2007, Harbin, China, Dec 2007)
L. M. Patnaik
Department of Computer Science and Automation
Understanding the human brain is a daunting task. To gain a good understanding of the abilities of the brain, we must know about the functions of brain at different levels of organization: molecules, synapses, neurons and their interconnections, and brain maps. Improved knowledge of brain is crucial for better diagnosis and treatment of a variety of brain disorders. The brain can be viewed as a complex network and we present the results of our studies on small-world and scale-free architecture of the brain network. For this microscopic experimental study, we use a multi-electrode array. For EEG signal classification, support vector machine and neural networks have been used to yield accuracy of the order of 97.5%. Wavelets and support vector machine yield excellent classification of fMRI images. The studies of EEG signals and fMRI pertain to the macroscopic level.

Mining with Noise Knowledge: Error Aware Data Mining
Xindong Wu
Department of Computer Science
University of Vermont, Vermont, USA

Abstract
Real-world data are dirty, and therefore, noise handling is a defining characteristic for data mining research and applications. This talk will review existing research efforts on data cleansing and classifier ensembling in dealing with random noise, and then present our recent research on an error aware data mining design to process structured noise. This error aware data mining framework makes use of error information (such as noise level, noise distribution, and data corruption rules) to improve data mining results. Experimental comparisons on real-world datasets will demonstrate the effectiveness of this design.

Stephen D. Wolthusen
Norwegian Information Security Lab, Gjovik University College,
Norway Department of Mathematics Surrey Royal Holloway,
University of London, United Kingdom

Abstract
Tactical networks frequently need to be set up without adequate infrastructure in place or where infrastructure elements can be destroyed easily and, moreover, must themselves be mobile and extensible. It is therefore desirable to provide mechanisms based on mobile ad hoc networks, which have been studied intensely in recent years. However, the specific requirements for tactical networks differ from civilian networks in that robustness in the face of direct attacks and compromised nodes leading to Byzantine behavior must be maintained and that above and beyond the need for energy efficiency it is necessary to limit radio frequency emanations both in terms of output power and in the area covered by the signals. In this paper we therefore describe several techniques for modeling the specific requirements underlying tactical networks and provide selected models for efficient distributed computation using the example of trust authority services, which form part of the core infrastructure in an ad hoc network as these services are required to establish trust relations and key exchanges efficiently where pre-shared keying is not desirable or appropriate.

Study on Evolutionary Neural Network Based on Ant Colony Optimization
Gao Wei
Wuhan Polytechnic University
Hubei, Wuhan 430023, P. R. China
wgaowh@hotmail.com

Abstract
The evolutionary neural network model can be generated combining the evolutionary optimization algorithm and neural network. Based on analysis of merits and demerits of previously proposed evolutionary neural network models, combining the continuous ant colony optimization proposed by author and BP neural network, a new evolutionary neural network whose architecture and connection weights evolve simultaneously is proposed. At last, through the typical XOR problem, the new ENN is compared and analyzed with BP neural network, traditional ENN based on genetic algorithm and evolutionary programming. The computing results show that the precision and efficiency of the new ENN are all better.

Fault Tolerant Control of a Class of Unknown Multivariable Nonlinear Systems Using Fuzzy Approximation
Shaocheng Tong
Department of Basic Mathematics of Liaoning University of Technology,
JinZhou, 121001, P.R. China
jztsc@sohu.com
Shuo Tong
Institute of System Sciences,
Northeastern University,
ShenYang, 110004, China

Abstract
In this paper, we have developed an adaptive fuzzy fault tolerant control approach for a class of MIMO unknown nonlinear systems based on the idea of a corrective control law which activated in the presence of a fault. Online approximators, in the forms of fuzzy logic systems, are used to learn the unknown dynamics and the unknown fault functions on-line and provide the fault tolerant control law. The closed-loop stability of the proposed fault tolerant control scheme is rigorously proved using Lyapunov theory and illustrated based on a simulation example.

H∞ Fuzzy Decentralized Control of Nonlinear Time-Delay Interconnected Systems
Tao Wang Shaocheng Tong
Department of Basic Mathematics of Liaoning University of Technology,
JinZhou, 121001, P.R. China
Quwangtao_65@sina.com

Abstract
H∞ Fuzzy decentralized state feedback is proposed for a class of continuous nonlinear interconnected systems with time-delay. First, an equivalent T-S fuzzy model represents the continuous nonlinear interconnected system with time-delay, then fuzzy decentralized state feedback control scheme is developed to override the external disturbances such that the H∞ control performance is achieved. Furthermore, the stability of the nonlinear interconnected system with time delay is also guaranteed. Finally, the simulation example is given to illustrate the effectiveness of the proposed methods.
An Improved Fuzzy Clustering Method to Detect Moving Objects
Yu Lu 1,2, Hao Zhu 1,2 and Qinzhang Wu 1
1 Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, P. R. China;
2 Graduate School of the Chinese Academy of Sciences, Beijing, P. R. China

Abstract
The classical fuzzy clustering method needs to determine the number of group for classification before all samples are processed and the number of group is fixed during iteration, which does not help to ensure the classification precision. Considering this, an improved fuzzy clustering method with elastic grouping logic is proposed. The elastic grouping logic, based on the samples’ ascriptions and their distances to the centers of each group, can dynamically adjust the number of group and achieve the accurate classification. Our improved clustering method is applied in the optical flow field. The experimental results show that our method has superiority over the classical clustering method in precision and can detect the moving object with precision.

Self-optimum Fuzzy Controller Based on Minesweeping Strategy
Hu Jing-Song, Wang Jia-bing, Yang Chuang-Xin
School of Computer Science and Engineering
South China University of Technology, Guangzhou 510641, China
{cshjs, jbwang}@scut.edu.cn

Abstract
The partly continuous algorithm (PCA) [1] is a simple and fine quality fuzzy control method, which can operate at high speed by a normal digital chip computer with few memories. A fast global strategy, called minesweeping strategy, is presented to optimize the fuzzy controller based on the partly continuous algorithm. The minesweeping strategy lets the current search “jump out”, from the current local minimum by exploiting a new area that is far away from local minima obtained earlier. Simulating Annealing and Tabu Search lets the current search “climb out”, step by step, hardly and wonderingly. Therefore the strategy to solve local minimum problem is more successful and faster than other methods. The selfoptimum fuzzy controller based on minesweeping strategy realizes real-time optimization and fine control quality to a nonlinear plant, of which mathematic model is not known.

Fuzzy Partition Based Curvelets and Wavelets Denoise Algorithm
Naizhang Feng, Liyong Ma and Yi Shen
School of Information Science and Engineering, Harbin Institute of Technology at Weihai
Weihai, 264209, P. R. China
{fengnz@yeah.net, hitmaly@yahoo.com.cn, shen@hit.edu.cn}

Abstract
Curvelets denoise approach has been proposed to obtain high quality result images recently. But artifacts often appear in the result images after applying curvelets denoise approach. A fuzzy partition based
A denoise algorithm was proposed to suppress the artifacts employing result images of curvelets and hidden Markov tree based wavelets denoise approaches. After fuzzy partition was applied to the image support, the local properties of the fuzzy nwindows were estimated. Image fusion was applied to the curvelets and wavelets result images where the weights were decided by the local properties. Experimental results demonstrated that the algorithm improved the visual quality of result images efficiently and suppressed the artifacts in result images evidently.

Variable Universe Multiple-Fuzzifications Control
Tianli Li, Hong Hu, Liang Zheng
Mechanical Engineering and Automation
Harbin Institute of Technology Shenzhen Graduate School
Lt988@hit.edu.cn

Abstract
A novel method is being proposed for the design of the fuzzy logic controller (FLC) in order to improve the controlling precision. This paper describes the design and implementation of some FLCs based on the variable universe and the multiple-fuzzifications methods. They are different from conventional FLC’s design method. No complex algorithm is required to implement the controllers. The actual performance of the novel FLCs at controlling the water tank temperature were evaluated against the performance of an intelligent temperature controller. The experiment results show that the design of fuzzy controllers can not only be carried out simply and easily, but also can improve the control performance. The effective methods mproposed are easily implementable on commonly used equipment such as PLC. Generally, the novel fuzzy controllers can both improve the performance of control system and cut down the cost of hardware.

Study on Fuzzy self-tuning PID internal model control algorithm and Its application
Zhang Ming-guang, Wang Peng, Wang zhao-gang
College of Electrical and Information Engineering, Lanzhou University of Technology,
Gansu Lanzhou, 730050, China
Wangpeng0617@163.com

Abstract
Through introducing 1/1 pade series to approximate the time delay unit and using the two steps design approach, the internal model control system can be changed into conventional PID unity feedback control system. Then used fuzzy inference to tune the PID parameters online, the fuzzy self-tuning PID internal model controller is realized. This controller combines the advantage of fuzzy control, internal model control and PID control. Fuzzy control is used to overcome the uncertainty of mathematical model of the real plant. Internal model control is used to resolve the large time-delay of the coke oven temperature control system. Simulation experiments have been done to coke oven temperature control system. Simulation results show that system adopted fuzzy self-tuning PID internal model control has smaller steady error, shorter adjusting time, smaller overshoot, faster rising time and comparatively strong robustness.
Solving Fuzzy QoS Constraint Satisfaction technique for Web Service Selection

Liu Zhuang 1, Huang YuanFei 2, Jian WeiGuang 3, Zhou JiangBo 4, Guo He-Qing 5
(1,5. South China University of Technology, 510641, PR.China
2,3,4. The Labour and Security Information Center of GuangZhou Municipal 510635
PR.China)
1. verdureview@yahoo.com.cn 2. hyf@gzlabour.gov.cn

Abstract
In global Web Services selection, it involves to multi-objectives optimization and tradeoffs of diversified QoS criteria, therefore a suitable genetic algorithm is proposed to tackle the service selection problem. Since the QoS criteria are not always explicit and usually containing of fuzzy element, So this paper focuses on the relation between constraint satisfaction of fuzzy QoS criteria optimization and fitness evolution in multi-objective Web services selection and how to adjust the fuzzy QoS criteria of individual to fit for the evolution of population.

mbedded Ethernet Communication Sever and Its Application in Family-and-School Communication
Tan Hai East China Institute of Technology (Nanchang Campus), Nachang 330013, China
htan@ecit.edu.cn
Zhou Xinqin East China Institute of Technology (Nanchang Campus), Nachang 330013,
China xqzhou@ecit.edu.cn

Abstract
Based on Supervisory & control system of Ethernet and traditional internet, the article puts forward a special embedded Ethernet sever which can contact PCs and internet console and supply electricity for internet console. It also offers detailed design and specific work process and finally explains its practical application in communication between home and school.

Study on Revising Configure Parameter in Embedded System and its Application
Tan Hai East China Institute of Technology Nanchang Campus, Nanchang 330013,
China htan@ecit.edu.cn
Zhou Xinqin
East China Institute of Technology Nanchang Campus, Nanchang 330013, China
xqzhou@ecit.edu.cn

Abstract
The article expounds the technology that UPD protocol is applied when revising configured the parameter remotely in embedded system. It also introduces the process in realizing the system with the corresponding codes in detail and related communication protocols. Finally gives a example how the research being applied for the “home-school-communication” system.
O2 Concentration Measurement of Furnace
Yihu Huang
College of Automation and Electron Engineering
Qingdao University of Science and Technology
Qingdao, China
hyhuzi@163.com

Abstract
Oxygen content of flue is key parameter to judge whether furnace is working on optimal state or not. Long time-lag of O2 Concentration and short life of its detection device have been influenced optimization operation of furnace. A novel Elman Neural Network model is proposed for measuring oxygen content of furnace. The model uses a novel category method to design input parameter of Elman NN, which reduce numbers of input parameter of neural network; therefore it meet the challenge of real-time control. By selecting different time of input value and output value (measured value of oxygen content) to study and train neural network, which time-interval is delay time of oxygen content of flue between the influencing factors of O2 Concentration, soft sensing of oxygen content of flue is changed to chamber’s. Comparing with the data measured by routine device that installed bottom of flue, Trial results show that good dynamic regulation performance of system can be obtained, and fuel efficiency is improved greatly.

A Method about Load Distribution of Fishing Mills Based on RBF Neural Network*

* This work is partially supported by the National Natural Science Foundation of China (Grant No. 60573065, 60373013), the Natural Science Foundation of Shandong Province (Grant No. Y2005F26).

Yan Wang Dongdong Liu
School of Control Science and Engineering, University of Jinan, Jinan
250022, China
E-mail: cse_wy@ujn.edu.cn

Quan Yang Yikang Sun
National Engineering Research Center for Advanced Rolling Technology, University of Science and Technology Beijing, Beijing
100083, China

Abstract
This paper use RBF neural networks to establish finishing thickness and rolling force models. Compared with those finishing models which have or have not traditional models as input, the importance of traditional models in application of neural networks is obvious. In order to improve the predictive precision of finishing thickness and rolling force, using BP and RBF neural networks to establish finishing models, the result indicates that the model of load distribution based on RBF neural network is more accurate also solving over-fitness problems in network application.

Application of Neural Networks in Wireless Sensor Network Routing Algorithm

Wenhui Zhao1, 2, Daxin Liu1, Yu Jiang2
1College of Computer, Harbin Engineering University, Harbin, China, 150001;
Abstract
The paper proposes a new routing algorithm in wireless sensor network. The main idea and the implementing approaches of the algorithm are introduced. The algorithm doesn't require any extra hardware. Simulations show that the algorithm can accomplish routing process correctly and quickly and increase the wireless sensor network's life obviously.

Radial Basis Function Neural Network Based on Ant Colony Optimization
Man Chun-tao,
School of Automation
Harbin University of Science and Technology
Harbin 150080, China
mct68@hrbust.edu.cn
Li Xiao-xia
School of Automation
Harbin University of Science and Technology
Harbin 150080, China
xiaoxia015@yahoo.com.cn
Zhang Li-yong
School of Measurement-Control Tech & Communications Engineering
Harbin University of Science and Technology
Harbin 150080, China

Abstract
To settle the problem that the cluster results of k-mean clustering Radial Basis Function (RBF) is easy to be influenced by selection of initial characters and converge to local minimum, Ant Colony Optimization (ACO) for the RBF neural networks which will optimize the center of RBF neural networks and reduce the number of the hidden layer neurons nodes and a model based on this method were presented in this paper. Compared with k-mean clustering RBF Algorithm, the result demonstrates that the accuracy of Ant Colony Optimization for the Radial Basis Function (RBF) neural networks is higher, and the extent of fitting has been improved.

Robust Designs for Templates of Directional Extraction
Cellular Neural Network with Application
Jinzhui Liu
School of Information Engineering
University of Science and Technology Beijing
Beijing, 100083, China
Abstract
The cellular neural/nonlinear network (CNN) is a powerful tool for image and video signal processing, robotic and biological visions. In this paper, the Selected Objects Extraction (SOE) CNN was generated to Directional Extraction (DE) CNN which enhance the capabilities of CNNs and improve their efficiency. Based on analytical approach, a theorem of designing robust templates for DE CNNs was established, which provides parameter inequalities to determine parameter intervals for implementing the corresponding functions. Several examples are provided to illustrate the effectiveness of the theorem for extracting selected objects directionally in binary images.

Models for Predicting the Value of E-commerce Trade in China
Min Liu1,2, Shudong Sun1
1. Northwestern Polytechnical University, Xi’an, 710072, China
2. Xi’an University of Finance and Economics
minliu_xian@163.com
Abstract
In the literature review, few studies exist, which predict the value of e-commerce. The study establishes models for predicting the value of e-commerce trade in China by use of main statistical indicators and data in Statistical Report on the Internet Development in China released by CNNIC. Firstly, factors affecting e-commerce trade value in China and their relation with e-commerce trade value are analyzed. Secondly, models for predicting the future of the factors are proposed. Finally, The combined model is constructed to predict the value of e-commerce in China in the near future, and is proved to be satisfied because the prediction results are close to related statistics released by authority organizations recently.

A Hybrid EA Approach with Cooperation between Individuals to Substructure Discovery in Graphical Databases
Xingong Chang
School of Management
Tianjin University
BOX 9034, Tianjin 300072, China
c_x_g@126.com
Minqiang Li
School of Management
Tianjin University  
92, Weijin Road,  
Tianjin 300072, China  
mqli@tju.edu.cn  
Jisong Kou  
School of Management  
Tianjin University  
92, Weijin Road,  
Tianjin 300072, China  
jskou@tju.edu.cn

Abstract  
A hybrid EA based algorithm is developed to discover potentially useful substructures from graphical databases. During the searching process, losing instances is very common and vital to the algorithm performance. To address this issue, an individual cooperation operator is proposed, which enables different individuals to search the same substructure in a cooperative way. In addition, a new mechanism is also proposed to preserve the diversity regarding both the composition of an individual and the composition of the whole population. Experimental results show that these hybrid scheme successfully enhances the searching capability of the algorithm and improves the qualities of solutions.

Searching Quasi-bicliques in Proteomic Data  
supported by the National Nature Science Foundation of China (60773010).  
Hongbiao Liu  
School of Computer, Wuhan  
University, Wuhan 430079,  
China  
Lobbyliu2004@hotmail.com  
Juan Liu  
School of Computer, Wuhan  
University, Wuhan 430079,  
China  
liujuan@whu.edu.cn  
Longhui Wang  
Wuhan National Laboratory  
for Optoelectronics,  
Huazhong University of  
Science and Technology,  
Wuhan, 430074, China

Abstract  
Finding a maximal biclique in a graph is an NPC problem. We developed a new, efficient method to search maximal quasi-bicliques from protein interaction network. At first, we divided the protein protein interaction network into vertex’s Distance-2-Subgraphs. Next, combining top down and branch and bound methods, we sought quasi-biclique from every vertex’s Distance-2-Subgraph. At last, we merged the redundant ones in the quasi-bicliques. We successfully applied our method on the Saccharomyces cerevisiae dataset and obtained 2754 distinct quasi-bicliques.
A Novel Attribute Reduction Algorithm Based on Rough Set and Information Entropy Theory
Baoyi WANG
School of Computer, North China Electric Power University, Baoding 071003, China
wangbaoyi@126.com
Shaomin ZHANG
School of Computer, North China Electric Power University, Baoding 071003, China
zhangshaomin@126.com

Abstract
The incompleteness of measurement approach of importance of attribute that is based on condition entropy is analyzed and proved through example. After the information entropy of element in positive region is introduced in the measurement of importance of attribute, both a novel measurement approach of importance of attribute and a novel measurement approach of importance of single attribute relative to attribute set are put forward. Based on above ideas, a heuristic attribute reduction algorithm is constructed by adopting SGF*(a, A, D) as heuristic information. Finally, the feasibility of the measurement approach of importance of attribute and the validity of the heuristic reduction algorithm are demonstrated by some classical databases in the UCI repository.

Knowledge Elicitation and Acquisition for Simulation Validation
Jun-Tao Wang, Fei-Yan Min
Shenyang Institute Aeronautical Engineering
College of Civil Aviation
No. 37, Daoyi South Street, Shenyang, 110136, P.R.C.

Abstract
The validation of simulation relies heavily on the opinions of domain experts, and it makes the validation task exhaustive and time-consuming. The knowledge-based methods can be applied for these problems. One of the main issues around this method is the elicitation and acquisition of the knowledge. Our knowledge elicitation approach falls in three phases, namely, position, description and discussion phase. Within each phase, the available acquisition techniques are introduced.

Improving the Non-dominate Sorting Genetic Algorithm For Multi-Objective Optimization
V. Seydi Ghomsheh i, M. Ahmadieh khanesar ii, M. Teshnehlab iii

i. Computer Department of Islamic Azad university of Kermanshah of Iran, member of ISLab K.N.Toosi
valhidsreydi@gmail.com

ii. K. N. Toosi university technology
Tehran, Iran, member of ISLab K.N.Toosi
ahmadieh@ieee.org

iii. K. N. Toosi university technology
Tehran, Iran
Abstract— the Non-dominant Sorting Genetic Algorithmic-II (NSGA-II) is a relatively recent technique for finding or approximating the Pareto-optimal set for multi-objective optimization problems. In different studies NSGA-II has shown good performance in comparison to other multi-objective evolutionary algorithms [10]. In this paper an improved version which is named Niching-NSGA-II (n-NSGA-II) is proposed. This algorithm uses new method after Non-dominant sorting procedure for keeping diversity. The comparison of n-NSGA-II with NSGA-II and other methods on ZDT test problems yields promising results.

Clonal Selection Algorithm with Adaptive Mutation and Roulette Wheel Selection
Yi He
School of Economics & Management
Chongqing Normal University
Chongqing, 400047, P.R.China
cqnuheyi@163.com
Chuanbao Jian
Development department
Shenzhen Lingyu Communications
Network Limited Company
Shenzhen, 518115, P.R.China

Abstract
In this paper, roulette wheel selection strategy and adaptive mutation operation were introduced to the basic immune clonal selection algorithm (ICSA) in order to overcome premature convergence and stagnation at the end stage of iterative optimization. The method was utilized to optimize two types of typical testing functions and the simulation results show that the algorithm can improve the ability of searching the global optimum and yield superior results compared with the basic immune clonal selection algorithm.

Security Operation Center Based on Immune System
Yi Niu
Department of Computer and Information Science,
City College,
Dongguan University of Technology,
Dongguan, Guangdong, China
ny3388@163.com
Quanjuzhang
Management Department,
City College,
Dongguan University of Technology,
Dongguan, Guangdong, China
zhangquanju@sina.com
Qilun Zheng
School of Computer Science and Engineering,
South China University of Technology,
Guangzhou, China,510610
csqlzhou@scut.edu.cn
Hong Peng
School of Computer Science and Engineering,
South China University of Technology,
Guangzhou, China,510610
Abstract
With the widespread application of large and complicated network, network safety has become an important issue. In this paper, we design a security operation center (SOC) using an analogy of natural world immunology. We adopt an immune mechanism that distinguishes self from non-self and cooperation among immune cells of the system. This system implements each immune cell as an agent based on our multi-agent language, which is an extension of concurrent logic programming languages. These agents can detect and reject intrusion by cooperating with each other.

Asymptotic Analysis of a Nonlinear SEIS Differential-Integral Equation Model
Xu Wenxiong, Zhang Tailei, Xu Zongben
(School of Science, Xi’an Jiaotong University, Xi’an, 710049, China)
E-mail: wxx@mail.xjtu.edu.cn

Abstract In this paper, a SEIS epidemic model with infection-age and nonlinear contact rate is studied, and the basic reproductive number which determines whether the disease dies out or persists is found. Further, the asymptotic stability of each equilibrium point is discussed, which extends the results of some related models. KeyWords Infection-age; Stability; Epidemic model; Basic reproductive number.

Approximation Algorithm for Pseudoknotted RNA Structure Prediction
Hengwu Li
School of Computer Science and Technology
Shandong University
NO.73 Jingshi Road, Jinan 250061, CHINA
Shandong Economic University
NO.7366 Erhuandong Road, Jinan 250014, CHINA
hengwuLi@mail.sdu.edu.cn

Abstract
Pseudoknotted RNA secondary structure prediction is an important problem in computational biology. Existing polynomial time algorithms have no performance guarantee or can handle only limited types of pseudoknots. Now for stacking base pairs prediction, the best approximation ratio of existing approximation algorithm is 3. In this paper allowing arbitrary pseudoknots, an approximation algorithm is given to maximize the number of stacking base pairs, and the approximation ratio of the approximation algorithm is improved from 3 to 1.5.

A New Algorithm for the Longest Common Subsequence Problem
Xuyu Xiang, a, b, Dafang Zhang, Jiaohua Qin, b
aSchool of Computer & Communication, Hunan University, Changsha, Hunan China, 410082
Abstract
In order to find the longest common subsequence (LCS) as soon as possible, we, with the method of match pairs, propose the new algorithm of the sequence of DNA, which is efficient both in time and in space on the basis of the improved dynamic programming theorem.

Extending Ontology Language for Semantic Web
Qing Yu
and Jinlin Wang

School of Computer Science and Technology, Tianjin University, Tianjin, 300072, China
School of Computer Science and Technology, Tianjin University of Technology, Tianjin, 300191, China
School of Electronic and Information Engineering, Tianjin University, Tianjin, 300072, China
qyu@tju.edu.cn

Abstract
The paper focuses on how to represent and infer the imprecise or fuzzy knowledge in real world. Ontologies are important technology used to describe the semantics of information, which provide a formal specification of a shared conceptualization. OWL is a promising ontology language which is intended to provide a formal description of concepts, terms, and relationships within a given knowledge domain. Although OWL has a powerful expressive ability on knowledge, it has no capability to represent the uncertain and imprecise information. In this paper, we extend OWL by fuzzy logic called FOWL (Fuzzy of OWL) for capturing imprecise or uncertain knowledge encountered in real world. In the end, we give an instance which shows that fuzzy information can be expressed well in the proposed ontology language.

Arithmetic Model Research of IDS Alarm Controlling
Qu Zhaoyang
Information Engineering College, Northeast Dianli University
qzywww@public.jl.jl.cn
Guo Liang
Information Engineering College, Northeast Dianli University
Guolianga0316@126.com
Wu Yan
College of Information Science and Engineering, SDUST

Abstract
In order to solve the high rate of wrong alarm in IDS, we designed alarm control model by analyzing alarming information. This model which using human olfaction passivation aims at the sustaining high frequency no-action alarming information in order to reduce rate of no-action alarming in IDS, achieve the low wrong alarming of IDS and make it convenient to administrators.
Using Relational Database to Build OWL Ontology from XML Data

Sources
Jiuyun Xu, Weichong Li
School of Computer & Communication Engineering, China University of Petroleum
jx13@leicester.ac.uk; liweychong@163.com

Abstract
The semantic web and web service take ontology into usage to describe the important concepts and relations among them. But the construction of ontology from scratch is costly and difficult. In this paper an approach is proposed to construct OWL ontology from XML document with the help of entity-relation model, and this approach will alleviate the difficulties in ontology construction.

Research and Realization of the Computer-assisted Colorimetry for Baked Porcelain Tooth

Jihong Liu
College of Information Science and Engineering, Northeastern University,
Shenyang,110004 Liaoning, China
Brain Science Research Center, Korea
Advanced Institute of Science and Technology,
Daejeon,305-701, Republic of Korea
liuji@ise.neu.edu.cn
Fangfan Han
Sino-Dutch Biomedical and Information Engineering School, Northeastern University,
Shenyang,110004 Liaoning, China
neusiluhuayu163@sina.com

Abstract
The defect of dentition and its abnormal and tooth row imperfection are the common diseases. Along with the development of science and technology, the dental restoration has already not only been limited to match in the shape, but also been requested the color matched with the natural tooth perfectly, make the dental case more lifelike on the sense of vision. The computer color matching (CCM) can satisfy this requirement. It can also avoid the effect of the surroundings to artificial colorimetric and improve the efficiency. After the analysis of tooth color character, three kinds of algorithms are adopted to carry on the colorimetry for baked porcelain tooth, which are the center colorimetry, the nine sub-areas subtraction colorimetry and the improved algorithm. Through analysis the accuracy and time consuming in colorimetry, the advantages and disadvantages of the three algorithms are compared. The Computer-aided Colorimetric System for Baked Porcelain Tooth(CaCSBPT) is also researched. This design is accomplished in Matlab platform. According to the reflection from clinicians, this design has better clinical value.
The Research of ASW Helicopter ACGF Construction Based on CXBR
HU Zheng-tao
School of Automation, Harbin Engineering University, Harbin 150001, China
navystrong@163.com
LIU Jian
Navy Submarine Academy, Qingdao 266071, China
jjjju@163.com

Abstract
In anti-submarine warfare (ASW) simulation system, agent based helicopter computer generated force (ACGF) has been an important and effective CGF by the use of agent AI knowledge. In order to have a better simulation of the behavior of ASW helicopter and to respond to different kinds of interrupts especially for the interrupts of different levels of action, it is essential to build an unusual ASW helicopter agent to the system need of interaction, flexibility and validity, and give a model of the behavior decision and a simulation frame. This article constructs a model of ASW helicopter ACGF on behavior decision making in the method named CXBR after the analysis of system firstly, then classifies the actions of the helicopter ACGF, moreover constructs a database for forces and environment and a database for tactics knowledge, and verifies the validity of the model to the need of system finally.

On Spam Detection Based on Cognitive Pattern Recognition
Tiancai Liang
College of Automatic Science & Engineering South China University of Technology Guangzhou PR 510641, China liang.tc@mail.scut.edu.cn
Youguo Pi
College of Automatic Science & Engineering South China University of Technology Guangzhou PR 510641, China auygpi@scut.edu.cn

Abstract
A spam detection method, based on cognitive pattern recognition, had been proposed. The connection between Email category and cognition of Email user interest within life and work, had been analyzed. Under the guidance of cognitive pattern recognition theory, the mechanism of spam detection, based on intelligent cognition of Email user interest within life and work, had been discussed. Then the spam detection algorithm and its concrete implementation was given. Experimental results demonstrate that the spam detection algorithm has a good learning ability, scalability, and a good ability to achieve high recognition accuracy

A New Algorithm for Predicting Future Actions in Plan Recognition
Jianwei Zhang, Zengyu Cai, Yong Gan, Baowei Zhang, Lei He
Plan recognition is useful in many fields. It is significant to develop efficient recognition algorithms. In this paper, the event relations in plan recognition were deliberatively studied, and a new plan recognition algorithm to predict future actions was presented. The algorithm is based on plan knowledge graph and it integrates the bottom-up and top-down methods to construct solution graph. The algorithm is more powerful and simpler, comparing with other algorithms. The experimental results show that the algorithm is linear-time with the domain knowledge.

The expert system of product design based on CBR and GA

Lai Chaoan
South China University of Technology
School of Business Administration
Guangzhou, Guangdong, 510640, China
chalai@scut.edu.cn

Abstract
This paper presents a simultaneous optimization method of a case-based reasoning (CBR) system using a genetic algorithm (GA) for product designing. Prior research proposed many hybrid models of CBR and the GA for product design. However, those models were not good at aiding at creative designing. In this study, CBR and GA combine with a algorithm process for simulation of directed similarity association according to human being’s thought models. Experimental results show that the new hybrid model outperforms other conventional approaches for creative design.
Keywords - Intelligent design; simultaneous optimization; Genetic Algorithms; Case-Based Reasoning

An Efficient Algorithm for Scheduling Problem with Batching and Common Due Window

Hongluan Zhao1 Guojun Li2 Jiqiang Wang2,4 Guoyong Han1
1 School of Computer Science and Technology, Shandong Jianzhu Univ., Jinan, China
2 School of Mathematics and System Science, Shandong Univ., Jinan, China
3 Computational Systems and Biology Lab., Department of Biochemistry and Molecular Biology The Univ. of Georgia, USA
4 School of Statistics and Mathematics, Shandong Finance Inst., Jinan, China
Email address: hongluanzhao@163.com, hlzhao@sdjzu.edu.cn

Abstract
Jobs share a common due window and belong to distinct families with
sequence-independent setup tasks on a single machine. The window location and size are decision variables with linear penalties. Our objective is to find a schedule minimizing the sum of the weighted number of early and tardy jobs, together with the determination cost of the due window. Following several properties of an optimal schedule, a polynomial algorithm is firstly proposed and range it to P-problem. 

**Keywords:** Scheduling; Due window; Family; Early; Tardy

---

**Chinese Keyword Extraction Based on N-gram and Word Co-occurrence**

Hui Jiao  
Department of Precision Instruments and Mechanology, Tsinghua University, Beijing 100084, China  
jiaoh04@mails.tsinghua.edu.cn  
Qian Liu  
Department of Precision Instruments and Mechanology, Tsinghua University, Beijing 100084, China  
liuqian00@mails.tsinghua.edu.cn  
Hui-bo Jia  
State Key Laboratory of Precision Measurement Technology and Instruments, Beijing 100084, China  
jiahb@mail.tsinghua.edu.cn

**Abstract**

This paper presents a new kind of Chinese text encoding method based on Chinese word, and establishes a new Chinese document format which deals with the automatic segmentation issue. This method makes word the smallest information unit. Chinese text analysis does not rely on segmentation by the method. On this word platform, N-gram and word co-occurrence statistical analysis are combined to carry out Chinese keyword extraction experiment. Firstly, candidate keywords are extracted with bi-gram model. Then, a set of co-occurrences between every word in bi-grams and frequent words is generated. Cooccurrence distribution shows importance of every word. According to the analysis result, keywords are chosen from bi-grams. This algorithm applies to a single document without using a corpus, and experimental results are satisfying.
Knowledge Mining for Web Business Intelligence platform and its sequence knowledge model

SHEN Jie
Yangzhou University,
Yangzhou City,
Jiangsu Province, China,
shenjie@yzu.edu.cn

XU Fayan
Yangzhou University,
Yangzhou City,
Jiangsu Province, China
xfyxfp@163.com

WEI Liuhua
Yangzhou University,
Yangzhou City,
Jiangsu Province, China
for_happy@sohu.com

BI Lei
Yangzhou University,
Yangzhou City,
Jiangsu Province, China
Bilei_518@163.com

HE Kun
Yangzhou University,
Yangzhou City,
Jiangsu Province, China
aiyia@163.com

SUN Rongshuang
Yangzhou University,
Yangzhou City,
Jiangsu Province, China
frost0412@163.com

Abstract

The everchanging market information makes the traditional information collection and the way for using it unfitted for enterprises' business requirements. Knowledge Mining for Web Business Intelligence (KB4WBI) platform is put forward in this paper, and online Web knowledge acquisition and knowledge semantics management are realized. Since Web business information has evident time effectiveness and contextrelated characteristic, great emphasis is placed on the research of Web sequence knowledge representation model of ontology evolution. Compared to the current methods, this platform comprehensively considers the real time characteristic and semantic attributions of Web knowledge, improves the knowledge precision and utility, and lays the basis of Web business intelligence.
Multi-Objective Evaluation Strategy for Evolvable Analog Circuit

XIA Xue-wen
School of Computer, Wuhan University
Wuhan Louyu Road, 430079, China

LI Yuan-xiang
State Key Laboratory of Software Engineering
Wuhan Louyu Road, 430072, China

Abstract
The researches of Evolvable hardware (EHW) have obtained much attention during the past decade. An effective evaluation-function is a crucial problem while searching a correct circuit. The emphasis of majority researchers’ experiments, however, was only circuit’s function, and little attention had been paid to circuit’s validity and practicality such as its complexity and stability. In this paper, an evaluation strategy based on multi-objective is proposed during the progress of evolvable analog circuit, in which many factors have been taken into account during the experiments besides the function. The results of experiments in the paper and practical lessons have indicated that only a circumspect circuit could meet the practical needs.

Application of Genetic Algorithms to Computing Unit Hydrograph

Li Hongyan Zhang Yonggen Bao Xinhua
Hydrology and Water resources Department,
College of Environment and Resources, Jilin University
6 Ximinzhu Street, Changchun, China, 130061
lihongyan@jlu.edu.cn, baoxh@jlu.edu.cn, globeman168@163.com

Abstract
In this paper, genetic algorithms and Collins method (GA-Collins) are integrated to compute unit hydrograph (UH). On the basis of entropy principle and distribution function, this method regards hydrological system of the basin as a generalized set, simulates the UH of the runoff-routing with distribution function, searches the distribution function parameters with genetic algorithms (GAs), and the initial UH (IUH) can be obtained. Then, the Collins method is used to complete the final UH. According to the comparative analysis of actual case study, the GA-Collins method has a more precise result than the other methods and it can also reveal the runoff-routing rule.

A Novel Assembly Evolutionary Algorithm for n-Queens Problem
Abstract
Individuals in nowadays evolutionary algorithms for n-queens problem do not satisfy some basic constraint conditions. Motivated by self-assembly computing, a novel assembly evolutionary algorithm for n-queens problem is presented. Each individual is made up of assembly-parts, assembly-seeds and status information. Some important notions and rules regarding the novel assembly evolutionary algorithm are discussed. Experimental results show that the algorithm finds a solution faster than other latest evolutionary algorithms.

A Three-dimensional Encoding Genetic Algorithm for Job Shop Scheduling

Hongli Yin
School of Computer Science and Information Technology, Yunnan Normal University, Kunming, Yunnan Province, China
hongli_yin@163.com
Enliang Hu
School of mathematics, Yunnan Normal University, Kunming, Yunnan Province, China
huenliangyn@21cn.com
Yongming Wang and Nanfeng Xiao
School of Computer Science and Engineering, South China University of Technology, Guangzhou, Guangdong Province, China
yymm_wang@163.com
Yanrong Jiang
School of Computer, Guangdong University of Technology, Guangzhou, Guangdong Province, China
yrjiang@163.com

Abstract
In so many combinatorial optimization problems, Job shop scheduling problems have earned a reputation for being difficult to solve. GA has demonstrated considerable success in providing efficient solutions to many non-polynomial-hard optimization problems. In the field of job shop scheduling, GA has been intensively researched, and there are nine kinds of methods were proposed to encoding chromosome to represent a solution. In this paper, we proposed a novel genetic chromosome encoding approach, in this encoding method, the operation of crossover and mutation was done in three-dimensional coded space. 5 selected benchmark problems were tried with the proposed three-dimensional encoding GA for validation and the results are encouraging.
Cooperative Algorithm for Multi-Agent Foraging Task Based on Modified Hawk-Dove Game
Yuehai Wang, Jie Liu
North China University of Technology
College of Information Engineering
Shijingshan Dist., Beijing, China
wangyuehai@ncut.edu.cn

Wei Meng
Beijing Forestry University
Dept. of Computer Science
35 Tsinghua, Haidian Dist., Beijing, China
hmxd@263.com

Abstract
Multi-agent foraging is a popular benchmark to verify the effectiveness of different cooperation algorithm. Markov game based approaches were wildly used although they could not select consistent equilibrium for the group.
Using evolutionarily stable strategy as optimal solution, we build a modified hawk-dove game model to simulate the interaction between agents, and then proposed a ponder-replicator algorithm to find certain consistent maximal reward equilibrium for the group. The simulation verified the efficiency of the proposed algorithm.

Automatic Test Data Generation Tool Based on Genetic Simulated Annealing Algorithm
Li Bin Li Zhi-Shu Chen Yan-Hong, Li Bao-Lin
School of Computer School of Computer School of Computer
University of sichuan University of sichuan University of sichuan
Chengdu 610064, China Chengdu 610064, China Chengdu 610064, China
rockli@163.net Lzshu5@yahoo.com.cn

Abstract
This paper presents an automatic test data generation tool that aims at generating test data dynamically by reducing the problem of test data generation to one minimizing function. The tool is composed of three parts: program instrumentation module; test path generation module and test case generation module. In order to enhance the computational efficiency, we makes some improvements on the encoding, crossover probability and annealing gene of the genetic simulated annealing algorithm (GASS), and then use the results to generate the test data on the program instrumentation. Experimental results show this approach has better effect.
An Efficient Evolutionary Algorithm for A Kind of Nondifferentiable Nonlinear Bilevel Programming
Dalian Liu and Dong Chen
Department of Basic Course Teaching
Beijing Union University, Beijing, 100101, China
ldlucky@sina.com

Abstract
A special kind of nonlinear bilevel programming problems (nonlinear BLPP in short) is transformed into an equivalent single objective nonlinear programming problem. To solve the equivalent problem effectively, we first design a fitness function based on entropy function. By using this fitness function, we not only can decrease the leader’s objective value, but also can force the infeasible solutions moving towards the feasible region, and improve the feasible solutions gradually. Then an effective crossover operator is used to generate high quality offspring. Based on these, a new evolutionary algorithm for nonlinear BLPP is proposed. Finally, simulations on several benchmark problems are made and the results demonstrate the effectiveness of the proposed algorithm.

A New Multi-objective Fully-informed Particle Swarm Algorithm for Flexible Job-shop Scheduling Problems
Zhao-hong Jia1, 2, Hua-ping Chen1, Jun Tang2
1Department of Information Management and Decision Science
University of Science and Technology of China
Hefei 230026, China
2Key Lab. of Intelligent Computing and Signal Processing, Ministry of Education
Anhui University
Hefei 230039, China
zhjia@mail.ustc.edu.cn, hpchen@ustc.edu.cn, tangjun@ahu.edu.cn

Abstract
A novel Pareto-based multi-objective Fullyinformed Particle Swarm algorithm (FIPS) is proposed to solve flexible job-shop problems in this paper. Firstly, the population is ranked based on Pareto optimal concept. And the neighborhood topology used in FIPS is based on the Pareto rank. Secondly, the crowding distance of individuals is computed in the same Pareto level for the secondary rank. Thirdly, addressing the problem of trapping into the local optimal, the mutation operators based on the coding mechanism are introduced into our algorithm. Finally, the performance of the proposed algorithm is demonstrated by applying it to several benchmark instances and comparing
the experimental results.

Fuzzy-Dominance and its Application in Evolutionary Many Objective Optimization
Gaoping Wang and Huawei Jiang
School of Information Science and Engineering, Henan University of Technology, Zhengzhou 450052, China
wgp888888@163.com

Abstract
This paper studies the fuzzification of the Pareto dominance relation and its application to the design of Evolutionary Many-Objective Optimization algorithms. A generic ranking scheme is presented that assigns dominance degrees to any set of vectors in a scale-independent, nonsymmetric and set-dependent manner. Different fuzzy-based definitions of optimality and dominated solution are introduced. The corresponding extension of the Standard Genetic Algorithm, so-called Fuzzy-Dominance GA (FDGA), will be presented as well. To verify the usefulness of such an approach, the approach is tested on analytical test cases in order to show its validity.

A New Particle Swarm Optimization Algorithm with Random Inertia Weight and Evolution Strategy
Gao Yue-lin 1,2
1Research Institute of Information and System Science, North National University, Yin Chuan 750021, China
2School of Economics and Finance, Xi’an Jiaotong University, Xi’an 710049, China
gaoyuelin@263.net
Duan Yu-hong 3
3School of Mathematics and Computer, Ningxia University, Yin Chuan 750021, China
duanyuhong2005@163.com

Abstract
The paper gives a new particle swarm optimization algorithm with random inertia weight and evolution strategy (REPSO). The proposed random inertia weight is using simulated annealing idea and the given evolution strategy is using the fitness variance of particles to improve the global search ability of PSO. The experiments with six benchmark functions show that the convergent speed and accuracy of REPSO is significantly superior to the one of The PSO with linearly decreasing inertia weight LDW-PSO.
A Particle Swarm Optimizer with chaotic Self-feedback for Global Optimization of Multimodal Functions
Zhang Huidang
College of Marine, Northwestern Polytechnical University, Xi’an, China
huidang@haut.edu.cn
He Yuyao
College of Marine, Northwestern Polytechnical University, Xi’an, China
heyyao@nwpu.edu.cn

Abstract
This paper proposes an improved particle swarm optimization utilizing Iterative Chaotic Map with Infinite Collapses (ICMIC) perturbations (ICMICPSO) for global optimization of multimodal functions. The chaotic perturbation generated by the ICMIC is incorporated into the particle’s velocity updating rule to make the particles have a larger potential space to fly. With the coefficient of chaotic perturbation decaying, the dynamics of ICMICPSO algorithm is a chaotic dynamics first and then a steepest descent dynamics. The proposed ICMICPSO method as hybrid optimization is tested on several widely used multimodal functions. Numerical results are compared with that of some other Chaotic PSO methods available in the usual literature. The performance studies demonstrate that the effectiveness and efficiency of the proposed ICMICPSO approach are comparably to or better than that of the other CPSO variants in this paper.

Quantum-inspired Swarm Evolution Algorithm
Huang Yourui Tang Chaoli Wang Shuang
Anhui University of Science and Technology Huainan 232001, China
hyr628@163.com

Abstract
This paper proposes a novel quantum swarm evolution algorithm, called a quantum-inspired swarm evolution algorithm (QSEA), which is based on the concept and principles of quantum computing. The proposed algorithm adopts quantum angle to express Q-bit and improved particle swarm optimization to update automatically. After the quantum-inspired swarm evolution algorithm is described, the experiment results on the benchmark functions are given to show its efficiency.

CMAC Neural Network Model Based on Compose Particle Swarm Optimization
Man Chun-tao
School of Automation
Harbin University of Science and Technology
Harbin 150080, China
mct68@hrbust.edu.cn
Wang Su-ju
School of Automation
Harbin University of Science and Technology
Harbin 150080, China
Wangsuju_@126.com
Zhang Li-yong
School of Measurement-Control Tech &
Communications Engineering
Harbin University of Science and Technology
Harbin 150080, China

Abstract
In order to improve the training precision of traditional CMAC model, this paper suggests a new
CMAC model, whose weights are trained by composite particle swarm optimization. Traditional model’s
weights are trained by LMS algorithm, which can’t learn approaching function’s reciprocal and unfitted
nonlinear hyperplane. The new method makes full use of the disadvantages of swarm intelligence, and
improves above disadvantages effectively.

A Novel Method for Solving Fuzzy Programming Based on hybrid
Particle Swarm Optimization
Zhenkui Pei 1,2, Shengfeng Tian and Houkuan Huang 11
1 School of Comp.& Information Technology,Beijing Jiaotong University,Beijing 100044, P.R.China
2 College of Comp. & Comm. Engineering,China University of Petroleum, Dongying 257061, P.R.China
peizhk@hdpu.edu.cn

Abstract
Fuzzy programming offers a powerful means of handling optimization problems with fuzzy parameters.
Fuzzy programming has been used in different ways in the past. The particle swarm optimization (PSO) has
been applied successfully to continuous nonlinear constrained optimization problems, neural network, etc.
But we have not been found to use PSO for fuzzy programming in literature. In this paper, we combined
with fuzzy simulation, neural network and PSO to produce a hybrid intelligent algorithm. Based on this
hybrid intelligent algorithm, we introduced for solving fuzzy expected value models. Some numerical
examples are given to illustrate the algorithm is effective and powerful.
Using Expert’s Knowledge to Build Bayesian Networks

Hu Xiao-xuan,
School of Management
Hefei University of Technology,
Hefei, China, 230009
huxiaoxuan@vip.sina.com
Wang Hui
School of Management
Hefei University of Technology,
Hefei, China, 230009
wang_hui_mail@163.com
Wang Shuo
School of Management
Hefei University of Technology,
Hefei, China, 230009
wangshuo@ah.edu.cn

Abstract
Building Bayesian networks is considered to be difficult and time-consuming work. Researchers usually learn networks from data. However, it is of low efficiency because of the huge search space. Since Bayesian networks represent the causal relationships among random variables, domain experts can build Bayesian networks according to their knowledge and experience. In this paper, we develop a method to build Bayesian networks from experts. We use some knowledge elicitation tools to obtain high-quality knowledge, and ensure the validity of networks by combing knowledge from multiple experts. The experimental result indicates that this method can improve the modeling efficiency of Bayesian networks.

Cooperative Q Learning Based on Blackboard Architecture

Yongming Yang, Yantao Tian and Hao Mei
School of Communication Engineering, Jilin University, Changchun, China
yongmingyang@sohu.com, tianyt@jlu.edu.cn

Abstract
This paper presents cooperative Q learning based on the blackboard architecture. The learning process is executed at the blackboard architecture making use of all the robots in the training scenario to explore the learning space and collect experiences. Three kinds of Q value update strategies are proposed in order to deal with variation of Q value that may happen in the multi-robot learning scenario. Simulation experiments verify that the learning process converges faster and the control strategy obtained has better performance.
TD(\(\lambda\)) Optimization of Imperfect Information Game’s Evaluation Function

Xuan Wang, Zhaoyang Xu
Intelligence Computing Research Center
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen, 518055, China
wangxuan@insun.hit.edu.cn

Abstract
This paper studies a machine learning method – TD (\(\lambda\)), a kind of Temporal Difference learning in the evaluation function of imperfect information games. We combine TD (\(\lambda\)) with Monte Carlo sampling to solve a typical imperfect information game - Junqi. Static linear method and TD (\(\lambda\)) approach are compared. The static linear evaluation is used with all its parameters unchanged, whereas the TD (\(\lambda\)) approach updates its parameters according to the actual outcomes. It is demonstrated that this algorithm led to a population of intelligent agents successful playing Junqi against human beings with the search depth of 4.

Parallel Kriging Interpolation for Modeling of Stratified Stratum
Peng Chen1,2
1. Digital Engineering and Simulation Centre, Huazhong University of Science & Technology, 430074 Wuhan, China
2. College of Electrical Engineering & Information Technology, Three Gorges University, 443002 Yichang, China.
Email: febird@eyou.com
Cheng Wang, Bo Ren*
Digital Engineering and Simulation Centre, Huazhong University of Science & Technology, 430074 Wuhan, China
Email: wangch@mail.hust.edu.cn, popoxx@126.com

Abstract
Kriging is an advanced interpolation technique and often used to model the three-dimension stratified stratum, but too much time are needed for large area with a plenty of layers. In order to improve the speed of interpolation and visualization of stratified stratum, a novel parallel ordinary Kriging interpolation with medium granularity is presented. In the parallel computing environment established by PCs with Windows2000 OS, the parallel algorithm based on MPI is adopted to setup a 3D stratum model. The statistic data show that the parallel Kriging interpolation can save the computing time efficiently and has a good scalability.
A Robust Formulation for Support Vector Regression
Ping Zhong
College of Science
China Agricultural University
Beijing 100083, China
pingsunshine@yahoo.com.cn

Abstract
This paper investigates a new support vector regression model in which the observed data are corrupted with noise. We present a second-order cone programming formulation for designing robust regression which can handle uncertainty in data. Empirical results are included to show that the robust model is superior to the standard model.

A Parallel Ant Colony Optimization for Multi-depot Vehicle Routing Problem
Yao, Jinbao
School of Civil Engineering & Architecture
Beijing Jiaotong University
Beijing 100044, China
E-mail:y_jinbao72@126.com
Yao, Baozhen
Purchasing and Sourcing Dept.
Ryobi Dalian Machinery CO., LTD
Dalian 116600, China
E-mail: ybzhyb@163.com

Abstract
This paper presents a method for solving the multi-depot vehicle routing problem (MDVRP). Due to different vehicle capacities among companies, a mathematical formulation, which considers the variable costs and the vehicles' fixed costs simultaneously, is given. Since the inherent complexity of the MDVRP makes it difficult to be solved even for a relatively small scale, an improved ant colony optimization with a new strategy to update the increased pheromone (Ant-Weight) is developed for the MDVRP. Then, a parallelization strategy for ant colony optimization is used to increase computational efficiency. Finally, the proposed algorithm is examined with the data of Wuhu city in China. The results indicate that this method performs well in terms of the solution quality and run time consumed.

Mathematical Analysis of Swarm Robots Foraging Based on Division Strategy
Yongming Yang, Yantao Tian, Xiyue Qi and Xu Zhao
School of Communication Engineering, Jilin University, Changchun, China
yongmingyang@sohu.com, tianyt@jlu.edu.cn

Abstract
The mathematical model of swarm robotic system can predict the collective behavior of the system,
analyze the effect that individual characteristic has on the collective behavior, which can guide the improvement of individual control strategy. The mathematical model of foraging based on division strategy is proposed, which is composed of a series of coupled differential rate equations. The mathematical model is used to analyze the time evolution of the number of robots in different states and the number of undelivered foods. The performance of foraging based on homogeneous strategy and division strategy is investigated utilizing mathematical models.

A Phylogenetic Tree Constructing Algorithm Based on Ant Colony Optimization

This research was supported in part by the Chinese National Natural Science Foundation under grant No. 60673060, Natural Science Foundation of Jiangsu Province under contract BK2005047, and the Jiangsu Foundation for Graduated Students Scientific Research.

Ling Chen
Department of Computer Science
Yangzhou, University
Yangzhou, China
National Key Lab of Novel Software Tech
Nanjing University
Nanjing, China
lchen@yzcn.net

Ling Qin
Institute of Information Science and Technology
Nanjing University of Aeronautics and Astronautics
Nanjing, China

Lingjun Zou
Department of Computer Science
Yangzhou University
Yangzhou, China

Abstract

An algorithm for constructing phylogenetic tree based on ant colony optimization (Ant-PTC) is presented. To take full advantage of the strong optimization ability of ant colony algorithm, a graph is built using all the input species according to their distances. The pheromone on the edges is adaptively updated when the ants travel on the graph. Then the graph is modified by omitting some edges with less pheromone. Clusters of species extracted from the connected components of the graph are used to construct the phylogenetic tree progressively. Experimental results show that our algorithm Ant-PTC can obtain higher classification accuracy, higher convergence speed than other similar method.

Stable Neighborhood Preserving Embedding
Jing Wang  
the School of Information Science and Technology  
Huaqiao University  
Quanzhou, 362021, P. R. china  
wroaring@yahoo.com.cn

Abstract
The problem of dimensionality reduction arises in many fields of information processing. In this paper, we propose a novel linear dimensionality reduction algorithm called Stable Neighborhood Preserving Embedding (SNPE). It represents the local geometry by using multiple linearly independent weight vectors that are approximately optimal, and then finds an optimal embedding in the low-dimensional space which is linearly mapped from the high-dimensional space to preserve the local geometry exploited by multiple weights. Numerical examples are given to show the improvement and efficiency of the proposed algorithm.

A Shot Clustering Based Algorithm for Scene Segmentation
Xuejun Wang  
Jilin University  
Changchun China  
xjwang@jlu.edu.cn  
Shigang Wang  
Jilin University  
Changchun China  
Wangshigang@vip.sina.com.cn  
Hexin Chen  
Jilin University  
Changchun China  
chx@jlu.edu.cn  
Moncef Gabbouj  
Tampere University of Technology  
FIN-33101 Tampere  
Moncef.Gabbouj@tut.fi

Abstract
A scene segmentation method utilizing both visual features and motion features of video is presented in this paper. Not only the visual similarity but also the motion consistency of shots within a scene is considered in clustering shots into scenes. In addition, a method to merge the over-segmented scenes is presented also. And the experimental results show the effectiveness of the proposed algorithms.
Visual Mouse: SIFT Detection and PCA Recognition
Hailing Zhou\textsuperscript{1,2}, Lijun Xie\textsuperscript{1,2}, Xuliang Fang\textsuperscript{1,2}
\textsuperscript{1}College of Computer Science, Zhejiang University, Hangzhou, 310027, China
\textsuperscript{2}Center for Engineering and Scientific Computation, Zhejiang University, Hangzhou, 310027, China
hailing.zhou@hotmail.com, zdxlj@zju.edu.cn, fxlzju@gmail.com

Abstract
The paper presents the Visual Mouse (VM), a novel and simple system for interaction with displays via hand gestures. Our method includes detecting bare hands using the fast SIFT (Scale-Invariant Feature Transform) algorithm saving long training time of the Adaboost algorithm, tracking hands based on the CAMShift algorithm, recognizing hand gestures in cluttered background via Principle Components Analysis (PCA) without extracting clear-cut hand contour, and defining simple and robustly interpretable vocabularies of hand gestures, which are subsequently used to control a computer mouse. The system provides a fast and simple interaction experience without the need for more expensive hardware and software.

An Efficient Visual Tracking Method for Multiple Moving Targets
Xiaohui Chen
Nanjing University of Posts and Telecommunications
College of Automation
Nanjing, Jiangsu Province, China
jkdcxh@yahoo.com.cn
Lyudmila Mihaylova
University of Bristol
Department of EEE
Woodland Road, Bristol BS8 IUB, UK
Mila.mihaylova@bristol.ac.uk
David R Bull
University of Bristol
Woodland Road, Bristol BS8 IUB, UK
Department of EEE
David.Bull@bristol.ac.uk
Nishan Canagarajah
University of Bristol
Department of EEE
Woodland Road, Bristol BS8 IUB, UK
Nishan.Canagarajah@bristol.ac.uk

Abstract
An efficient algorithm of the edge detection according to integrating the edge gradient with the average filter is proposed, which can significantly reduce sensitivity of the background subtraction method to noise and illumination. Taking into account the features of the target such as colour, size, etc., a new modified nearest neighbour (NN) algorithm for data association using the target features is designed. A designed interacting multiple model (IMM) filter is utilized to track the maneuvering target motion, i.e.
the feature point (called the centroid of the target) motion of the target. The algorithms are validated via an example with natural video sequences. The results show the algorithms are performances and validity for visual tracking. In complex environment, the algorithm can still work well.

Blind Non-independent Image Separation Based on Independent Component Analysis

Wu Guo
ATR Laboratory, NUDT, Changsha, Hunan, China
guowu2000@yahoo.com.cn

Peng Zhang
ATR Laboratory, NUDT, Changsha, Hunan, China
zp80272@yahoo.com.

Runsheng Wang
ATR Laboratory, NUDT, Changsha, Hunan, China
rswang@nudt.edu.cn

Abstract

Blind separation of mixture images which mutually independent has been solved efficiently by some independent component analysis (ICA) methods. But these methods often failed in case of the source images are statistically non-independent. A novel fixed-point FastICA algorithm based on complexity pursuit is presented in this paper and with the algorithm the mixed images which not mutually independent can be separated successfully. Experimental results demonstrate the efficiency of our proposed method.

An Algorithm for Removing Facial Makeup Disturbances Based on Clifford Algebras

The research is supported by the National Science Foundation of China (No.60576055)
The main goal of the paper is to show that Clifford algebras can be used to solve problems of removing facial makeup disturbance. After simulation and practical application experiments, the algorithm is a natural and effective manner.

---

Super Resolution of 3D Surface Texture
Junyu Dong
College of Information Science and Engineering, 
dongjunyu@ouc.edu.cn
Zuozen Liu
College of Information Science and Engineering, 
liuzzozen@163.com
Jing Ren
College of Information Science and Engineering
Ocean University of China

Abstract
Real-world surface textures commonly consist of a spatial variation of reflectance properties combined with rough surface geometry, called 3D surface texture. Variation of illumination can produce dramatic changes their appearance. While previous work on super resolution pays great attention to 2D images, this paper proposes an inexpensive method for super resolution on 3D surface textures. First, four images under different illumination angles are captured for each sample surface texture, from which the surface gradient maps and the albedo map are extracted by Photometric Stereo. Then the surface gradient and albedo maps and three selected original images, which represent 3D surface texture, are processed by a modified 2D Example-based super resolution method to generate result representation sets with higher resolution. Finally, relight surface representations to generate high resolution texture images under any different illumination conditions. Experimental results show that this method provides more fine details compared to interpolation techniques.

---

Models of Vehicle Speeds Measurement with a Single Camera
He Zhiwei, Liu Yuanyuan, Ye Xueyi
Dept. of Communication Eng., Hangzhou Dianzi University
No.2 Street, Xiaasha High-education Zone, Hangzhou, China
{zwhe, liuyuanyuan, xueyiye}@hdu.edu.cn

Abstract
The rapid development of hardware technology make it possible for computers or even micro-computers to
handle the problem of traffic information gathering utilizing image/video processing and pattern recognition. In order to measure the speed of a vehicle, several models are proposed in this paper. Firstly, the background subtraction method with a proper background updating model is used to detect the moving vehicle, whose position in the image is then traced with the obtained distinct features. The real position of the vehicle in the world coordination system corresponding to the traced pixel position can then be calculated according to one of the two proposed imaging models in the paper. With the real distance and the time period between successive image frames obtained, the speed of a vehicle can then be calculated easily. The proposed models are used in an embedded traffic information gathering system and results show the convenience and the high accuracy of the proposed methods.

A Relevance Feedback Algorithm Based On SVM Model’s Dynamic Adjusting For Image Retrieval
Yihua Zhou1, Weimin Shi1,Lijuan Duan1, Cuiying Niu2
1College of Computer Sci and Tech,Beijing University of Technology,Beijing 100022,China
2Beijing Longdachengxin Project Management Co.,Ltd,Beijing 100021, China
E-mail:{zhouyh,shiweimin,ljduan}@bjut.edu.cn, niu_cy@163.com

Abstract
A fixed SVM model setting is not suitable for the evolvement of the pattern of user’s interest. In this paper a relevance feedback algorithm based on SVM model’s dynamic adjusting for image retrieval is presented. In this algorithm, there is no need to fix the model’s parameters beforehand, and the parameters of SVM model will be automatically adjusted corresponding to the changing of the training samples. Experimental results show the proposed algorithm outperformed other algorithms with fixed model’s parameter.

Application of Image Texture for Discrimination of Tea Categories Using Multi-spectral Imaging Technique and Support Vector Machine
Di Wu
College of Biosystems Engineering and Food Science, Zhejiang University
268 Kaixuan Road, 310029, Hangzhou, China
ilkb8mvp@yahoo.com.cn
Xiaojing Chen
Department of Physics, Xiamen University
South of Simin Road, 361005, Xiamen, China
Chenxj9@163.com
Yong He
College of Biosystems
Engineering and Food
Science, Zhejiang University
268 Kaixuan Road, 310029,
Hangzhou, China
yhe@zju.edu.cn

Abstract
This study investigated multi-spectral imaging technique as a rapid method to discriminate the tea category. Tea was spread over the whole images. The images for each sample were captured using a red, near infrared and green channel multi-spectral camera. 320 images were obtained. Three texture features were obtained through the entropy of three channels and then set as the input variables for pattern recognition. Principal components analysis (PCA) and least squares-support vector machine (LS-SVM) were used for the pattern recognition. The cluster ability of PCA cluster plot was not good while the discrimination rate of LS-SVM model was 97.5%. We used one channel image to subtract another one, and six images of each sample were obtained. Then six new entropy values were obtained. The cluster ability of the new PCA cluster plot is better than the old one and the discrimination rate of LS-SVM model was 100%. It is concluded that multi-spectral imaging technique can identify categories of green tea fast and non-destructively.

Binary Trademark Image Retrieval Using Region Orientation Information
Entropy
Cai-kou Chen, 2 Qiang-qiang Sun
Jing-yu Yang
1Information Engineering College, Yangzhou University, Yangzhou, China, 225009
2College of Computer Science and Technology, Nanjing University of Science and Technology,
Nanjing, China, 210094
yzcck@126.com (C.K. Chen), sunqiang6417@163.com (Q.Q. Sun)

Abstract
This paper presents a new trademark image retrieval method based on the region orientation information entropy. In the first stage, image is rotated according to principal orientation, and the object region in the rotated image is extracted. Then, the object region is partitioned into a lot of sub-blocks. In the third stage, the information entropy of each partitioned region is computed, which construct a feature vector for describing the shape of the image. Finally, the Euclidean distance is adopted to measure the similarity between the images based on the feature vector of each image obtained. Experiments performed on a database containing more than 2,000 trademark images show that the region orientation information entropy keeps good invariance under rotation, translation, scale and the retrieved results satisfy human visual perception very well.
Frequent closed informative itemset mining
Huaiguo Fu, M’iche’al ´O Foghl´u, Willie Donnelly
Telecommunications Software & Systems Group
Waterford Institute of Technology, Waterford, Ireland
{hfu, mofoghlu, wdonnelly}@tssg.org

Abstract
In recent years, cluster analysis and association analysis have attracted a lot of attention for large data analysis such as biomedical data analysis. This paper proposes a novel algorithm of frequent closed itemset mining. The algorithm addresses two challenges of data mining: mining large and high dimensional data and interpreting the results of datamining. Frequent itemset mining is the key task of association analysis. The algorithm is based on concept lattice structure so that frequent closed itemsets can be generated to reduce the complexity of mining all frequent itemsets and each frequent closed itemset has more information to facilitate interpretation of mining results. From this feature, the paper also discusses the extension of the algorithm for cluster analysis. The experimental results show the efficiency of this algorithm.

Data Extraction from Deep Web Pages
Jufeng Yang Guangshun Shi Yan Zheng Qingren Wang
Institute of Machine Intelligence
Nankai University, 300071 Tianjin, China
richard_nkimi@yahoo.com.cn {gssshi, yanzheng, qrwang}@imi.nankai.edu.cn

Abstract
In this paper, we propose a novel model to extract data from Deep Web pages. The model has four layers, among which the access schedule, extraction layer and data cleaner are based on the rules of structure, logic and application. In the experiment section, we apply the new model to three intelligent systems, scientific paper retrieval, electronic ticket ordering and resume searching. The results show that the proposed method is robust and feasible.

Web pages Classification Using Domain Ontology and Clustering
Sima Soltani
Intelligent Systems Laboratory
Amirkabir University of Technology
Tehran, Iran
Sima.soltani@gmail.com
Ahmad Abdollahzadeh Barforoush
Intelligent Systems Laboratory
Amirkabir University of Technology
Tehran, Iran
ahmadaku@aut.ac.ir

Abstract
Transferring the current Websites to Semantic Websites, using ontology population, is a research area within which classification has the main role. The existing classification algorithms and single level execution of them are insufficient on web data. Moreover, because of the variety in the context and structure of even common domain Websites, there is a lack of training data. In this paper, we had three experiences: 1- using information in domain ontology about the layers of classes to train classifiers (layered classification) with improvement up to 10% on accuracy of classification. 2- experience on problem of training dataset and using clustering as a preprocess. 3- using ensembles to benefit from both two methods. Beside the improvement of accuracy from these experiences, we found out that with ensemble we can dispense with the algorithm of classification and use a simple classification like Naive Bayes and have the accuracy of complex algorithms like SVM.
A Multi-agent based Autonomic Management Architecture for Large-scale Server Clusters
Zhenghua Xue, Xiaoshe Dong, Weizhe Liu, Junyang Li, Shihua Liao
Department of Computer Science and Technology, Xi’an Jiaotong University, Xi’an, China
E-mail: zhenghua_xue@163.com, xsdong@mail.xjtu.edu.cn

Abstract
As the size of the server cluster increases, management of clusters has been a daunting task. Traditional management architecture of cluster systems fails in providing efficient management as the scale of cluster increases. In this paper, a novel management architecture of a large-scale cluster system, called cooperation-oriented hierarchical autonomic architecture (CHAA), has been proposed to achieve an efficient management. We employed multi-agents to construct CHAA. Considering that the intrusion caused by bidding increases dramatically when the number of agents is large, we proposed hierarchical Contract Net Protocol (HCNP) to relieve the overhead. Generalized partial global planning (GPGP) has been introduced into CHAA to enable agents recognize their potential interrelationship and it has been combined with HCNP as the cooperation method of agents in CHAA. We made performance measurement on the traditional management architecture and CHAA, and the results showed that CHAA is a light weight management architecture which promises good scalability.

Quantum Varying Deficit Round Robin Scheduling Over Priority Queues
Weiming Tong, Jing Zhao
Department of Electrical Engineering and Automation
Harbin Institute of Technology
Harbin, 150001 P.R. China
dianqi@hit.edu.cn, zhaojing8006@163.com

Abstract
At the time of this paper writing, all scheduling algorithms are looking for tradeoffs between low complexity, low latency, and fairness. The priority queuing (PQ) scheduling can meet the requirements of real-time applications but is not good at fairness. Sorted priority algorithms like WFQ achieve better results in latency and fairness by calculating priorities dynamically at the cost of work complexity up to O(log(n)) (where n is the number of queues); frame-based schemes such as DRR, resolve the fairness variable length packets transmitting with O(1) work complexity, but sacrifice latency performance. In this paper, we break off the relationship between the duration packet stays in queue and the number of the queue having been served. We set the priority for each queue, insert packets into different queues according to their real-time needs. Then over all of them, we run Quantum Varying DRR algorithm we proposed, which keeps not only all advantages DRR has, but provides better low latency than DRR. It also achieves the fairness of Max (Max is the longest size of packets coming from all input links.). Analytical results and simulations verify all these characteristics.

iRBO: Intelligent Role-Based Object for Object-based Storage Device
Yinliang Yue, Fang Wang*, Dan Feng
School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan, China
Key Laboratory of Data Storage System, Ministry of Education
yylcshust@163.com, wangfang@mail.hust.edu.cn, dfeng@hust.edu.cn

Abstract
The intelligence of Object-based Storage Device (OSD) is crucial for an autonomous Object-based Storage Device Cluster (OSDC) and the intelligence of OSD depends on the intelligent Objects. Traditionally, object defined in OSD-2 draft is the container of data and attributes (such as user object) and lacks for intelligence which is the basis of an intelligent OSD. Consequently, the construction of an intelligent object will catch the fancy of most researchers. The task of traditional object is similar to each other and some special tasks aren’t taken by the specific objects. Some specific objects are urgent needed to be added into OSD for the special missions. This paper presents intelligent Role-Based Object (iRBO) for OSD. The construction of intelligent objects is proposed firstly. Methods, rules, trigger and feedback mechanism...
are introduced into object defined in OSD-2 draft, so an object is comprised of data, attributes, methods, rules, trigger and feed back mechanism. After the relationship among these six components is built up, the object is no longer passive but active. Then, the model of iRBO is discussed and some specific objects for special missions are introduced.

**L-Chord: Routing Model for Chord Based on Layer-Dividing**

Biqing Wang, Peng He

*College of Electrical Engineering and Information Technology, Information Technology Center, Three Gorges University, P.R.China*

w-bq@tom.com

**Abstract**

Chord is a kind of structured P2P network, but the routing table in Chord suffers serious information redundancy and it is not very efficient. Therefore, a routing model and algorithm implementation for Chord based on layer-dividing (L-Chord) is proposed. Simulation experiments show that L-Chord compresses the routing table length of most nodes into only ones so as to eliminate repetitious entries and reduce the average lookup path length. L-Chord coordinates lookup efficiency and routing table length well.

**Implementation and Performance Evaluation of an Adaptable Failure Detector for Distributed System**

Jingli Zhou, Guang Yang, Lijun Dong, Gang Liu

*College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan, 430074, China*

yangchgang@gmail.com

**Abstract**

Unreliable failure detectors have been an important abstraction to build dependable distributed applications over asynchronous distributed systems subject to faults. Their implementations are commonly based on timeouts to ensure algorithm termination. However, for systems built on the Internet, it is hard to estimate this time value due to traffic variations. In order to increase the performance, self-tuned failure detectors dynamically adapt their timeouts to the communication delay behavior added of a safety margin. In this paper, we propose a new implementation of a failure detector. This implementation is a variant of the heartbeat failure detector which is adaptable and can support scalable applications. In this implementation we dissociate two aspects: a basic estimation of the expected arrival date to provide a short detection time, and an adaptation of the quality of service. The latter is based on two principles: an adaptation layer and a heuristic to adapt the sending period of "I am alive" messages.

**An Adaptive Join Strategy in Distributed Data Stream Management System**

Xiaojing Li Yu Gu Dejun Yue Ge Yu

*College of Information Science and Engineering, Northeastern University, Shenyang 110004, China*

lxj_neu@126.com

**Abstract**

As data stream springs up in various areas, distributed data stream management systems are being paid more and more attention. In DSMS, join is one of the most common but complicated operators, and the efficiency of continuous queries may be influenced by join directly. This paper mainly studies the join operation over data stream located on two different sites in WAN. Firstly, data model, query model and cost model are defined, and then a simple direct-join strategy and a semi-join strategy are proposed, which are respectively ideal under certain conditions but can’t adapt to the variation of data stream. Finally, based on the analysis of the two strategies, an optimized adaptive join strategy is presented. The efficiency and flexibility of our strategy is proved by extensive experiments. Key words: distributed data stream management, continuous query, adaptive join.

**TopicOriented Search Model Based on MultiAgent**
Abstract

The users’ retrieval words are distinguished, judged, and classified by utilizing the intelligence character of agent, and the concept of topic derivation is introduced. Some subtopics, which are derived from the known topic, are submitted to the agent for searching, therefore, the retrieval results could be classified according to the topics and be convenient for user to choose. The test demonstrates that in combination the fixed topic and the topics were recommend, the knowledge warehouse is enriched for perfecting the procedure of topic derivation, the retrieval range is narrowed and the local memory is reduced.

A Formal Open Framework Based on Agent for Testing Web Applications
Huaikou Miao, Shengbo Chen, Zhongsheng Qian
School of Computer Engineering and Science, Shanghai University, Shanghai 200072, Chinahkmiao@shu.edu.cn, csb_hust@163.com, changesme@163.com

Abstract

This work employs and extends the Gaia methodology to design a formal open framework based on agent for automatically testing Web applications. In our framework, each test task corresponds to a role and the agent takes this role to achieve its test task or cooperates by interaction with other agent to finish the test task. The agent can not only join or leave agentsociety at will, but also take or release roles at runtime dynamically. Our framework can be extended easily by adding new roles to provide much more function. At the same time, agents and roles are loosely coupled: role classes and agent classes can be designed at the same time by different teams. The internal design of multi-agent system (MAS) is independent of the Web applications. This framework helps to implement automatically testing of Web applications.

A Recognition Approach for Adversarial Planning Based on Complete Goal Graph

Abstract

Based on classical plan graph and goal graph, complete goal graph (CGG) is constructed against the characteristics of adversarial domain. The complete goal graph makes the action relate with its goal directly, which is more efficient to recognize adversarial goals. The conception of complete degree of goals will be put forward to distinguish adversarial high level goals. Then, a deep research is done on adversarial plan recognition algorithm based on CGG, which not only can predict adversarial next step action, but also can recognize adversarial goals indifferent levels with complete degrees. The research is of great significance for the plan recognition problem of uncontrollable and nondeterministic domain such as contest robot, information security, business strategy, game role design and etc.

A Quantifiable Trust Model for Multi-agent System based on Equal Relations
Li Li, Hao Li, Gehao Lu, Shaowen Yao
School of Information Science and Engineering, Yunnan University, Kunming, China lily@ynu.edu.cn, lihao707@ynu.edu.cn, gehaol@gmail.com, yaosw@ynu.edu.cn

Abstract

The paper first analyzes trust relations, combining the characteristic of multi-agent system, investigates the equal-relations based trust mechanism for multiagent system, and proposes a possible trust model to quantify and manage the reliability of agent in multiagent system through building trust database and network of agent. Simulation experiment show that the model is able to promptly evaluate and update trust relation among agents, and improve the reliability and efficiency of interaction between agents, providing a solution for the trust problem of multi-agent system.

A Multi-Agent and PSO Based Simulation for Human Behavior in
Emergency Evacuation

Abstract
A new emergency evacuation model based on Multi-Agent framework and Particle Swarm Optimization was presented. This model simulated human individual behaviors and social behaviors in multi-exit evacuation environment. The Linear Weight Decreasing Particle Swarm Optimization (LWDPSO) was introduced to simulate individual’s movement. A hierarchy of behavior rules was described, and a series of individual behaviors and social behaviors during evacuation were defined. A prototype system of emergency evacuation simulation was implemented based on Geographic Information System (GIS) application framework. The result shows that the simulation system well performs some typical evacuation behaviors, the model based on multiagent and LWDPSO has good efficiency and practicability.

Theoretical Investigation on Post-Processed LDA for Face and Palmprint Recognition

Abstract
Recently, a class of post-processing approaches has been proposed to improve the recognition performance of LDA in face recognition. In-depth analysis, however, has not been presented to reveal the effectiveness of the post-processing approach. In this paper, we investigate the rationale of the post-processing approach, and demonstrate the interrelationship of the post-processing approach and the image Euclidean distance method (IMED). We then use the FERET face and the PolyUpalmprint databases to evaluate the post-processed LDA method. Experimental results indicate the effectiveness of the post-processing approach and reveal its relation to IMED.

New Parallel Models for Face Recognition
Heng Fui Liau, Kah Phooi Seng, Yee Wan Wong, Li-Minn Ang
Faculty of Engineering and Computer Science, University of Nottingham Malaysia Campus
Jalan Broga, 43500 Semenyih, Selangor, Malaysia
eyx6lhf@nottingham.edu.my

Abstract
Subspace methods such as principal component analysis (PCA) and linear discriminant analysis (LDA) extract the features based on space domain. Transformation such as discrete cosine transform (DCT) extracts features based on frequency domain. In this paper, we present two parallel models which intend to utilize the features extracted from frequency and space domain of facial images. Both features are combined under a fusion based scheme. FERET database is chosen to evaluate the performance of the proposed method. Simulation results indicate that the proposed method outperforms other traditional methods and enhances the representation of facial image under low-dimensional features.

A Multi-Pattern Matching Algorithm on Multi-language Mixed Texts for Content-based Network Information Audit

Abstract
Content-based network information audit systems have to process multi-language mixed texts usually. The characteristics of multi-pattern matching on multilanguagemixed texts and how existing multi-pattern matching algorithms perform on multi-language mixed texts are analyzed. A novel multi-pattern matching algorithm based on the hash Trie tree is proposed, which expands the standard Trie structure, constructs the hash Trie matching machine with the ISN of characters. Theoretic analysis and experimental results demonstrate that the proposed algorithm efficiently solves the space cost expansion problem and processes multi-language mixed texts correctly and efficiently with lower time and space complexity, satisfied the requirement of content-based network information audit.

Face Detection from Greyscale Images Using Details from Categorized Wavelet Coefficients as Features for a Dynamic Counterpropagation
Network
Lee Seng Yeong, Li-Minn Ang, and Kah Phooi Seng
The University of Nottingham, Malaysia
Department of Electrical and Electronic Engineering
Jalan Broga, Semenyih, Selangor.

Abstract
A dynamic counterpropagation network based on the forward only counterpropagation network (CPN) is applied to facedetection in this paper. Thenetwork, called the dynamicsupervisedforward-propagationnetwork (DSFPN) trains using a supervised algorithm and can grow dynamically during training allowing subclasses in the training data to be learnt. Thenetwork is trained using the categorized wavelet coefficients of the image as features of the image. Theresults suggests a 98% correct detection rate can be achieved with 4% false positives by increasing network complexity.

An Improved Competitive and Cooperative Learning Approach for Data Clustering

Abstract
The recently proposed Competitive and Cooperative Learning algorithm (CCL) (Cheung 2004) has provided a promising way to perform the data clustering without knowing the number of clusters. Nevertheless, its performance is somewhat sensitive to the initialization of seed points. Also, its cooperative mechanism is applicable to the homogenous clusters only. In this paper, we will therefore suggest using the FSCL algorithm to initialize the seed points such that each cluster of data will at least have a seed point. Furthermore, we update the cooperation radius of seed points in CCL, whereby the improved CCL (ICCL for short) can be applicable to the heterogeneous clusters as well. Experiments show the efficacy of the proposed algorithm.

Shape Modification of B-spline Curve with Geometric Constraints
Siyuan Cheng and Xiangwei Zhang
Faculty of Electromechanical Engineering,
Guangdong University of Technology
Guangzhou 510006, China
imdesign@gdut.edu.cn

Abstract
A new physically based model for the shape modification of B-spline curve with geometric constraints is presented. The deformation energy of the B-spline curve is minimized based on finite element method, while geometric constraints can be imposed to control the modified shape. By changing the external force, different methods of modification can be obtained. The method based on least square, which results from applying no force, is local and simpler, but the modified shape seems less smooth. While the method based on global deformation, which is more complicated by adding synthetic spring force, can give more natural and smooth results.

A new anisotropic diffusion equation with adaptive fidelity term
Abstract When denoising with the method of Weickert’s anisotropic diffusion equation, textures and details will be compromised during the process, so a fidelity term is added into the equation. The coefficient of fidelity term will vary adaptively with the content of position, which makes that the diffusion term and the fidelity term come to a better compromise. Otherwise, in order to realize the fact that different type of diffusion can be used in different position, the two eigenvalues are reset by combining edge-enhancing model and coherence-enhancing model. Experiment results show that the new method has obvious effect in preserving textures and details.

An Effective Approach towards Contour-Shape Retrieval

Abstract

Distance histogram has been used for shape representation and retrieval. Though it is efficient and effective, it loses the spatial information of a contour. In this paper, the pixels of a contour are classified into different types, convex, concave and smooth pixels. In addition to distance histograms, two novel descriptors named spatial location distribution (SLD) and spatial distribution entropy (SDE) are introduced. These descriptors have powerful descriptive power for contour with more spatial information. Comparisons are conducted between our method and several other feature descriptors. The results show that the new method is efficient and it provides noticeable improvement to the performance of shape retrieval.

A Fast and Robust People Counting Method in Video Surveillance

Abstract

Video surveillance has become more and more prevalent. It is a basic problem to get the number of access people in scenes. When occlusions occur, it becomes difficult to count people. We propose a fast and robust people counting method, and implement a system. In our system, we use group tracking to compensate weakness of multiple human segmentation, which can handle complete occlusion. Our system can run in real-time about 30fps for CIF video, with counting accuracy defined by frame above 95%.

A Hard Decision Error Correction Scheme for Corrupted Arithmetic Codes

Mengmeng Zhang1, Yuehai Wang1, Jingzhong Wang1, Shumin Zhou2

1 College of Information Engineering, North China University of Technology, Shijingshan District, Beijing, China
2 Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

E-MAIL: zmm@ncut.edu.cn, xxxy@ncut.edu.cn

Abstract

A robust decoder for the corrupted arithmetic codes is proposed, which provides good error correction capability by reserving space for invalid symbol. The proposed decoder acts as a stand-alone error correction tools and it can be used together with any other existing error correction schemes. Keywords: error, correction, hard

LEVEL SET METHOD FOR LICENSE PLATE LOCALIZATION TECHNOLOGY

Yuwang Yang

Computer Department of Nanjing University of Science and Technology(210094), Jiangsu, China
yuwangyang608@163.com

Abstract

Level set method is being applied actively in image field due to its mathematical perfection and maturity. In this paper, based on Mumford-Shah model with Level Set method, the finite difference and third order TVD (total variation diminishing) Runge-Kutta schemes are employed for space and time discretization respectively to solve the model equation. The computation of license plate localization shows that better
A New MRF Framework with Dual Adaptive Contexts for Image Segmentation

Abstract
This work presents a new Markov random field (MRF) framework for image segmentation by incorporating exact contexts in the label field as well as the observed data. On the one hand, the new framework presents MRF with adaptive neighborhood (MRF-AN) system to model adaptively the contextual information of the hidden label field. On the other hand, the new framework models observations via a conditional random field (CRF), which incorporates the contextual information in observed data. The new MRF framework with the dual adaptive contextual information offers several advantages over the conventional framework. In this work, we demonstrate the advantages in an application of detail preservation in image segmentation.

Human Body Segmentation in The Presence of Occlusion
Bi Sheng Xiaoyan Shen Wang Qiang
Information Engineering College, Dalian Maritime University
Dalian, Liaoning, China (116026)
Bisheng@dlmu.edu.cn

Abstract
Human body segmentation in complex situation is an important processing stage in video surveillance. The results have great affects on tracking, behavior recognition or object identification. In this paper, we present a method to segment region in which human bodies are overlapping or walking together. The multiple human objects region is segmented using potential function clustering in the vertical projection histograms of the region, the segmented results are verified by analyzing their geometry features. If the results are not consistent with the human geometry feature, it shows that multiple humans are overlapping. A binocular vision algorithm is proposed to segment the region based on distance. The Experimental results prove the algorithm works robustly, adaptively and efficiently.

An Effective Approach to Content-based 3D Model Retrieval And Classification
Abstract
The Development of effective content-based 3D model retrieval and classification is still an important research issue due to the growing amount of digital information, this paper present a novel 3D model retrieval and classification algorithm. In feature representation, a method combining distance histogram and moment invariants is proposed to improve the retrieval performance. A major advantage of the distance histogram is its invariance to the transforms of scaling, translation and rotation. Based on the premise that two similar images should have high mutual information, or equivalently, the querying image should convey high information about those similar to it, this paper proposed a mutual information distance measure to perform the similarity comparison. Multi-class support vector machine performs the classification for it has a very good generalization performance. This paper tested the algorithm with a 3D model retrieval and classification prototype, the experimental evaluation demonstrates the satisfactory retrieval results and good classification accuracy.

3D Feature Extraction of Head based on Target Region Matching
Haibin Yu1), Jilin Liu2), Jingbiao Liu1)
1) Institute of System Integration, College of Electronic & Information, Hangzhou Dianzi University, Hangzhou, 310018
2) Institute of Information & Communication Engineering, Department of Information & Electronics Engineering, Zhejiang University, Hangzhou, 310027
shoreyhb@hdu.edu.cn

Abstract
In order to recognize and track all of the headsexactly in top view images, a novel approach of 3D feature extraction of heads based on target region matching is presented. The main idea starts from the disparity of head region, which is generally extracted in global dense disparity image obtained by block matching method. Different from the block matching, the correspondence searching in target region matching is not done in the regions around every pixel in image but in the candidate head regions extracted in advance by monocular image processing. As the number of candidate head regions is far less than the resolution of image, the computational complexity and time consume can be largely reduced. After the disparity of candidate head regions are obtained, the 3D features of head, including the height feature and the perspective feature, can be extracted to largely improve the accuracy of head recognition.

Extraction of Semantic Keyframes Based on Visual Attention and Affective Models
Zhi-Cheng Zhao, An-Ni Cai
School of Telecommunication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
zhao.zc@gmail.com, annicai@bupt.edu.cn

Abstract
The Extraction of video keyframe is convenient for browsing and retrieving of video content. However, since the “keyframe” is a subjective concept which involves in vision and psychology, it is difficult to be described by low-level features of video. In this paper, we propose a method of keyframe extraction based on visual attention and affective models. To be concrete, film elements such as character, lighting and camera motion, crucial to human attention, are fused into a visual attention model, and the film is segmented into scenes according to a short-time memory model. The “scene importance” is then computed by using the affective arousal which determines audience’s excitability in the 2D emotion space. Finally, according to the attention model and the scene importance, scene keyframes are extracted. Experimental results indicate that keyframes extracted by our approach are coincident with human perception, and would be in favor of further semantic analysis.

A Color and Texture Feature Based Approach to License Plate Location
Abstract
A novel license plate locating approach based on the color and texture features is presented. Firstly, the input image is converted to the hue-saturation-intensity (HSI) color space. Then a target image is obtained by applying a sequence of image processing techniques to the hue and saturation component images. After that, the space-pixel histogram of the target image is analyzed and mathematically modeled, so that the horizontal candidate is extracted. Finally, discrete wavelet transform is performed on the candidate, and the sum of the first order difference of the DWT subimages highlights the texture information of the LP area, telling the precise position of the license plate. The proposed algorithm focuses on combining the color features with the texture features, improving the locating reliability. Experiment was conducted on a database of 332 images taken from various illumination situations. The license plate detecting rate of success is as high as 96.4%.

Salience-based Evaluation Strategy for Image Annotation
Yong Ge1, Jishang Wei2, Xin Yang1, Xiuqing Wu1
1University of Science and Technology of China, Hefei, 230027 P.R.China
2Xi’an Jiaotong University, Xi’an, 710049 P.R.China

Abstract
Evaluating the efficiency of an image autoannotation method is a requisite to guide the development of auto-annotation method. This paper firstly investigates most existing evaluation strategies, and proposes a novel salience-based evaluation strategy. In the most existing evaluation strategies, every keyword in the annotation results is considered equally. We argue that different keywords in the annotation results have different semantic salience and the keyword which corresponds to the most prominent concept for one image should be the most semantically salient one. In our salience-based evaluation strategy, we consider different keywords according to their semantic salience and we design two evaluation parameters: salience-score and noisy-coefficient, which are more reasonable and more explicit. We conduct our experiments on standard Corel dataset, after obtaining annotation results with three classical statistical models, we compare variant evaluation strategies on these annotation results. The results demonstrate that our evaluation strategy is more consistent to human perception.

Study on conversion method of color space under a big color gamut
Abstract
Since the equipment in computer color quantification system has different color gamut and color feature, accurate control and transmission of color information in this system is particularly difficult, and therefore the color luminance meter is selected for marking the color quantification system. Munsell color system is selected to establish the mutual conversion between RGB and L*a*b* color model for camera. The training set includes 1550 samples and the testing set includes 52 samples, which certainly will lead to the redundant problem of the hidden-layer node number, so the two-hidden-layer neural network is considered. The training program, testing program and foreseeable program is compiled respectively by Neural Network Toolbox in Matlab applications. The conversion relation under a big color gamut is expressed by four-layer BP network. Through training this network, the training error is 0.000748566, using the data of testing set to test this network and calculating the color difference between forecast value and true value, the maximum color difference is 3.6357 NBS, the minimum color difference is 0.5311 NBS, and the average color difference is 3.1744 NBS. The result shows that the network can express the color quantitatively, and it is not subjective and vague, the quantitative mensuration and control of color could be done.

Image Restoration Using Gaussian Particle Filters
Yuelu Liu, Tingzhi Shen, Xinyi Wang
Beijing Institute of Technology
Department of Electronic Engineering
{vladimirliu, shentz, wxybear}@bit.edu.cn

Abstract
Sequential Monte Carlo method has received intense attention among the literature due to its promising applicability to non-linear and non-Gaussian problems. However, while adopting the standard particle filtering method to the area of image restoration, two main drawbacks are found. Firstly, the...
computational complexity, which mainly comes from a procedure called resample (in a serial implementation), of particle filters would render it too resource-requiring for image restoration. Secondly, the sample impoverishment introduced by resample can affect the filter’s performance. In this paper, we adopt a new type of particle filters which do not require resample to the area of image restoration—the Gaussian Particle Filters (GPF). Simulation results are presented to show the GPF’s better performances over conventional particle filters. Key words: particle filter, Gaussian particle filter, resample, sample impoverishment

Spectral Correspondence Using Local Similarity Analysis

Jun Tang, Dong Liang, Nian Wang, Zhao-Hong Jia
Key Lab of Intelligent Computing & Signal Processing Ministry of Education, Anhui University, Hefei 230039, China
tangjun@ahu.edu.cn, dliang@ahu.edu.cn, wn_xlb@ahu.edu.cn, zhjia@mail.ustc.edu.cn

Abstract
This paper presents a novel algorithm for point correspondences using graph spectral analysis. Firstly, the correspondence probabilities are computed by using the eigenvectors and eigenvalues of the proximity matrix as well as the method of alternating row and column normalizations. Secondly, local similarity evaluated by shape context is incorporated into our spectral method to refine the results of spectral correspondence via a probabilistic relaxation approach. Experiments on both real-world and synthetic data show that our method possesses comparatively high accuracy.

A Combined Feature for Partial Fingerprint Recognition

Abstract
Partial fingerprint recognition is an important challenge especially when the partial image does not include singular points such as core and delta. In this paper, we propose a new localized feature named combined feature for partial fingerprint recognition. The combined feature combines the information of every two minutiae of the image and the ridge structure between them. This feature is defined based on the minutiae including ridge endings and bifurcations. The combined feature is invariant with respect to the global transformations such as rotation and transformation. The recognition is performed in three steps: minutiae extraction, combined feature extraction and matching. Experimental results on FVC2004 show efficiency and accuracy of the proposed method.

Face Recognition Using Topology Preserving Nonnegative Matrix Factorization

Taiping Zhang, Bin Fang, Guanghui He, Jing Wen and Yuanyan Tang
Department of Computer Science, Chongqing University, Chongqing, P.R.China

Abstract
In this paper, a novel Topology Preserving Nonnegative Matrix Factorization (TPNMF) method is proposed for face recognition. The TPNMF is based on minimizing the constraint gradient distance, compared with L2 distance, the gradient distance is able to reveal latent manifold structure of face patterns. Compared with PCA, LDA and original NMF which search only the Euclidean structure of face space, TPNMF finds an embedding that preserves local topology information, such as edges and texture. In the way, the proposed TPNMF method is robust for variable in lighting and facial expression. Experimental results show that the proposed TPNMF approach provides a better representation of face patterns and achieves higher recognition rates in face recognition.

2D-NPP: An extension of Neighborhood Preserving Projection

Abstract
A novel method to reduce dimensionality for face representation and recognition was proposed in this paper. This technique attempts to preserve both the intrinsic neighborhood geometry of the data samples and the global geometry. It is derived from ONPP. The main difference between ONPP and 2d-NPP is that the latter does not change the input images to vectors, and works well under the undersampled size situation. First, an “affinity” graph was built for the data in 2DNPP, in a way that is similar to the method of LLE. While the input was mapped to the reduced space implicitly in LLE, 2D-NPP employs an explicit linear mapping between the two. So it is trivial to handle these data just by a simple linear transformation. We also show that it is easy to apply the method in an unsupervised setting. Numerical experiments are reported to
Laser Printer Fuzzy Identification Based on Correlative Specific Area of Character Image
Ning Wang
School of Computer Science and Engineering, South China University of Technology, Guangzhou 510641, China
Guangzhou Public Security Bureau, Guangzhou 510030, China
gz0609@sina.com

Abstract
The type of printer needs to be identified in many cases as evidence. This paper proposed a new method to identify the type of Laser printer according to the feature of printed character image. Character image is segmented into 16 equal-area quadrate sections. Specific area is the ratio of the area of strokes of whole character to the area of character image or is the ratio of the area of strokes of section to the area of section. As the eigenvalue of printed character image, the specific area is relatively constant and structural feature of character image. According to specific area, the correlation coefficient of printed character images is calculated. It is used to evaluate the similarity of standard and identified character image. With the correlation coefficient, the type of laser printer is got by Fuzzy synthetic evaluation. The result of experiment showed that this method is accurate and effective.

Improved Facial Feature Points Calibration Algorithm Based on ASM
Dai Liming, Liu Miao, Chen Yuanyuan
Computer Science and Technology Department, Jilin University
dailiming@yahoo.cn

Abstract
The matching results of traditional ASM are greatly affected by the model initial position. An improper position will lead algorithm to fail. To enhance the accuracy of feature detection, a Quick Rough Positioning Model (QRPM) algorithm is proposed, which makes use of the image and model gray information to calculate the similar coefficient between the model and the region detected. Coarse and fine explorations are adopted to extract the rough region, where the initial model will be set. Experimental results show that the improved algorithm can effectively enhance the accuracy in facial feature points’ calibration, and avoid the ASM results falling into the local minimum.

A Constrained Genetic Algorithm for Efficient Dimensionality Reduction for Pattern Classification
Rajesh Chandrasekhar Panicker Sadasivan Puthusserypady
National University of Singapore
Department of Electrical and Computer Engineering
4 Engineering Drive 3, Singapore 117576
{rajesh.c, elespk}@nus.edu.sg

Abstract
In automated pattern recognition systems, the two main challenges are feature selection and extraction. The features selected directly affects the number of measurements required, and extracting low-dimensional features from these selected ones reduces the computational complexity of the classifier. In traditional approaches, human expertise is obligatory for feature selection and statistical techniques are employed for feature projection. In this paper, a constrained genetic algorithm for performing these two tasks simultaneously, in conjunction with the k-nearest neighbor classifier is proposed. This algorithm requires minimal human intervention as it realizes good tradeoff solutions between classification accuracy,
Pruning Neighborhood Graph for Geodesic Distance based Semi-Supervised Classification

Chun-enguang Li, Jun Guo and Hong-gang Zhang
Beijing University of Posts and Telecommunications, PRIS lab., Beijing, 100876, China
chunguang.lee@gmail.com

Abstract
Recently semi-supervised learning has been gain a surge of interests, but there is a few of research on semi-supervised learning using geodesic distance. The simplest semi-supervised classification algorithm is geodesic nearest neighbors (GNN). However the naive implementation of GNN algorithm is sensitive to the neighborhood scale parameter and suffers from the dilemma of neighborhood scale parameter selection. In this paper, instead of searching for the best neighborhood parameter, we propose a pruned-GNN, which utilize the non-negative reconstructing coefficients to prune the neighborhood graph in order to facilitate the selection of neighborhood scale parameter. Experimental results on several benchmark databases have shown that the proposed pruned-GNN can produce promising accuracies.

Traffic Signs Detection and Recognition by Improved RBFNN

Yangping Wang, Jianwu Dang and Zhengping Zhu
1School of Electronic & Information Engineering, Lanzhou Jiaotong University
2Department of Computer Science, Lanzhou City University
E-mail: wangyangping@mail.lzjtu.cn

Abstract
The paper develops radial basis function neural networks (RBFNN) applications in the traffic signs recognition. Firstly traffic signs are detected by using their color and shape informations. Then genetic algorithm (GA), which has a powerful global exploration capability, is applied to train RBFNN to obtain appropriate structures and parameters according to given objective functions. In order to improve recognition speed and accuracy, traffic signs are classified into three categories by special color and shape information. Three RBFNNs are designed for the three categories. Before fed into networks, the sign images are transformed into binary images and their features are optimized by linear discriminant analysis (LDA). The training set imitating possible sign transformations in real road conditions, is created to train and test the nets. The experimental results show the feasibility and validity of the proposed algorithm.

Extracting Digital Fingerprints from Chinese Documents

Guo-Hua Liu, Hui-Dong Ma, Xu Li, Peng Liang
College of Computer Science
Yanshan University
Qinhuangdao 066004, China
ghliu@ysu.edu.cn

Abstract
It is an important problem to extract features from Chinese documents for protecting intellectual property. The existing approaches are major oriented to words frequency or semantic, they can’t extract features efficiently. By mapping Chinese documents into an ordered set of integers, we find that a Chinese document can be corresponded to a unique ordered set of integers and the set is an isomorphism of the document. So, we propose an algorithm which can hash the set to three kinds of hash value sequences: paragraph sequence, sentence sequence and chunk sequence, which can represent the features of the document completely. In order to reduce the numbers of the features defined as digital fingerprints in this paper, we present an optimal strategy to select some hash values from the sequences. The experimental results show that the algorithms proposed are efficient.
A Model for Fitting the Yield Curve Based on a Continuous Penalty Function

Abstract
This paper establishes a model to fit the yield curve of interest rate. Our research bases on the cubic Bspline function, puts a penalty on the objective function, and then develops a fitting model on the yield curve of SEE T-bonds. We set penalty function by a continuous function, and use second difference operator to improve the computation efficiency. The model is simple for fitting the spot rate and the forward rate, performances good in accuracy and smoothness, and can be an effective method for estimating the term structure of China.

Case-based Reasoning Combined with Information Entropy and Principal Component Analysis for Short-term Load Forecasting
Jinsha Yuan, Li Qu, Weihua Zhang and Li Li
North China Electric Power University
Department of Electronic and Information Engineering
Baoding, Hebei, Province, China
quli_quli@126.com

Abstract
Short-term load forecasting (STLF) plays a vital part in the operation of electric power system, and it relates the security, stability, and economic dispatch of the system. In this paper, rough sets information entropy (IE) and principal component analysis (PCA) are applied to the attributes reduction of load cases, and respectively, the significance and relativity of load data are disposed. Thus, not only is the training time in the process of retrieval decreased, but also is effective control implemented aiming at petit factors to essential ones. In the process of revision, some impactful amendments are presented to improve prediction precision. Finally, this scheme is performed on the data of Bao Ding Electric Power Company (BDEPC) during 2000-2004, and the testing result shows that the proposed model is feasible and promising for load forecasting.

Index Terms - short-term load forecasting, case-based reasoning, information entropy, principal component analysis, neural network

MPIDA: A Sensor Network Topology Inference Algorithm
Tao Zhao, Wandong Cai, Yongjun Li
School of Computer Science, Northwestern Polytechnical University, Xi’an 710072, China
zhaotaonwpu@gmail.com

Abstract
Knowledge of sensor network topology is useful for understanding the structure of the sensor network, and it also plays an important role in resource management and deployment. Additionally, it is a major component of sensor network tomography techniques. Considering sensor network characteristics, we propose a topology inference algorithm based on end-to-end measurement in this paper. Specifically, we consider the case of inferring sensor network topology during the aggregation of the data from a collection of sensor nodes to a sink node. The simulation shows that the proposed approach can discover the sensor network topology accurately and quickly, and scale to the large networks. Keywords: Sensor network, network tomography, topology inference, data aggregation, sensor network tomography

Exploring the Relationships between Personal Characteristics, Aims, and
Reasons of Learning in Further Education by Associating Rule Mining

Abstract Learning occurs when previous perceptions of reality are not in harmony with current experience, creating dissonance. To deepen understanding of the complexities of adult learning, this study presents the relationship within students’ mode of study, the aims of learning and the motivation of choosing the course in further education. Associating rule mining will be used to explore the dataset, associate with these three factors and extract valuable rules. Several important adult learning theories will be reviewed and applied to examine the result. This research will provide valuable insight into how individual learning styles are shaped and developed in the further education.

Image Retrieval with Simple Invariant Features Based Hierarchical Uniform Segmentation

† Mingxin Zhang1,2, Zhaogan Lu1, Junyi Shen1
1. Dept. Information and Communication Engineering, Xi’an Jiaotong University, Xi’an 710049, P.R. China;
2. Dept. of Computer Engineering, Lanzhou Polytechnical College, Lanzhou 730070 China
zhangmx@mail.xjtu.edu.cn, luzhaogan@mailst.xjtu.edu.cn

Abstract According to local information of images, region-based image retrieval is the focus of recent research works, as the approaches based global features cannot achieve the expectation querying results. The objects of interest generally occupy only one small part of images, so the image segmentation with different object regions must be conducted for the region-based image retrieval schemes. However, accurate object segmentation is still beyond current computer vision technique. Here, we proposed one feasible image retrieval scheme based the hierarchical uniform segmentations, which avoid the complexity of image segmentations. Firstly, the querying image is segmented into equal blocks at different hierarchical levels, and the more blocks with larger hierarchical levels. Then, according to the similar metrics of these different size blocks to the expectation image into segmentations, the images containing querying objects can be retrieved with information about scales and locations of query objects in retrieved images. Finally, the proposed image retrieval schemes are tested by experiments via database with 500 images, and the retrieval accuracy can achieve 78% for the optimal similar metric threshold, and is comparable to that of region-based schemes.

A New Topic Influence Model Research in Online Community
Gao Jun-bo An Bo-wen Song An-jun Wang Xiao-feng
(Department of Computer Science, Shanghai Maritime University, Shanghai, 200135, China)
Email:jbgao@cie.shmtu.edu.cn

Abstract The continual development of the Internet has witnessed a huge accumulation of information from the online community and forum. While this has drawn attentions of more and more people, Internet has become the fourth media of information release. Using the probability representation method, we have made an improvement of the Influence Diffusion Model (IDM) proposed by Matsumura. We also proposed a topic influence model in online community, and have supplied a method of finding topics from large amount of forum information that are concerned or potentially will be concerned for the forum administrators and information analysts.

Study of Immune PID Adaptive Controller and Its Applications in Thermal Control System

Abstract Due to the characteristics of large inertia, long time lag and variation with time for the thermal control
system in power plant, conventional PID control strategy can’t achieve satisfied control effect. Biology immune system is characterized by its strong robustness and self-adaptability even when encountering amounts of disturbances and uncertain conditions. Prompted by the regulation rule of biology immune feedback response, an immune PID adaptive control strategy for thermal control systems is presented in this paper. Simulation results show that this control strategy is superior to conventional PID control. It can adapt the changing of object’s parameters and has strong robustness, self-adaptability and disturbance rejection ability. Keywords: Immune system; Immune feedback; Immune PID adaptive control; Thermal control system

A Fuzzy Clustering Algorithm based on Artificial Immune Principles

Abstract
The Fuzzy C-Means algorithm (FCM) is a widely applied clustering method. However, it is usually trapped into the local optimum. In addition, its performance is very sensitive to the initialization. This paper proposes a new fuzzy clustering method based on the immune clonal selection principle, namely CFCM. The clonal selection algorithm is first used to optimize the number of fuzzy cluster centers. The FCM is next employed for clustering the input data. Simulation results demonstrate that our novel approach can overcome the drawbacks of the regular FCM with an improved data clustering performance.

Construct a Real-time Selective Neural Group Network Controller for Internet-based Teleoperation System
Xiang Li1, 2 Yuechao Wang1
1Robotics Laboratory of Shenyang Institute of Automation, Chinese Academy of Sciences
Shenyang, Liaoning 110016, China
2Graduate School of Chinese Academy of Sciences
Beijing, 100049, China
xiangli@sia.cn ycwang@sia.cn

Abstract
The existence of random time-delay in the Internet makes telerobot unable to receive the timely correct instructions. This may seriously decrease the stability and reliability of the system. To solve this problem, many researchers have turned their interest to increasing the local autonomy of the telerobot. In this paper, a real-time selective neural group network controller for the local telerobot system is presented and described in details. In the simulation experiments, we compared it with the traditional fuzzy logic strategy. Simulation results showed: the ability of online learning, information accessing and the predicted evaluation about selective strategy are much higher than the fuzzy logic strategy.

Neurodynamic Analysis for Symmetric Schur Decomposition Problems

Abstract
This paper presents neurodynamic analysis for solving symmetric Schur decomposition problems. A series of dynamical systems are proposed for finding the orthogonal decomposition matrix X for a given symmetric matrix A which are demonstrated to converge to the rows of the matrix X. It is also demonstrated that all the dynamical systems are invariant in the sense that the system’s trajectories will never escape from feasible region of an optimization problem when starting at it. By constructing a well-defined energy function corresponding to a dynamical system, it is shown that the orthogonal decomposition matrix X can be realized by the proposed dynamical systems. The theoretical analysis given here shows that the neurodynamic method is an alternative promising approach for solving the symmetric Schur decomposition problems.
Fuzzy Control System Based on Wavelet Analysis
Rui Wang, Zhaoming Lei, Hexu Sun, Yi Zheng
Hebei University of Technology
Institute of Automation
Rd. Guangrong, 300130 Tianjin, China
LeiZm@hebut.edu.cn

Abstract
In the paper, we discuss the relationship between the membership function of the fuzzy control system and the wavelet basis function. We prove that a wavelet mother function can be described by a membership function of the fuzzy control system and a membership function of the fuzzy control system can also be described by a simple wavelet mother function. The one-to-one corresponding relationship between the membership function of the fuzzy control system and the wavelet basis function is verified. Thus the essence of the fuzzy reasoning and fuzzy control is revealed. This paper presents a new approach to applying wavelet analysis to fuzzy system identification, fuzzy control and fuzzy data analysis, etc.

Some Geometric Aggregation Operators Based on Interval-valued Intuitionistic Fuzzy Sets and Their Application to Group Decision Making
GUI-WU WEI1, XIAO-RONG WANG 2
1 Department of Economy and Management, Chongqing University of Arts and Sciences, Yongchuan, Chongqing, 402160, P. R. China
2 Office Department, Chongqing University of Arts and Sciences, Yongchuan, Chongqing, 402160, P. R. China
E-mail: weiguiwu@163.com

Abstract
Methods for aggregating interval-valued intuitionistic fuzzy information are investigated. Some operational laws of interval-valued intuitionistic fuzzy numbers, score function and accuracy function of interval-valued intuitionistic fuzzy numbers are introduced. Based on these operational laws, some aggregation operators, including interval-valued intuitionistic fuzzy ordered weighted geometric aggregation (IIFOWGA) operator and interval-valued intuitionistic fuzzy hybrid geometric aggregation (IIFHGA) operator, are proposed. An approach to multiple attribute group decision making (MAGDM) with interval-valued intuitionistic fuzzy information is developed based on the IIFWGA and the IIFHGA operators. Finally, an illustrative example is given to verify the developed approach and to demonstrate its practicality and effectiveness.

Fuzzy Distribution Games with Minimum Risk Criteria
Bin Sun Yan-Kui Liu
College of Mathematics and Computer Science
Hebei University
Baoding 071002, Hebei, P. R. China
sunbinboy2001@163.com yliu@mail.hbu.edu.cn

Abstract
In this paper, we present a new class of two-stage minimum risk distribution games model based on credibility theory and two-stage fuzzy optimization method. Then we first introduce approximation approach to dealing with the approximation of the distribution games problem. After that, a hybrid algorithm, which
Combining approximation approach, neural network (NN) and particle warm optimizer (PSO), is designed to solve the distribution games problem, and a numerical example is given to show the feasibility of the hybrid algorithm.

**Bounds on the value of fuzzy solution to fuzzy programming problem**

Ming-Fa Zheng Yan-Kui Liu
College of Mathematics and Computer Science
Hebei University
Baoding 071002, Hebei, P. R. China
mingfazheng@126.com yliu@mail.hbu.edu.cn

**Abstract**
The paper is concerned with finding the refined bounds on the value of fuzzy solution to fuzzy programming problem. In this paper, we first present the definitions which are the sum of pairs expected value (SPEV), the expected value of the reference scenario (EVRS), and the expectation of pairs expected value (EPEV), and obtain the value of fuzzy solution (VFS) defined by difference between the recourse problem solution and the expected value of reference solution. In addition, several numerical examples are also given in order to explain the definitions specifically. Finally, the properties concerning the concepts are studied, which result in refined bounds on the value of fuzzy solution.

**On Fuzzy Modulator for the PMSM Step Motion Control**
Zhaoming Lei, Hexu Sun, Yan Dong, Yi Zheng
Hebei University of Technology
Institute of Automation
Rd. Guangrong, 300130 Tianjin, China
LeiZm@hebut.edu.cn

**Abstract**
The paper presents a fuzzy modulator for the PMSM step motion control to modulate the current vector duration to improve the response speed and reduce the torque ripple of the system, on the basis of analyzing the principle of step motion control and introducing the fuzzy logic in. The results of simulation and experiment suggest that the presented approach can cut down the torque ripple and improve the control performance and the positioning precision.

**Fuzzy Random Portfolio Selection Problem**
Fang-Fang Hao Yan-Kui Liu
College of Mathematics and Computer Science
Hebei University
Baoding 071002, Hebei, P. R. China
hff29@163.com yliu@mail.hbu.edu.cn

**Abstract**
In this paper, we discuss a portfolio selection problem in a fuzzy random decision system. A new type of portfolio selection model is proposed based on fuzzy random theory. To solve the proposed model, we first present the variance formulas of triangular fuzzy random variables, then design a genetic algorithm. Finally, we provide a numerical experiment to illustrate the feasibility and effectiveness of the proposed algorithm.
A Fuzzy Model of Interval speed Continuous Petri Nets*
Yueying Peng and Weizhi Liao
Department of Information Technology,
Guangxi Teachers Education University,
Nanning 530001, China
e-mail: pengyy@gxtc.edu.cn,
liaowz@gxtc.edu.cn
* Natural Science Foundation of Guangxi
0542049, 0640032, China

Abstract
The Interval speed Continuous Petri Nets (ICPN) isa continuous model of time Petri nets. It is shown that the descriptive capability of the proposed Interval speed Continuous Petri Nets (ICPN) Model is stronger than the other ICPN Model. Although the action of the continuous petri nets is non-linear and not easy to combine, fuzzy theory makes it possible to complete the analysis of the proposed ICPN and the task of control design. In order to achieve this goal, a fuzzy model of the ICPN is proposed. It also makes a definition of the fuzzy rule of the ICPN, discusses the fuzzy control of the ICPN, and gives the theorem marked and restrained by the collection house. All these provide some theoretical foundation for the control of fuzzy system on the basis of description of the ICPN. The feasibility of the fuzzy control of the ICPN is also shown.

Selection of Delay Time Window and Delay Time in Phase Space Reconstruction

Abstract
A new method called C-C-3 method is suggested, which can amend at least 4 drawbacks of the C-C method (which is a popular method of the phase space reconstruction). The correlation integral algorithm of the time series is improved; and based on the theory of the chaotic system period N, the first local minimum of $S_3(t)$ which can show the period N of the chaotic time series is looked for, and by which the optimal delay time window can be determined. Only the first local minimum of the average $\Delta S_3(t)$ is wanted to estimate the optimal delay time. The results by the new method are more stable and more appropriate. Furthermore, the robustness of the C-C-3 method reaches 70%, whereas that of the C-C method is 30%. Keywords: Delay Time Window; Delay Time; Correlation Integral; Phase Space Reconstruction

A Novel Architecture for the Computation of 2D-DWT and its Implementation on Virtex-II Pro FPGA

Abstract
This paper proposes a new approach for the design of hardware architecture for the computation of 2D-DWT for an 8 x 8 image. The key feature of this design is to directly apply 2D-DWT on alternate pixels of an image, called as the Non-Separable method, and implement it on an FPGA. The resulting design was implemented using only 6 adders and 10 multipliers, thus optimizing the number of multipliers and adders required for the computation of 2D-DWT. Thus our approach provides a cost effective solution as compared to the conventional 2D non-separable methods without compromising on speed performance. The design is implemented on Xilinx Virtex II Pro FPGA development kit and synthesized using Xilinx XST (VHDL/Verilog) synthesis tool. Key terms: 2D-DWT, Signal Processing, VLSI, FPGA, filter coefficients, IDWT.
Order Holon Modeling Method Based on Time Petri-nets and Its Solution with Particle Swarm Optimization

Abstract
The manufacturing system change from hierarchy to parallel structure, from concentration to distribution based on notion of Holonic Manufacturing System. In this paper, the problem of how to demarcate the unit of the manufacturing system, management style of the unit, control structure and the corresponding control method are settled. The model on order settlement in system reconfiguration model based on time Petri-net is put forward, order intelligent operation series is guided by particle swarm optimization. Simulation results show that the proposed model and algorithm are effective to order evaluation and implementation.

Research on Improving Training Speed of LMBP Algorithm and Its Simulation in Application

Abstract
This paper analyzes the rudimental principle and cyber-realization of LMBP (Levenberg Marquardt Back Propagation) algorithm and finds out the main factors which restrict the training speed of this algorithm. One method of quickening the training speed is proposed and applied into the basic LMBP algorithm. When calculating the increment of weights and biases, the calculating speed is three times of that of the basic LMBP algorithm. At last, this paper applies this ameliorated LMBP algorithm into the training simulation of fault diagnosis based on some device’s gearbox. The result indicates that the total training speed of single-hidden layer BP neural network based on the improved LMBP algorithm is approximately three times of that of the basic LMBP algorithm.

A Dish Parallel BP for Traffic Flow Forecasting
Guo-zhen Tan, Qing-qing Deng, Zhu Tian, Ji-xiang Yang
Dalian University of Technology
Department of Computer Science and Engineering
gztan@dlut.edu.cn, compu54@163.com, tian-zhu@163.com, jixiang_yang@126.com

Abstract
Reducing training time for artificial neural network (ANN) when training large samples is an active area of research. The back propagation (BP) is wildly used in Short-term Traffic Flow Forecasting which require the training set size be much larger than the network size. In order to improve training speed, Data parallelism is a good idea. A novel data parallel BP based on dish network is proposed in this paper. Theoretical and experimental evidence proves that the dish data parallel BP reduce the communication cost compared with the traditional one. Meanwhile, by using the real traffic flow data of DaLian city, experiments show that this dish dataparallel BP improves the training speed and enhances speed-up ratio.

An Improved Neural Network Model for Graduate Education Evaluation
Bao Qiong, Gu Xingsheng, Shen Yongjun
Research Institute of Automation, East China University of Science and Technology, Shanghai, 200237, China
E-mail: baiegufan@sohu.com, xsgu@ecust.edu.cn, gufanbaihe@sohu.com
Abstract
As an important part of higher education evaluation, graduate education evaluation plays a significant role in safeguarding a sustainable development of higher education, especially graduate education. Considering the problems that traditional evaluation methods mainly depend on the experience of experts to a certain extent and there are many correlate factors which make it difficult to establish the evaluation model, a novel multiple improved PIDNN model is proposed in this paper to get the education evaluation model. In this model, the concepts of variable integral and partial differential are introduced into the design of hidden-layer of PIDNN, and the multiple improved PIDNN are dynamically combined to get the evaluation output with a gating network. The simulation results with the real data provided by East China University of Science and Technology indicate the validity of this modeling approach. Keywords — education evaluation; PID neural network (PIDNN); variable integral; partial differential; multi-model

Supervised FCNN Classification for Garment Seams

Abstract
In this paper, a supervised fuzzy clustering neural network (SFCNN) is introduced for constructing the garment seam evaluation system. Our experimental results demonstrate that the proposed system could efficiently be used as an objective garment seam evaluation system with high accuracy and is robust for various structures and mechanical properties of middle-thickness cotton fabric.

Simulation of T-S Fuzzy Neural Network to UASB Reactor Shocked by Toxic Loading

Abstract
The neural network was conducted based on the Takagi-Sugeno fuzzy systems. Predictions of the biogas production rate, volatile fatty acid and CH4 for the UASB reactor were made using fuzzy neural network based on database collected from the anaerobic systems shocked by the Chloroform and 2, 4-dinitrophenol loading. The correlation coefficients of observed and simulated values were above 0.940 for the training set, and above 0.860 for testing set. The results showed that fuzzy neural network can perfectly predict the performance of UASB shocked by the toxic loading, and has greatly adaptability to the variations of the anaerobic treatment system.

The Off-line and On-line Fuzzy Backstepping Controllers for Rotary Inverted Pendulum System

Abstract
In this study a new combination of nonlinear backstepping scheme with fuzzy system is presented for controlling a rotary inverted pendulum system to achieve better performance in nonlinear controller approach. This study uses two different fuzzy systems: off-line and on-line to consider different concept. The purpose of this study is to design a stabilizing controller that balances the inverted pendulum in the upright position.

Dynamic System Modeling with Multilayer Recurrent Fuzzy Neural Network

Abstract
A multilayer recurrent fuzzy neural network (MRFNN) is proposed for dynamic system modeling in this
paper. The proposed MRFNN has six layers combined with T-S fuzzy model. The recurrent structures are formed by local feedback connections in the membership layer and the rule layer. With these feedbacks, the fuzzy sets are time-varying and the temporal problem of dynamic system can be solved well. The parameters of MRFNN are learned by modified chaotic search (CS) and least square estimation (LSE) simultaneously, where CS is for tuning the premise parameters and LSE is for updating the consequent coefficients accordingly. Simulation results of chaos system identification show the proposed approach is effective for dynamic system modeling with high accuracy. And then the proposed approach is applied to a batch reactor modeling.

**Study of an Adaptive Immune Detection Algorithm for Anomaly Detection**

Ya-jing Zhang (yajing_zh@163.com)
Zhen-bin Du (zhenbindu@yahoo.com.cn)
Yi-ming Zhai (zhaiyiming@163.com)
Dian-tong Liu (diantong.liu@163.com)
Institute of Computer Science & Technology, Yantai University, Yantai, Shandong, 264005, China

**Abstract**
On the basis of research for anomaly detection in the biological immune principles, a gene immune detection algorithm is provided. It combines innate immune and adaptive immune mechanism of the biological immune system. An adaptive approach that changes the thresholds of match in real time is suggested. This paper discussed some problems of anomaly detection in computer immune system. Shown by simulation experiments, the algorithm improves self-immunity and variety of antibodies. And it has such advantages as, high detecting efficiency, less computing time and adaptive character.

**Keywords:** Anomaly detection; Immune; Vaccine operator; Adaptive

**A Method of Fine-grained Authorization and Access Control for ASP Pages**

Ting Wang Xingyuan Chen Bin Zhang Lichun Pei
Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004, China
wt82325@yahoo.com.cn

**Abstract**
As the amount of active web pages increased, the need to restrict access only to specific users or for specific usage surely arises. The protection of information contained in active web pages, however, is difficult because the content of pages changes dynamically based on the access context. In this paper, we propose a fine-grained authorization model for ASP pages expecting that we can find some useful thought in addressing the problem of access control of general active web pages. The method proposed supports authorization at different levels, takes into consideration access context, and provides fine-grained protection for information contained in ASP pages.

**The Research and Application of Resource Dissemination Based on Credibility and UCON**

**Abstract**
Based on the concept of credibility and a new access control model—usage control (UCON),
A Flexible Subscription Model for Broadcasted Digital Contents
Franz Kollmann
University of Klagenfurt
franz@syssec.at

Abstract
This paper introduces subscriptions as authorizations to access contents within time periods. For a technical realization of the subscriptions, a new key assignment scheme is proposed that supports fine-granular adjustable restrictions on both, contents and validity duration. Its security is based on the reliance of tamper-proof devices and hash functions. Since per subscription only one key pair is required, it is very suitable in practice. Additionally, a concept based on prepaid cards is given that unburdens the server from user authentication and preserves the users’ anonymity.

A biometric verification system addressing privacy concerns
Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassì and Fabio Scotti
Dipartimento di Tecnologie dell’Informazione
Universit`a degli Studi di Milano
Via Bramante 65
26013 Crema, Italy

Abstract
Biometric techniques are more and more exploited in order to fasten and make more reliable the identification process. Recently, many proposals have been formulated combining cryptography and biometrics in order to increase the confidence in the system when biometric templates are stored for verification. In this work we present a biometric authentication technique based on the combination of multiple biometric readings. The authentication control can be performed offline and the stored identifier does not disclose any information on the biometric traits of the identified person, so that even in case of loss or steal of the document, privacy is guaranteed. Keywords: Biometric identification, Privacy, Securesketch.

A New Forward-Secure Threshold Signature Scheme Based on Schnorr Cryptosystem

Abstract
Based on Schnorr cryptosystem, this paper proposes a new forward-secure threshold signature scheme. It ensures that both the signature’s secret key and the signature are forward-secure through efficiently hiding the current secret key in the signature phase and using the time-parameter effectively in the verification phase. This scheme has the new property that it is infeasible for an attacker to forge any valid signature pertaining to the past even if
he has corrupted up to more than or equal to the threshold members and has obtained the current key. It is also proven to be forward secure based on the hardness of factoring in the random oracle model.

A Novel Trust Community Based on Direct Certifying for Pervasive Computing Systems*  

Abstract  
In the vision of pervasive computing, there are a great diversity of services in the environment and a great deal of nomadic users walking through them. The traditional proof-making mechanisms of access control are no longer appropriate for the new context, in which people expect to access information in a more flexible and non-intrusive way. Instead of asking people for the certificates, this paper advocates a direct certifying mechanism, in which delegation relationships are directly verified by asking the delegator. By dynamically discovering potential credential chains, a trust community is maintained. Existing credential chain discovery methods are not scalable enough for that they either need collecting all credentials in the system or need referring to all the potential users. In our approach, each user keeps a trust list to reduce the fan-out of searching steps. The simulation shows that the performance is greatly improved.

Audio-Visual Recognition System with Intra-modal Fusion  
Yee Wan Wong, Kah Phooi Seng, Li-Minn Ang, Wan Yong Khor, Heng Fui Liau  
Faculty of Engineering and Computer Science,  
The University of Nottingham Malaysia Campus,  
Jalan Broga,  
43500 Semenyih, Selangor Darul Ehsan, Malaysia  
Yeewan.wong@nottingham.edu.my  

Abstract  
In this paper, a new multimodal biometric recognition system based on feature fusion is proposed to increase the robustness and circumvention of conventional multimodal recognition system. The feature sets originating from the output of the visual and audio feature extraction systems are fused and being classified by RBF neural network. Other than that, 2DPCA is proposed to work in conjunction with LDA to further increase the recognition performance of the visual recognition system. The experimental result shows that the proposed system achieves a higher recognition rate as compared to the conventional multimodal recognition system. Besides, we also show that the 2DPCA+LDA achieves a higher recognition rate as compared with PCA, PCA+LDA and 2DPCA.

An Efficient Credential-based Scheme for Cross-domain File Sharing  

Abstract  
As cross-domain file sharing is important and existing schemes have some shortcomings, an efficient credential-based scheme is proposed in this paper. Symmetric-key credential, delegation without intervention of any centralized administrator, no need for traditional ACL and mapping remote group names to local identifiers are the features of the scheme. Symmetric-key credential is flexible, computationally efficient and can provide some useful revocation means. The way of no centralized administrator can ease management and administration overheads, and also avoid center point failure. The features of no need for traditional ACL and mapping remote group names to local identifiers have the advantage of reducing the burden of storage server. The processes of cross-domain delegation, authentication and revocation are discussed. And the security analysis indicates that the scheme is good.

An Effective Genetic Algorithm for Self-Inverse S-boxes
Hua Chen, Dengguo Feng  
Institute of Software Chinese Academy of Sciences  
State Key Laboratory of Information Security  
4 South Fourth Street, Zhong Guan Cun, Beijing  
chenhua@is.iscas.ac.cn

Abstract  
As unique nonlinear components of most block ciphers, S-boxes provide the most important confusion effect. How to design secure S-boxes is a key problem in the design of block ciphers. There have existed many methods to design S-boxes, among which the method with genetic algorithms has attracted much interest in recent years. In this paper, an effective genetic algorithm is provided for the current popular self-inverse S-boxes, which consists of fitness function, breeding function, selection function and mutation function. Under the given algorithm, a large number of good self-inverse S-boxes can be obtained.

Design of an Instruction for Fast and Efficient S-box Implementation  
Meifeng Li, Guanzhong Dai, Hang Liu, Wei Hu  
Research Institute of Control and Network,  
College of Automation,  
Northwestern Polytechnical University,  
Xi’an, Shan Xi, 710072, China  
llaannfeng@yahoo.com.cn

Abstract  
With the development of cipher instruction set extension, design of s-box instruction has received more and more attention. An s-box instruction named SboxPer is designed in this paper for fast and efficient implementation of s-boxes in common symmetric-key ciphers. By introducing PLUT, this instruction improves the efficiency of table lookup. Half-byte permutation is performed after the table lookup operation, which leads to the result that no additional instruction is needed to obtain the final result of S-box operation. Results of performance estimate show that this instruction can improve the execution speed of sbox lookup in symmetric-key ciphers significantly and occupies little memory space.

Pairing-Based Proxy Signature Scheme with Proxy Signer’s Privacy Protection  

Abstract  
Based on bilinear pairings, a proxy signaturescheme with proxy signer’s privacy protection is proposed, in which a proxy signer signs messages on behalf of the original signer while the proxy signer is anonymous to anyone but the original signer. If necessary, the anonymity can be revoked by the original signer to identify the proxy signer. Neither this scheme needs any trusted third party nor the proxy signers need publish the extra public key corresponding to their alias. On the other hand, both the original signer and the proxy signers can open the identities of the proxy signers from a valid proxy signature. Then, neither the original signer nor the proxy signer can deny the identity of a valid proxy signature. So, the proposed scheme can be used in voting, e-auction and other environment where individual privacy needs careful protection.

An Improved Key Agreement Protocol based on Key Association Set for Dynamic Peer Group
Abstract
Secure group communication is a research hotspot. The Tree-based Group Diffie-Hellman Protocol is a fairly good key management scheme for dynamic peer group communications. Through analyzing TGDH protocol, the authors have found out that a deficiency exists with its communication mode. A lot of redundant messages are used to complete group re-keying so that more communication bandwidth will be consumed in TGDH. This paper aims to solve the deficiency and improve TGDH through designing a preparatory algorithm of finding a Key Association Set. A new re-keying protocol is also designed by using the algorithm. Theoretical analysis shows that our protocol effectively decreases the communication and storage overload of TGDH, with the communication bandwidth descending from \(O(n \log n)\) to \(O(n)\) and the key storage descending from \(O(n)\) to \(O(\log n)\). The simulation result also shows the improved protocol has a better communication performance.

Efficient Zaps and Signatures of Knowledge

Chunming Tang, Dingyi Pei
School of Mathematics and Information Sciences
Guangzhou University, China, 50006
tangcm622@hotmail.com, gztcdpei@scut.edu.cn
Zheng-an Yao
School of Mathematics and Computational Mathematics
Zhongshan University, China, 51006
mcsyao@mail.sysu.edu.cn

Abstract
The concept of Zaps, two-round witness indistinguishable proofs, was introduced by Dwork and Naor in 2000. They constructed Zaps based on non-interactive zero knowledge proof. This left open the following problem: does there exist a non-interactive Zaps? Barak et al. and Groth et al. answered this question affirmatively under the assumption of the existence of Hitting Set Generators against co-nondeterministic circuits and Decisional Linear Assumption, respectively. In this paper, we will construct efficient non-interactive Zaps under the assumption of one-way function. In 2006, Chase and Lysyanskaya defined and constructed signatures of knowledge based on non-interactive zero-knowledge proof. We prove that their signature is not secure and point out that they exist under the existence of trapdoor permutation. Feige and Shamir stated that digital signature cannot be zero-knowledge (otherwise they are forgeable) and it can be witness hiding. In this paper, we will revise the definition of the signatures of knowledge by using witness hiding protocol and construct them under the existence of one-way function.

Game-based Analysis of Multi-party Non-repudiation Protocols
Wang Xueming, Li Xiang
Institute of Computer Science, Guizhou University, Guiyang 550025, China
ie.xmwang@gzu.edu.cn

Abstract
Fairness and non-repudiation turn out to be increasingly important security services with the fast growth of electronic commerce on the Internet. We have made some game based analysis of multi-party non-repudiation protocols recently. We use alternating transition systems, a game based model, to model protocols and alternating temporal logic, a game based logic, to express requirements that the protocols must ensure. Fairness and non-repudiation of the MK multi-party non-repudiation protocol are automated analyzed by using Mocha, a model-checker that supports the alternating transition systems and the alternating temporal logic. Finally we have made some improvement of the protocol which enable it to have fairness and non-repudiation.

Forward Secrecy for an Efficient Password-Based Authenticated Key Exchange
TingJun Liu, ShuHua Wu and YueFei Zhu
Abstract
A password-based authenticated key exchange (PAKE) protocol in the three-party setting allows two clients communicating over a public network to agree on a common session key with the help of a server. In the setting the users do not share a password between themselves, but only with the server. In this paper, we propose a new efficient password-based authenticated three-party key exchange protocol and provide a rigorous conclusion of forward security for it in both the random-oracle and the ideal-cipher models under the gap Diffie-Hellman intractability assumption. It is a significant advantage that our protocol is proved secure in a model that allows the adversary to make adaptive corrupt queries, in contrast to previous solutions.

A Note on Shacham and Waters Ring Signatures

Abstract
In 2007, Shacham and Waters [9] propose the first efficient ring signature scheme, without random oracles, based on standard assumptions. And the signature size is linear in the size of the ring. In this paper, we analyze the security of Shacham and Waters ring signature [9] when using the structure of ring signature proposed by [6]. We claim that, in some cases, Shacham and Waters ring signature can be applied in a more efficient way, i.e., the size of the ring signature can be constant. Moreover, the signer can decide whether to provide linkability by herself.

Generalized Synchronization Theorem for Bidirectional Discrete Systems with Application in Encryption Scheme
Ye Ji*, Ting Liu† and Lequan Min*,†
*School of Applied Science and †School of Information Engineering

Abstract
This paper establishes a theorem of generalized chaos synchronization (GCS) for bidirectional discrete systems. Based on this theorem, one can construct new chaotic systems which can achieve GCS among some of the state variables. As a first application, a four-dimensional bidirectional GCS discrete system (BGCSDS) is introduced, whose prototype is the Sinai map. Numerical simulation shows that two pair variables of the BGCSDS achieve GCS via a predesigned transform $H$. Based on the BGCSDS, an encryption scheme is introduced. This scheme has the functions of the authentication of the data, and the one-time-pad. The scheme is able to encrypt and decrypt information without any loss. The analysis of the key space and sensitivity of key parameters shows that this scheme has sound security. The key space of the scheme is larger than $2^{300}$. It can be expected that our theorem and scheme provide new tools for understanding and studying the GS phenomena and information encryption.

A Provable Secure Key Management Program for Wireless Sensor Network

Abstract
This paper presents a new authentication and key agreement protocol EMSR for wireless sensor network. The program can achieve mutual authentication and establish a shared session key between nodes by using public key certificate. Meanwhile, it effectively prevents the authentication problems due to the
usage of purelysymmetric encryption mechanism, and it has smallcommunication cost, fast calculation and supporting lowconsumption sensor network nodes. In addition, we give the security proof of this new protocol EMSR with CKsecurity model, which indicates that EMSR has the corresponding security attributes of CK security model, and therefore it satisfies the requirements of sensor network.

A Single Key MAC Based On Hash127
Jin Xu
Beijing Electronic Science and Technology Institute, Beijing 100070, China
xjwy@besti.edu.cn
Dayin Wang
SKLOIS Lab, Institute of Software, Chinese Academy of Sciences, Beijing 100080, China
wdy@is.iscas.ac.cn

Abstract
There are well-known methods to construct message authentication codes using universal hash functions. This approch is very promising as it provides schemes that are both efficient and provably secure under reasonable assumptions. But those schemes all need two keys, one for the universal hash function and one for the block cipher. Hash127MAC, proposed here, uses only one key and can be proved security under reasonable assumptions.

To Solve the High Degree Congruence $x^n \equiv a \pmod{p}$ in $(p)$

Abstract
In this paper, the authors derive a new sufficient and necessary condition for the high degree congruence $x^n \equiv a \pmod{p}$ to have solutions from a known discriminant. Put forward the definition of the trivial solution to the congruence, elaborate two methods of computing the trivial solution in deterministic polynomial time, argue that non-trivial solutions to the congruence cannot be obtained cyclically from the trivial solution, and infer the two new methods of seeking the trivial solution. The paper analyzes the time complexity of a probabilistic algorithm for random solutions to the congruence without especially large $p$ and $n$, and gives the discrete logarithm time algorithm for non-trivial solutions to the congruence with especially large $p$ or $n$. Therefore, the paper discusses roundly the way how to seek solutions to the congruence $x^n \equiv a \pmod{p}$, which is helpful to designing new public-key cryptosystems.

Improvement on A Generalized Scheme of Proxy Signature Based on Elliptic Curves

Abstract
In a generalized proxy signature scheme with known signers, any $t_1$ or more original signers out of $n_1$ original signers ($1 \leq t_1 \leq n_1$) can represent the original group to delegate the signing capability, and $t_2$ or more proxy signers out of $n_2$ proxy signers ($1 \leq t_2 \leq n_2$) can represent the proxy group to sign message on behalf of the original group. In the paper, we show that Hwang et al.’s generalized proxy signature scheme is vulnerable to the original signers’ forgery attack. After a malicious original group of $t_1$ ($1 \leq t_1 \leq n_1$) signers obtains a proxy signature $(M_w, K, KOSID, M, R, S, APSID)$, the original signer can collude to generate a generalized proxy signature without the agreement of the proxy group with the identities APSID. Hwang et al.’s generalized proxy signature scheme is unable to meet nonrepudiation. We propose an improved generalized proxy signature scheme which can resist our original
A Robust Estimator for Evaluating Internet Worm Infection Rate

Abstract

The Internet worm is a menace for the security of the Internet users. To detect and protect the Internet worm becomes an important research topic in the field of Internet security. A robust estimation method for evaluating worm infection rate is proposed in this paper. The robust estimator of worm infection rate is derived based on the robust maximum likelihood estimation principle at first; The corresponding elements of the equivalent weight matrix constructed by the residuals and some chosen weight functions are given; The error influence functions related to the robust estimator and the least squares estimator are respectively analyzed; At last, a simulated example is carried out. It is shown that the robust estimation is effective and reliable in resisting the bad influence of the outlying scan data on the estimated worm infection rate with high computation convergence speed.

A Typical Set method of Intrusion Detection Technology Base on Computer Audit data

Duan Xuetao, Jia Chunfu, Fu Yubing
College of Information Technology and Science, Nankai University
Tianjin 300071, China
jason@mail.nankai.edu.cn, cfjia@nankai.edu.cn, fuyb@mail.nankai.edu.cn

Abstract

The signature database of intrusion detection system is usually built by the short sequences of system call. The real-time efficiency and accuracy of intrusion detection is greatly influenced by the scale of signature database and the approach of intrusion data analysis. In this paper, a typical set method is provided to compress the normal signature database. Using the data set of UNM CERT sendmail for testing, the feasibility of typical set method is validated, and an appropriate rate of typical set for intrusion detection is proposed. Meanwhile, the LSM (Linux Security Modules) framework is presented to hook system calls and other audit data from operation system to build intrusion detection system signature database and to identify intrusion activity. A system service process oriented detection idea is also introduced to make the intrusion detection more pertinent and accurate. Abnormal detection experiments results show good performance of our intrusion detection method.

A Context-based Analysis of Intrusion Detection for Policy Violation

Kaiyu Wan
Department of Computer Science
East China Normal University, Shanghai, PRC
kaiyu.wan@gmail.com

Abstract

Existing intrusion detection systems (IDS) operate independently from security policy enforcement mechanism. Incurrent IDS the functionality has been restricted to detecting only anomaly in system behavior and system misuse. In order to assist system administrators in restoring and strengthening system security after an intrusion is detected, this paper proposes a method that will link the security violation to a non-empty subset of the policy base. A multiagent system is proposed to automate the intrusion detection and analysis. Keywords: Intrusion detection, security context, policy base

DDoS Attack Detection Based on RLT Features
Tu Xu (cscsi999@yahoo.com.cn)
Dake He (dkhe_scce@home.swjtu.edu.cn)
Yu Luo (yuluo77@163.com)

School of Information Science and Technology, Southwest Jiaotong University, ChengDu

Abstract
To use SVM to detect DDoS precisely, the features vector that can distinguish normal stream from attack stream is required. According to the characters of DDoS, a group of relative values features (RLT features) are proposed. For indicating the existence and intensity of DDoS attack simultaneously, multi-class SVM (MCSVM) is introduced to DDoS detection. As shown in the emulation experiments, our method can detect various DDoS attacks effectively and indicate the attack intensity. The detection result is better than other present detection measures. Because RLT features include more attack information than the detection measures using single attack character, a better detection result is available.

Scenario Discovery Using Abstracted Correlation Graph

Abstract
Intrusion alert correlation techniques correlate alerts into meaningful groups or attack scenarios for the ease to understand by human analysts. These correlation techniques have different strengths and limitations. However, all of them depend heavily on the underlying network intrusion detection systems (NIDSs) and perform poorly when the NIDSs miss critical attacks. In this paper, a system was proposed to represent a set of alerts as subattacks. Then correlates these subattacks and generates abstracted correlation graphs (CGs) which reflect attack scenarios. It also represents attack scenarios by classes of alerts instead of alerts themselves to reduce the rules required and to detect new variations of attacks. The experiments were conducted using Snort as NIDS with different datasets which contain multistep attacks. The resulted CGs imply that our method can correlate related alerts, uncover the attack strategies, and can detect new variations of attacks.

A Parameter Selection Approach for Mixtures of Kernels using Immune Evolutionary Algorithm and Its Application to IDSs
Chun Yang, Haidong Yang, Feiqi Deng
College of Automation Science and Engineering
South China University of Technology
Guangzhou, Guangdong, China, 510640
Email: yang.tree@gmail.com, hdyang, aufqdeng@scut.edu.cn

Abstract
Supervised anomaly intrusion detection systems (IDSs) based on Support Vector Machines (SVMs) classification technique have attracted much more attention today. In these systems, the characteristics of kernels have great influence on learning and prediction results for IDSs. However, selecting feasible parameters can be time-consuming as the number of parameters and the size of the dataset increase. In this paper, an immune evolutionary based kernel parameter selection approach is proposed. Through the simulation of the denial of service attacks in mobile ad-hoc networks (MANETs), the result dataset is used for comparing the prediction performance using different types of kernels. At the same time, the parameter selection efficiency of the proposed approach is also compared with the differential evolution algorithm.

A Hybrid Approach for Real-Time Network Intrusion Detection
Systems

Abstract
This paper proposes a hybrid approach for real-time Network Intrusion Detection Systems (NIDS). We adopt Random Forest (RF) for feature selection and Minimax Probability Machine (MPM) for intrusion detection. RF provides the variable importance by numeric values so that the irrelevant features can be eliminated. However, the NIDS based on RF is slow to build intrusion detection model. We employ MPM, since MPM has been shown a better performance compared with RF in terms of model building time. To validate the feasibility, we carry out several times of experiments with KDD 1999 intrusion detection dataset. The experimental results show the proposed approach is faster and more lightweight than the previous approaches while guaranteeing high detection rates so that it is suitable for real-time NIDS.

Research on the Resilience of Key management in Sensor Networks

Abstract
Resilience against node capture is one of the main indicators of the key pre-distribution security in sensor networks. On providing the attack model and the definition of the resilience against node capture of sensor networks, the resilience of basic random key predistribution, Q-composite random key pre-distribution and their reinforced schemes are analyzed and compared in depth. Research results show that the size of key pool, the numbers of the keys stored in nodes and the value of Q determine the resilience of random key pre-distribution. The tradeoff between the resilience, security connectivity and costs in sensor networks is presented. These researches lay a foundation on the design of the secure protocol and the algorithm in the specific application environment of sensor networks.

A New Centralized Group Key Distribution and Revocation in Sensor Network

Abstract
Sensor networks have a wide spectrum of military and civil applications, particularly with respect to security and secure keys for encryption and authentication. This paper presents a new centralized approach which focuses on the group key distribution with revocation capability for sensor networks. We propose a new personal key share distribution. When utilized, this approach proves to be secure against k-number of illegitimate colluding nodes. In contrast to related approaches, our scheme can overcome the security shortcomings while keeping the small overhead requirements per node. It will be shown that our scheme is unconditionally secure and achieves forward secrecy. The analysis is demonstrated in terms of communication and storage overheads.

An Efficient Identity-based Short Signature Scheme from Bilinear Pairings

Abstract
In this paper, we present an ID-based signature scheme that is proved to be secure in the random oracle model under the hardness assumption of k-CAA problem. The proposed scheme upholds all desirable properties of previous IBS schemes, and requires general cryptographic hash functions instead of MapToPoint hash function that is inefficient and probabilistic. Furthermore, our scheme requires less computation cost and is significantly more efficient than all known IBS schemes, and the size of signatures generated by our scheme is approximately 160 bits, which is the shortest ID-based signatures so far.

A Tight Security Reduction Identity-based Signature Scheme

Abstract
In ACISP 2006, Paterson and Schuldt (PS) presented an inefficient identity-based signature scheme in the
standard model. Their scheme is obtained from a modification of Waters' identity-based encryption scheme. It employed two Waters Hash functions, one for identity, other for message, so the security reduction efficiency is very low. We slightly modify PS's scheme and change the parameters selection insecurity proof to obtain a tight security reduction identity-based signature scheme. The new scheme's security rests on computational Diffie-Hellman assumption.

Security Assurance for Dynamic Role Mapping in a Multi-Domain Environment

Abstract
Multi-domain application environments where the redistributed domains interoperate with each other are becoming a reality in Internet-based enterprise applications. The secure interoperation in a multidomain environment is a challenging problem. Role-based access control (RBAC) is used for specifying these security requirements of multi-domain applications in this paper. Then, role mapping relationship between domains is described by XML documents. Furthermore, the situations where dynamic role mapping violates separation of duties (SoD) which is one of the three basic security principles for the RBAC model are analyzed in detail, and relevant algorithms to detect the above security problem are designed in this paper.

Toward Assessing Vulnerability and Risk of Sensor Networks under Node Compromise

Abstract
It is important to assess vulnerability of network and information system to countermeasure against a variety of attack in effective and efficient way. But vulnerability and risk assessment methodology for network and information systems could not be directly applied to sensor networks because sensor networks have different properties compared to traditional network and information system. This paper proposes a vulnerability assessment framework for cluster-based sensor networks. The vulnerability assessment for sensor networks is presented. Finally, the case study in cluster-based sensor networks is described to show possibility of the framework.

A Security Model for Networked Manufacturing System
Lujiong Wang, Aiping Li, Liyun Xu
Institute of Advanced Manufacturing Technology
Tongji University, Shanghai 200092, China

Abstract
Information Security is one of the major concerns of networked manufacturing system. A security model for networked manufacturing system is presented. A role-based access control model with time character is discussed. For time constraint affecting more than one session, the method of Analytical Hierarchy Process is proposed to calculate the weight of each session, according to which maximum live time of each session is set. An illustrative example using the security model is demonstrated.

An Email Geographic Path-based Technique for Spam Filtering

Abstract
This paper proposes a spam filtering technique called EGPA (Email Geographic Path Analysis) which allows network administrators to cut off some spam traffic with forged route information on email delivery. In our approach, route information is first extracted to build email path, and then geographic
location of each node in the path is determined. Further, we detect spam by nodes’ geographic information deviation. We evaluate the performance of our EGPA algorithm, using email traffics captured from one backbone link which crosses geographic boundary of China. Experimental results indicate that the method is effective and practical, with at least 13.9% reduction of email traffic for anti-spam.

**An Improved DAD Check Scheme MLD-Based in FHMIPv6**

SUN Wei, CHEN Lin, SONG Jian
Modern Networking Education College
Lanzhou University of Technology
Lanzhou Gansu Province, 730050, China
sunwei@lut.cn, darlingchen2008@hotmail.com

**Abstract**

The HMIPv6 protocol has been proposed as an improved technology of MIPv6 to solve the problem that the handover management mechanism between macro-mobility and micro-mobility. But a majority of handover latency is occupied by DAD check of RCoA and LCoA, by which handover efficiency has been affected badly. Therefore, in this paper it is proposed a DAD Check scheme MLD-Based and the realized process of arithmetic has been described in theory. It is proved that the handover arithmetic has been optimized, handover efficiency has been enhanced and the mobility management has been improved by NS-2 simulation. Keywords: DAD check; MLD; HMIPv6; mobility management;

**An Efficient Survivability Hierarchy Analysis Model for Networked Information System**

Lejun Zhang, Lin Guo, Wu Yang, Wei Wang, Yongtian Yang
Information Security Research Center of Harbin Engineering University,
Harbin Engineering University, Harbin, 150001, China
zanglejun@hrbeu.edu.cn; guolin@hrbeu.edu.cn; yangwu@hrbeu.edu.cn; w_wei@hrbeu.edu.cn; yangyongtian@hrbeu.edu.cn

**Abstract**

This paper presents an efficient survivability hierarchy analysis method for networked information system. In the hierarchical model, the top level is the survivability of system; the second is the survivability of essential service; the third is the survivability of atomic module; the lowest one is vulnerability. With the help of attack graph, the survivability (3R+A) is quantified according to the records of the QoS before and after attack. Keywords: survivability, hierarchical model

**Testing Approach of Component Security Based on Fault Injection**

Jinfu Chen, Yansheng Lu and Xiaodong Xie
college of Computer Science and Technology, Huazhong University of Science and Technology,
Wuhan City, Hubei Province, 430074, China
cjffnet@gmail.com

**Abstract**

Component-Based Software Engineering (CBSE) has been the research focus in the field of software engineering at present. But problems with their reliability and security of components have not yet been resolved, which worried the component developer and user. Testing the software components is an important approach which guarantees and enhances their reliability and security. This paper proposes a testing approach of component security based on fault injection (TAFI), and then defines and
A Novel Approach to Network Security Situation Awareness Based on Multiperspective Analysis

Abstract
Describing the security situation and its trend is the research hotspot of network security. As a new research field, Network security situation awareness (NSSA) includes three phases: situation perception, situation evaluation and situation prediction. This paper proposes a novel approach to NSSA model. The situation evaluation model adopts a multi-perspective analysis. It uses the description of security attacks, vulnerabilities and security services to evaluate current network security situation. The situation prediction model adopts time series analysis. It uses past and current situation map to forecast future network security situation. Simulation results show that the model is suitable and efficient.

A Quantitative Evaluation Model for Network Security
Dapeng Man, Wu Yang, Yongtian Yang, Wei Wang, Lejun Zhang
Information Security Research Center,
Harbin Engineering University, P.R.China

Abstract
The existing network security assessment models have the problems of inadequate capacity of quantitative analysis and lacking for vulnerabilities correlation. To address these problems, a hierarchical network security evaluation model is proposed. The network is divided into vulnerability level, service level, equipment level and network level. The model uses attack graph to correlate the network vulnerabilities, and then calculates the probabilities of successfully exploiting the vulnerabilities. On this basis, the quantitative risks of each level are calculated. Since this model much more accords with the features of network structure, it is an effectively guidance for the network administrators to develop and improve the network security policies.

A Period-finding Method for Shor’s Algorithm
Weiqiang Zhang Chen Xu Feipeng Li Jiqiang Feng
Institute of Intelligent Computing Science
Shenzhen University Shenzhen China
weiqiangzhangchina@yahoo.com.cn

Abstract
Shor’s algorithm is a significant quantum algorithm for factoring a number N. The key technique of the Shor’s algorithm is turning the factoring problem into the problem of finding the period of a function. Based on the key technique and the monotony of the mode function, an approach how to determine the period of a function is introduced. Meanwhile, important parameter selection for period-finding is optimized. Several experiments discussed imply that the approach and the parameter selection are both rigorous.

Hidden-ID Authentication Scheme and Its SVO-Logic based Formal Analysis
Jin Jiang 1,2, Lei Li 2, Zhihong Huang 2
Abstract
Generally, users are required to submit their identity information at the beginning of the authentication process. Hence, adversaries can follow the tracks of specified users' information and decrypt the corresponding authentication messages. Against these security risks caused by identity information, this paper proposes a Hidden-ID authentication scheme, in which users can be authenticated without submitting their identity information directly. Meanwhile, a formal analysis of the Hidden-ID authentication scheme based on SVO Logic is also presented, which shows the proposed scheme meets the design objectives.

Research of Software Reliability Based on Synthetic Architecture

Abstract
In this paper we introduce some typical architecture-based software reliability model for software architecture reliability estimation, and modify model of software reliability estimation so that to improve precision of estimating software architecture reliability. Our approach is based on Markov chain properties and software architecture. At the same time, we propose the method of how to use the modified model to make a reliability estimation in synthetic architecture so that to expand the application domain of this model. In addition, we conduct an experiment on to validate this method.

An EMAIL Based Automated Trust Negotiation Model *
Zhensong Liao, Hai Jin, Deqing Zou, Chisong Li
Services Computing Technology and System Lab
Cluster and Grid Computing Lab
Huazhong University of Science and Technology, Wuhan, 430074, China
hjin@mail.hust.edu.cn

Abstract
Automated trust negotiation (ATN) is an important means to establish trust between strangers through the exchange of digital credentials and mobile access control policies specifying what combinations of credentials a stranger must submit. While ATN provides a good mechanism to share resources in the open and distributed environments, there still exist some pitfalls. A notable problem is that the negotiation process is easy to be interrupted, which leads to negotiation failure. Therefore, current protection techniques are somehow complex and heavyweight, which greatly limits ATN's applications. To solve these problems, an Email Based ATN Model (EBAM) is proposed. A credential template and an access control policy template are specified to carry information. All the transmitted messages are encrypted by private keys. The data exchange is realized through the negotiators' emails. A use case is given to show how it works, which proves the model sound and reasonable.

An Artificial Intelligence Based Approach for Risk Management Using Attack Graph

Abstract
In today's large complex organizational network, security is a challenging task for most of the administrators. The typical means by which an attacker breaks into a network is through a series of exploits, where each exploit in the series satisfies the pre-condition for subsequent exploits and makes
acausal relationship among them. Such a series of exploits constitutes an attack path and the set of all possible attack paths form an attack graph. Present-day vulnerability scanners are able to identify the vulnerabilities in isolation but there is a need for correlation among these vulnerabilities to identify overall risk of the network. In this paper we propose a novel approach by finding out an attack path consisting of logically connected exploits and extending it to an attack graph. The solution also finds out the set of root cause vulnerabilities for overall security threat while taking care the inherent time and scalability problem of attack graph generation.

**Game Theory Based Optimization of Security Configuration**

Jin SHI, Yin LU, Li XIE
State Key Laboratory of Novel Software Technology, Nanjing University
Nanjing 210093, P.R.China
{shijin,luyin}@dislab.nju.edu.cn, xieli@nju.edu.cn

**Abstract**

How to make a trade off between the security of systems and the usability of users is an important issue in network security configuration. To resolve this problem, an optimization method of security configuration based on game theory is proposed. Firstly, a security configuration model based on non-cooperative game is built which infers the optimal strategy of systems and users respectively by calculating their strategies and incentives. Secondly, to optimize security configuration further, it cooperatively optimizes the individual optimal strategy by cooperative game, thus eliminating the cases that individual optimal is not the overall optimal. An illustrated experiment shows that this method can coordinate the security of network systems and usability of users so that the security configuration of system is optimized magnificently.

**Adaptive Trust Management in MANET**

Feng Yunfang
HuangShi Institute of Technology Huangshi
College of Computer
Huangshi, Hubei, China, 435003
fengyunfang1968@126.com

**Abstract**

In MANET, trust management is an effective measure of interoperation and collaboration. The authorization decisions to collaborate with a stranger are often tackled by two different trust management systems: a policy-based approach, where authorization decisions are built on logical rules and verifiable properties encoded in signed credentials, and a reputation-based approach, based on collecting, aggregating and disseminating reputation among the principals. However, the overhead caused by proof of compliance on authorization and the un-availability caused by lack of evidence to make decision may negate the strong and objective security advantages of a policy-based approach, whilst vagueness, complexity and inaccurate characterization caused by reputation evolution may eliminate the quantitative and flexible advantages of reputation-based approach. Actually an integrated approach would enhance significantly trust management systems. We integrate the notion of policy proof and reputation evolution into trust management such that the decision process is aware of not only the strong and objective security implications, but also the calculability and the availability security implications. Finally, a trust management framework that incorporates trust is presented.

**A New Provably Secure Authentication and Key Agreement Mechanism for SIP Using Certificateless Public-key Cryptography**
Abstract
The authentication procedure in session initiation protocol (SIP) typically uses HTTP digest authentication, which is vulnerable to many forms of known attacks. This paper proposes a new secure authentication and key agreement mechanism based on certificateless public-key cryptography (SAKA) between two previously unknown parties, which provides stronger security assurances for SIP authentication and media stream, and it is provably secure in the CK security model. Due to using certificateless public key cryptography, SAKA effectively avoids the requirement of a large Public Key Infrastructure and conquers the key escrow problem in previous schemes.

A Model of Hierarchical Key Assignment Scheme with CRT

Abstract
A model of the hierarchical key assignment scheme is established in this paper, which can be applied with any one-way function. With the scheme, the users in the system are divided into several groups according to their predecessors and have a parameter with the group. Applied with CRT, a user key is bounded with its ID in the scheme. By sharing a parameter within the group, the scheme will use less space for parameters. Also, the scheme model is able to meet the optimal dynamic control property. Together with the security, dynamic and complexity analysis of the scheme model, this paper also includes an application example of the model with the discrete logarithm.

A Game Theoretic Method for Decision and Analysis of the Optimal Active Defense Strategy

Abstract
This paper presents a game-theoretic method for analyzing the active defense of computer networks. We regard the interactions between an attacker and the defender as a two-player, non-cooperative, zero-sum, finite game and formulate an attack-defense game (ADG) model for the game. An optimal active defense strategy decision (OADSD) algorithm is developed using the ADG and cost-sensitive model. Optimal defense strategies with minimizing costs are used to defend the attack and harden the network in advance. Finally, experiments show that our ADG model and the OADSD algorithm are effective in reducing the overall cost of defense systems and defend attacks that may occur in the future.

Handling Information Release and Erasure in Multi-threaded Programs
Li Jiang, Lingdi Ping, Xuezeng Pan
College of Computer Science and Technology, Zhejiang University, China
ljiang@zju.edu.cn; ldping@cs.zju.edu.cn; xzpan@cs.zju.edu.cn

Abstract
Language-based information flow security properties such as noninterference ensure confidential data cannot interfere with public data. But in real computing systems sensitive information sometimes needs to be released or to become more confidential. In this paper, we propose a new security property including support for both information release and erasure. Since the property is in the style of strong bisimulation equivalence, it is applicable to multi-threaded programs. To ensure that declassification cannot be exploited to reveal more secret data than intended, our property addresses what information may be released. Moreover, the property guarantees that dynamic upgrading the security label of data due to erasure requirement cannot affect the publicly visible behavior.

A Quantitative Security Model of IMS System
Xiaofeng Qiu1,2 Ning Zhi2 XinXin Niu2
1.School of Continuing Education
2.Information Security Center, State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications
qiuxiaofeng@bupt-bcnl.com ning1133@sina.com xxniu@bupt.edu.cn

Abstract
Many efforts have been made on survivability model of various systems, but little of them focus on controller application layer of telecommunication network, even less can be realized and applied. In this paper, an applicable method is provided to model the controller layer of telecommunication network such as IMS (IPMultimedia System), which has complicated message exchanges. How to calculate survivability quantitatively is also introduced.

An Efficient Authentication Strategy for Reprogramming of Sensor Networks

Abstract
Remote reprogramming of sensor nodes through the wireless channel is a very important function for efficient sensor networks management. Traditional reprogramming protocols do not provide any security scheme, hence make the sensor network vulnerable to some kinds of simple attacks; new secure reprogramming protocols use asymmetric cryptography schemes needing many computational overhead and large memory size, may not be acceptable for wireless sensor node. An efficient authentication strategy for reprogramming of sensor networks is presented in this paper; it hides asymmetric key with code attestation running on a legitimate node and base station separately, and has dynamic characteristics through transmitting a parameter r from the base station to the sensor. By means of integrating this strategy with existing reprogramming protocol MNP, this strategy can ensure security of reprogramming at lower communication cost and short delay through simulation.

Protecting XML Databases against Ontology-based Inference Attack
Lu Yang, Xiao Junmo and Liu Jing
Institute of Communication Engineering
PLA University of Science and Technology
Nanjing, Jiangsu Province 210007, China
luyangnsd@163.com, jmxiao753@vip.sina.com, liujing@163.com

Abstract
In this paper we study the ontology-based inference attack problem in large distribute XML databases. Supported by the semantically rich ontologies, the ontology-based inference attack can lead to undesired information disclosure via replicated XML data under different syntactic formats and inconsistent secure classifications. To address this new security problem, we propose a framework called Semantic-based XML Security Inference Engine (Semsie) to detect replicated XML data exposed to ontology-based inference attack. Compared to the existing works, our main technical contribution is the development of a semantic matching module based on the successful matching methods. Supported by this module, Semsie can detect the inference channels resulting from the inconsistent security classifications of replicated data automatically without basing the detecting process on any knowledge bases pre-defined manually.

Image Encryption Algorithm of Double Scrambling Based on ASCII Code of Matrix Element
Guodong Ye
College of Science,
Guangdong Ocean University
Zhanjiang, Guangdong, China

Abstract
A new image encryption algorithm of doublescrambling based on ASCII code of image matrix element is proposed in this paper. The new algorithm implements position scrambling and gray scrambling at the same time, and overcomes the shortcoming of traditional algorithm that single algorithm can only deal with position scrambling but not gray scramblings simultaneously. Finally, tests show that the new image encryption algorithm presented has better scrambling effect and can effectively ensure the security of protected image than traditional algorithm.

SEA: Secure Encrypted-Data Aggregation in Mobile Wireless Sensor Networks
Shih-I Huang1,2 Shiuhpyng Shieh2
Industrial Technology Research Institute1
Dept. of Comp. Sci. and Info. Eng., National Chiao Tung University2
E-mail: sihuang@itri.org.tw, {sihuang, ssp}@csie.nctu.edu.tw

1 Abstract
This paper proposes a Secure Encrypted-data Aggregation (SEA) scheme in mobile wireless sensor networks (MWSN) environment. Our design for data aggregation eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. In contrast to conventional schemes, our proposed scheme provides security and privacy, and duplicate instances of original readings will be aggregated into a single packet; therefore, more energy can be saved.

Multi-Perspective Quantization Model for Cyberspace Security Situation
Tan Xiaobin
Department of Automation
University of Science and Technology of China
Hefei, Anhui, P.R.China
xbtan@ustc.edu.cn
xihs@ustc.edu.cn

Abstract
Cyberspace security situation is the status and trends of whole network’s security, which is influenced by hardware, software and user’s behaviors of whole network, so the cyberspace security situation awareness is the perception, comprehension, and forecast of cyberspace security situation. However, according to the different view points and purpose, it is very difficult to give a widely accepted result. Multiperspective quantization model for cyberspace security situation awareness employs three perspectives, namely, threat oriented, essential oriented, and holistic, for evaluating and forecasting the security of network system. The aim is to try to ensure objectivity, and because it adopts multi-perspective parameters, the results can be used in various purposes of cyberspace security situation awareness. This model is suitable for all kinds of users, and it can help users get objective results.

Secure and Flexible Digital Rights Management in a Pervasive Usage Mode
Ma Zhaofeng, Yang Yixian and Niu Xinxin

Abstract
With the development of storage and computing technologies, digital content such as music, digital movies, games, cartoon and DV et al gets more and more popular for entertainment, how to control
The rights of digital content are now becoming a very important issue. In this paper, a secure and flexible Content Protection Secure DRM scheme (named CPSec DRM) is proposed for online/offline rights management, in which content objects (COs) and rights objects (ROs) were separated respectively, the COs were encrypted by content encryption key (CEK), while ROs were encapsulated rights encryption key (REK) that is related to the device information of the end user. Therefore, if ROs were illegally copied and spread, however, it will not pass the authentication of license verification. As for domain and offline license management, a license transfer scheme was developed for N-total sub-licenses redistribution, once the sublicenses were released to N copies, then the master license cannot be transferred and redistributed again. The proposed CPSec DRM scheme does not only support online rights management, but can still work in an offline mode for pervasive usage.

**Controlled Secret Leakage**

Tianjie Cao, Shi Huang, Hui Cui, Yipeng Wu, Qihan Luo
School of Computer, China University of Mining and Technology, Xuzhou, 221166, China
tjcao@cumt.edu.cn

**Abstract**

How to leak authoritative secrets in an elegant way? The paper aims to solve this problem. The desired security properties i.e. Semantic-Security; Recipient-Designation; Verification-Dependence; Designated-Verifier Signature-Verifiability; PublicSignature-Verifiability; Recipient-Ambiguity; Designated-Verifier Recipient-Verifiability; PublicRecipient-Verifiability; Signer-Ambiguity; Signer-Verifiability are specified in secret leakage. Based on Chow-Yiu-Hui’s ID-based ring signature scheme and techniques of zero-knowledge proof, an ID-based controlled secret leakage scheme is proposed. The proposed scheme satisfies all specified security properties and can be used in trust negotiation.

**A New Method Considering Creditability Degree and Connection of Buyers and Sellers in E-Broker System**

**Abstract**

In the situation that there is not enough consideration about the trust level of the buyers and sellers in the existing connection methods which considers buyers’ attributes more, a connection method based on the buyers and sellers is proposed, which heightens the importance of the trust level of the users in the computation of the transaction success probability. In this paper, we propose a material computing method for the attribute value, which is used in the new connection method. We use an improved trust model based on multiple factors for computing the users’ creditability degree, which heightens the validity of the user’s creditability degree. Theory and experiments all show that this method is more objective.

**Modified Original Smart Cards and Smart Card Clone Countermeasures**

**Abstract**

Conditional Access Systems are used in Pay-Tv Systems to ensure conditional access to broadcasted data and charge subscribers a subscription fee. Smart cards are end-user security devices to store subscribers' entitlements, required to access data. On the other hand, pirates clone or modify smart cards to gain access to broadcasted data without paying any fees. This paper presents new countermeasures, based on fingerprints, to avoid smart cards cloning or modifying in Conditional Access Systems for digital TV broadcasting.
Design of a New Selective Video Encryption Scheme Based on H.264
Yajun Wang, Mian Cai, Feng Tang
Beijing University of Technology, China, 100022
wangyajun@emails.bjut.edu.cn

Abstract
With the development and application of H.264 standard, the technology of H.264-based video data security becomes increasingly important. This paper proposes a new selective encryption scheme based on H.264, it combines the AES OFB mode with the sign encryption algorithm, and encrypts DCs and parts of ACs respectively. This method not only keeps advantages of former selective encryption algorithms in computational complexity and error-propagation prevention, but also efficiently makes up for the deficiency in security and compression performance. Experimental results show that the proposed method exhibits low complexity and good security, and it has little effect on compression ratio and supports error propagation prevention. Moreover, it is suitable for secure transmission of mobile multimedia and wireless multimedia network based on H.264.

CMS System of DRM Technology based that Use Web Contents Certification Code

Abstract
From diversification of contents, CMS (content Management System) is operated variously for government official of contents. Present CMS plain applies a DRM technology and is protecting contents copyright based on only possession members. Therefore, global use of contents is limited and use is impossible mutually and original copyright protection of contents is impossible. Therefore, in this paper, we are designed License module of public key base for copyright protection. This packager module that encrypt contents to base, encoded contents un-packager module, contents public ownership server and client module that decode encryption design. CMS between heterogeneous supports contents use limitation and copyright protection based on a DRM technology that proposed so that can take advantage of various contents in various CMS because shares integration metadata and operates integration CMS through transaction server and uses web contents certification code.

A Context-aware Trust Establishment and Mapping Framework for Web Applications

Abstract
In order to reflect the dynamic feature of situations and of peers’ behavior more accurately, context information, which contains different attributes of situations, should be considered explicitly when evaluating trust. A context-aware trust establishment framework based on Bayesian networks is proposed. In our proposal, the contextual factors are inferred statistically, not assigned in ad hoc way as most existing solutions. We also propose a Bayesian trust mapping approach between related contexts to help application agents infer the trustworthiness in an unfamiliar context from the trust information in other contexts. We argue that the relevance of contexts is specific to agents and it should not be estimated independent of agents’ trust or even fixed as in other frameworks. Our approach makes the relevance measurement implicit together with trust mapping through Bayesian networks. Simulation experiments show that our system can make more accurate trust inferences than ad hoc context-aware systems.

A Digital Fingerprint Coding Based on Turbo Codes
Zhiguang Zhang, Xiaosu Chen, Miao Zhou
College of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan 430074, China
zgzhang@mail.hust.edu.cn
Abstract
Digital fingerprinting is a technique for identifying unauthorized copy and tracing back to its user. The distributor marks each individual copy with a unique fingerprint. A group of colluders having access to multiple copies with different fingerprints may construct a pirate object with a fingerprint that cannot be traced. In this paper, we propose a new collusion-secure fingerprinting code which is composed of outer Turbo codes and inner codes based on Boneh-Shaw model. The collusion security, code length and performance are proved and analyzed. The results indicate that the proposed scheme has shorter code length and achieves effective traitor-tracing in largescale contents distribution environments.

A Stream Cipher Engine for Ad-hoc Security

Abstract
Overall demands of ever growing ubiquitous environment are security, speed, and power consciousness in processing huge amount of multimedia data. Especially, the critical issue is the security threat due to the spread of mobile platforms. Then, ad-hoc security is very important to keep the temporary security of ubiquitous devices without permanent network infrastructure. A practical solution to meet these demands is a safety aware, high performing single chip processor. According to this scheme, we have exploited hardware cryptography embedded processors named RAP (random addressing accelerated processor) and HCgorilla. We have conceived from RAP and HCgorilla cryptography called RAC (random addressing cryptography). RAC is a practical cipher promising formultimedia streaming that has ability to keep the temporary security of ubiquitous devices without usual network infrastructure. Abstracting the potential feature of RAC from RAP and HCgorilla, we have developed a multimedia stream cipher engine that has a compact multicore processor structure. In this article, we describe the overall architecture and cryptographic structure of the stream cipher engine, RAC run on the stream cipher engine and its ad-hoc aspects compared with usual cipher techniques.

Secure Hop-Count Based Localization in Wireless Sensor Networks

Abstract
Many sensor network applications rely on sensors' location information. However, most of existing locationalgorithms assume a non-adversarial environment or assume beacons lying within 1-hop. In this paper, we focus on Hop-Count based localization (multihop) and developa Secure Hop-Count based Localization scheme called SHOLOC, to make localization attack-resistant. In SHOLOC, we assume both ordinary nodes and beacon nodes can be moving, and the whole network periodically restarts localization. SHOLOC proposes a protocol to authenticate beacon information and protect hop count from being arbitrary changed. SHOLOC employs beacon nodes to detect wormhole attacks. Theoretical analysis and simulation results are presented. Our conclusion also includes two interest findings: 1) hops-count increment attacks are not effective to Hop-Count based algorithms, 2) filter mechanisms such as least mediansquares (LMS) are not resistant to wormhole attacks, and our method of detecting at beacon nodes side work well.

A Scheme for Protecting Mobile Agents Based on Combining Obfuscated Control Flow and Time Checking Technology

Abstract
Mobile agents are programs that travel autonomously through a computer network in order to perform some computation or gather information on behalf of a human user or an application. In most applications, the security of mobile agents is of the utmost importance. Obfuscation is a technique in which the mobile code producer enforces the security policy by applying a behavior transformation to the code before sending it to run on different platforms. This paper presents a protection scheme of mobile agent in network management application, which combining obfuscated control flow and time checking technology to verify the security of
Identity-Based Key Issuing Protocol for Ad Hoc Networks

Abstract
Secure key issuing is an important issue in identity-based cryptography. At present there are some key issuing protocols in ID-based cryptography, but existent protocols are not applied due to centerless, self-organization, free move and other distinct characteristics of ad hoc network. In this paper, we propose an identity-based key issuing protocol for ad hoc networks, in which it makes use of the blind signature to ensure the secure issuing of the private key of the nodes in public channel. None of the nodes can impersonate the users to obtain the private keys. And the protocol, which suits ad hoc networks, is secure against replay, man-in-the-middle and insider attacks.

A New Statistical Hitting Set Attack on Anonymity Protocols

Abstract
A new Statistical Hitting Set attack (SHS-attack) is presented, using the principle of statistical disclosure attack for reference, to effectively link senders and receivers of an anonymous system. We analyze previous work and some associated bottlenecks of statistical attack. Thereafter we design and implement an algorithm which has been proved computationally efficient. Compared with the previous SHS-attack, ours improves the accuracy of solution while all the recipients congregate in a small group, and effectively estimates the number of victim’s recipients which is hard to get in real-world. The simulations show that our attack is highly effective at compromising the end-to-end anonymity of the system.

Research on Video Watermarking Scheme Based on Chaos, DWT and JND Model
Abstract

The paper presents a novel and robust video watermarking scheme for copyright protection based on chaos, DWT and JND model of HVS. Firstly, in order to ensure security of watermarking and reduce the quantity of computation in the embedding process, we adopt a technique called chaotic selection to select the embedding frames from the video. To every selected frame, we transform it by DWT and detect the variation status of the coefficient in low frequency domain. Because HVS isn't too sensitive to the motive things, we choose those coefficients whose variations are large as the embedding coefficients. Finally, the watermarking signals are embedded and detected according to the JND model. The experimental results show that the proposed watermarking algorithm is robust to additive noise, MPEG compression, frame deleting and so on.

Robust Watermark Model based on Subliminal Channel

Abstract

Current watermark models cannot reflect the conflicting relationship among cover fidelity, watermark robustness and watermark capacity. And there is no effective guidance for designing robust watermark algorithms in content security applications, such as the copyright protection. A robust watermark model based on subliminal channel for content security applications is proposed. In this model, the half symmetry of watermark communication is pointed out. Based on the model, the approaches to solve the conflicting relationship are presented as to increase the entropy of cover, to decrease entropy of watermark message and to increase mutual information between cover and watermark through cover transformation, watermark encoding, public and subliminal channel encoding. The conditions and methods of the cover transformation and watermark encoding are presented. This model and its approaches will offer theory guidance for researches on robust watermark algorithms in content security applications.

Two-dimensional Wavelet Filters for Watermarking

Jianwei Yang, Wenbing Chen, Guosheng Cheng
College of Math & Physics,
Nanjing University of Information Science and Technology,
Nanjing, 210044, P. R. China
yjianw@hotmail.com

Abstract

Discrete non-separable wavelet transform (DNWT) reveals more features than discrete separable wavelet transform (DSWT) does. We propose to embed watermark by DNWT. To construct non-separable wavelet filters, we introduce a novel transformation – shift unitary transform (SUT) of conjugate quadrature filter (CQF). Based on this transformation, a parametrization construction of two-dimensional wavelet filters is provided. Non-separable wavelet filters derived by this method are applied to a blind watermarking scheme. Experimental results show that watermarking scheme based on these filters is more resistant to sharpening than watermarking scheme based on separable wavelet filters does.

Analysis on the Sensitivity Attack to Watermarking Schemes with Patchwork Detection Boundaries

Qiyang Zhao, Zhonglin Wang, Baolin Yin
NLSDE, Beijing University of Aeronautics and Astronautics
37# Xueyuan Road, Haidian District, Beijing, China
zhaoqiyang, wangzhonglin, yin@nlsde.buaa.edu.cn
Abstract
The sensitivity attack is a main threat to the security of watermarking schemes with open detectors. By the attempts across the detection boundary, the attackers gain adequate information of the embedded watermark to remove it without introducing serious distortions into the watermarked works. In some image watermarking schemes, the detection boundaries are the patchworks of certain numbers of hyperplanes. Here the existing sensitivity attacks are not suitable anymore for the detection functions have numbers of different gradients. The letter proposed a new sensitivity attack in which the attacking directions were calculated with a certain number of gradients estimated separately with the old sensitivity attack. Our experiments show the new attack can remove the watermarks successfully without seriously tampering the fidelity.

A Blind Video Watermarking Algorithm Based on 3D Wavelet Transform
Xu Da-Wen
Ningbo University of Technology
School of Electronics and Information Engineering
Ningbo, 315016, China
dawenxu@126.com

Abstract
A blind video watermarking algorithm based on 3D wavelet transform is proposed in this paper. The original video frames are divided into 3D-blocks. According to HVS properties, the motive block with complex texture is selected to embed the watermark. The CDMA encoded watermark is embedded into the wavelet coefficients of the selected sub-block. Blind recovery of the embedded data is achieved using the auto-correlation of the orthogonal codes. Experimental results show the watermarked frames are indistinguishable from the original frames subjectively and the proposed video watermarking algorithm is robust against the attacks of additive Gaussian noise, frame dropping, frame averaging and lossy compression.

Adaptive Encrypted Information Hiding Scheme for Images

Abstract
Information hiding enables the seller to hide additional bits into multimedia content in an imperceptible manner. In most information hiding schemes for copyright protection, the seller always knows the embedded information uniquely identifying the buyer. However, it causes both framing issue and repudiation issue. To solve these problems, a variety of watermarking protocols have been proposed based on the encrypted information hiding scheme. In this paper, a new encrypted information hiding scheme with adaptive capacity is proposed, and it can improve the resistance against JPEG compression after decryption and detect image tampering at the information extractor. The blind information extractor employs the same threshold criterion and parameters as information embedding. The proposed encrypted information hiding scheme is a new solution to implementing the existing watermarking protocols.

Using Chain Graphical Model to Analyze the Efficacy of a Chinese Medicine

Abstract
This paper first uses the chain graphical model, an extension of Bayesian network, to study the efficacy of Jiangzhiling tablet, a new type of Chinese medicine. This novel approach provides an easily interpretable empirical description of the conditional independence structure and causal relationships among the relevant variables.

Gene Selection Using Neighborhood Rough Set from Gene Expression
Profiles

Abstract
Although adopting feature reduction in classic rough set theory to select informative genes is an effective method, its classification accuracy rate is usually not higher compared with other tumor-related gene selection and tumor classification approaches; for gene expression values must be discretized before gene reduction, which leads to information loss in tumor classification. Therefore, the neighborhood rough set model proposed by Hu Qing-Hua is introduced to tumor classification, which omits the discretization procedure, so no information loss occurs before gene reduction. Experiments on two well-known tumor datasets show that gene selection using neighborhood rough set model obviously outperforms using classic rough set theory and experiment results also prove that the most of the selected gene subset not only has higher accuracy rate but also are related to tumor.

An Improved Algorithm for Iris Location
Harbin Institute of Technology
No.92, West Da-Zhi Street, Harbin, China
zhifang.wang@ict.hit.edu.cn

Abstract
Biometric technologies have shown much more importance in various application. Among them, iris recognition is considered as one of the most reliable and accurate technologies. As the first step of iris recognition, the location of iris will affect the performance of the whole system. This paper proposes an improved algorithm to locate iris and eyelids. Morphological operation is applied to remove eyelashes in the process of iris boundary location. And optimal step length is calculated to reduce search time. Experimental results demonstrate that the proposed iris location algorithm is able to achieve a good performance with accuracy more than 97.6%.

Dynamical Behavior of Three-Order Cellular Neural Network with Application in Image Secure Communication

Abstract
The paper analyzes dynamic behaviors of three order Cellular Neural Network (3-order CNN). It shows that 3-order CNN is symmetric with regard to the origin; the system is dissipative and asymptotic motion settles onto an attractor. The system has diverse chaotic attractors with different parameters. So 3-order CNN can be applied in secure communications owing to its chaotic behaviors. The paper combines 3-order CNN with DES to propose an scheme of image secure communication. The results of security analysis indicate that this scheme not only has a large key space but also has a very sensitivity with respect to the initial conditions of 3-order CNN and the key of DES.

Generalized Synchronization Theorem for Non-autonomous Differential Equation with Application in Encryption Scheme

Abstract
This paper introduces a constructive theorem for designing a non-autonomous driven system, which can achieve generalized chaos synchronization (GCS) to a driving system. As a first application, an encryption scheme is established based on GCS non-autonomous systems. This scheme has the functions of the datum authentication and one-time-pad. As a second application, the non-autonomous Driven van der Pol...
The oscillator is selected as a driving system. An invertible transform $H$ is introduced to design a driven system such that the two systems are in GS with respect to $H$. Based on the GCS systems and the scheme one can encrypt and decrypt original information without any loss. The analysis of the key space and sensitivity of key parameters show that this scheme has sound security. The keyspace of the scheme is larger than $2^{148}$. It can be expected that our theorem provides a new tool for studying and understanding the GS phenomena and the scheme offers a new method for information encryption.

**The Representation of Chinese Semantic Knowledge and Its Application in the Document Copy Detection**

**Abstract**

Digital documents are easily copied and distributed illegally. Document copy detection is a powerful tool to protect the author’s intellectual property and to improve the efficiency of information retrieval. It is difficult for the existing copy detection systems to identify the sentence structure changed copies. To address the problem, we research the semantic level of natural language processing and propose a document copy detection method based on Chinese semantic knowledge. We introduce the realization mechanisms of Chinese language analysis, which contains syntactic parsing and semantic analyzing. We also report on the experimental comparison the proposed method with the representative document copy detection systems. The results are satisfying.

**Defaults Assessment of Mortgage Loan with Rough Set and SVM**

Bo Wang\(^1\), Yongkui Liu\(^1\), Yanyou Hao\(^2\), Shuang Liu\(^1\)

\(^1\) College of Computer Science and Engineering, Dalian Nationalities University, China

\(^2\) Dalian Branch of China Construction Bank, China

E-mail: wangb@dlnu.edu.cn

**Abstract**

Credit risk is the primary source of risk to financial institutions. Support vector machine (SVM) is a good classifier to solve binary classification problem. The learning results of SVM possess stronger robustness. We adjust these penalty parameters to achieve better generalization performances with using grid-search method in our application. In this paper the attribute reduction of rough set has been applied as preprocessor so that we can delete redundant attributes, then default prediction model of the housing mortgage loan is established by using SVM. Classification performance is better than some other classification algorithms.

**Optimistic design of jetty road height based on genetic algorithms**

YAN-LONG QIN\(^1\) MING-CHANG LI\(^2\) ZHAO-CHEN SUN\(^2\) YU-XIA YANG\(^1\) HAI-BIN Xu\(^1\)

\(^1\) Research Division of Offshore Engineering, Research Institute of Engineering Technology
Abstract
Jetty road is the link of onshore to artificial island. It is used for marine oil exploitation and production. As a result of special terrain conditions of shallow beach area affected by tide, the project construction of jetty road has characteristics of higher investment, higher degree of risk, longer construction duration and higher maintenance costs. Overflow roads have been developed recently with height lower than the highest water level. The roads are different from usual roads in that overflow is allowed during high tide. The most important factor that influences the cost is the height of jetty road. To assure reasonable working days, maintain quality and reduce the project cost, it is important to determine a proper road height. Combining with full life-cycle cost theory, this paper presents a genetic algorithms (GAs) model for multi-objective optimistic design of jetty road height. The model is applied to oil field around Bohai Sea, and the numerical results show that the optimistic models perform well for optimistic problem and reduce the engineering cost.

Calculation and Analysis of Double-fed VSCF Induction Generator Operating Performance

Abstract
By using electromagnetic field theory and calculus of variations, the mathematic model of double-fed variable-speed constant-frequency (VSCF) wind generators was established firstly in this paper, and the two-dimensional transient electromagnetic field finite element method (FEM) was presented. To satisfy the requirement of VSCF, the electromagnetic field was coupled with the outside circuit in FEM calculation, and the stator terminal voltage was taken as the convergence condition. Rotor exciting current was iterating calculated, and the performance of double-fed wind generators at different speed and different load was analyzed. Then the obtained results were compared with the experimental data, from which it could be seen that the calculated results satisfy the engineering requirements well. All these provide some useful reference for the design and analysis of windpower generation system.

Research on Refining Mesh of Ship Hatch Corner Based on Transition Element

Abstract
The hatch corner of containership is the stress concentrated region, it is an effective way that finite element mesh (FEM) model of hatch corner intercepted from the whole ship is refined and analyzed again. In this paper, an automatic FEM refining algorithms for hatch corner is presented. Then the necessity of evaluating the stiffness matrix and the commonly-used construction method of transition element is presented, and the distance of the new nodes at the transition edge is computed with the linear discrete method. Computing the times of iterative according to the refining mesh size and the number of nodes on transition edge, LBC of the refining model is the displacement of the sparse mesh model boundary. Results show that the refining mesh analysis can reflect the stress change in the region with larger gradient of stress variation, thus the analysis result is better than the one obtained from global analysis.

Speech Tagging Based Improvement of the RSS Polymerization News
Abstract
Since a significant amount of redundant information causes problems like inefficiency or congestion in the existing RSS, a method using part of speech (pos) tagging to extract keywords is proposed to solve these problems. Firstly, the title of news is analyzed by using Chinese word segmentation and speech tagging system. Then, the keywords of the title are identified according to their part of speech. All of the extracted keywords are compared, categorized and stored according to the proposed criterion in this paper. In that case, all the news in the same category is identical or similar. Thus, redundant news can be hidden to users. According to the operation, statistics, comparison and analysis of system, and the introduction of the value of P and R and the evaluation parameter, a good redundancy removing result is achieved.

Low-Complexity Line-Based Motion Estimation Algorithm
Li Wern Chew, Li-Minn Ang and Kah Phooi Seng
School of Electrical and Electronics Engineering
The University of Nottingham
43500 Selangor, Malaysia.
(eyx6clw, Kenneth.Ang, Jasmine.Seng)@nottingham.edu.my

Abstract
The intensive computation in full search blockmatching motion estimation algorithm is a common problem in the development and implementation of many visual processing systems. In this paper, a lowcomplexity motion estimation algorithm that involves transforming multiple bits video sequence into a one-bit representation using a line-based approach is presented. The advantages of the proposed method are that it reduces the computational complexity of motion estimation process and allows real-time video processing without causing a significant decrease in the motion estimation performance.

A Particle Swarm Optimization for Resource-Constrained Multi-Project Scheduling Problem

Abstract
This paper considers the resource-constrained multi-project scheduling problem (RCMPSP) and makespan minimization as objective. We present a new particle swarm optimization (PSO) approach to solve this problem. The particle representation is based on precedence feasible of activities list. Based on the particle representation, a new update method based one-point crossover is proposed. The framework of PSO for the RCMPSP according to the representation and the update method is developed. We test the algorithm, and the experimental results show that our PSO outperforms other heuristic methods.

A Data Engine for Controller Area Network
Weiming Tong, Chengde Tong and Yong Liu
Department of Electrical Engineering and Automation
Harbin Institute of Technology
Harbin, 150001 P.R. China
dianqi@hit.edu.cn, tongchengde@126.com, yliu@hit.edu.cn

Abstract
In this paper, a data engine model for CAN is proposed, so devices simply based on CAN could communicate with other applications and users could maintain the simply CAN based network and interfaced devices while utilizing the existing configuration software. The concept of an I/O tag is put forward.
and CAN messages could be mapped into tag items. By handling time, event and user triggered transmitions, the data engine enables a computer based system to maintain positive in the network. To improve the performance of the system, a genetic method is suggested for a message filter implemented by hardware.

**A Supply Chain Network Design Model for Deteriorating Items**

Kai Tang, Chao Yang, Jun Yang

Institute of Management Science and Decision, College of Management,
Huazhong University of Science and Technology,
Wuhan Hubei 430074, China

hustjulian@yahoo.com.cn and chao_yang@mail.hust.edu.cn

**Abstract**

We consider a supply chain network design problem for deteriorating items, involving a single supplier, some potential distribution centers and multiple retailers. This problem is to determine how many distribution centers to set up, where to locate them, how to serve the retailers using these distribution centers, and to determine the optimal inventory policies for the whole supply chain network. The goal is to minimize the total deterioration, inventory, transportation and facilities location cost. We formulate this problem as a nonlinear mix-integer programming model. This model is an NP-Hard problem, so we present a Lagrangian relaxation solution algorithm and a Genetic algorithm to solve our model respectively. Finally, numerical examples are given to illustrate the application of these two algorithms, and our computational results show that Lagrangian relaxation algorithm is more efficient for our problem.

**The Study of Compost Quality Evaluation Modeling Method Based on Wavelet Neural Network for Sewage Treatment**

**Abstract**

Because of the complicated interaction of the sludge compost components, it makes the compost quality evaluation system appear the non-linearity and uncertainty. According to the physical circumstances of sludge compost, a compost quality evaluation modeling method based on wavelet neural network is presented. We adopt a method of reduce the number of the wavelet basic function by analysis the sparse property of sample data, and use the learning algorithm based on gradient descent to train network. We select the index of sludge compost quality and take the high temperature duration, degradation rate, nitrogen content, average oxygen concentration and maturity degree as the evaluation parameters. With the ability of strong self-learning and function approach and fast convergence rate of wavelet neural network, the modeling method can truly evaluate the compost quality by learning the index information of sludge compost quality. The experimental results show that this method is feasible and effective.

**Structural Analysis of Printed Mathematical Expression With Heuristic Rules**

**Abstract**

Structural analysis plays an important role in printed mathematical expression recognition. In this paper, a reliable and efficient structural analysis method of printed mathematical expressions is proposed. Based on the baseline algorithm, this method employs heuristic rules to analyze special symbols and makes use of a mechanism of error detection to correct the recognition errors. Experimental results show that this method gains favorable correctness and adaptability in analyzing formula expressions.

**System Level Assertion-Based Verification Environment for PCI/PCI-X**
PCI-Express
Min-An Song
Lee-Ming Institute of Technology
Department of Electronic Engineering

Abstract Circuit design becomes more and more challenging with the advent of SoC era in that several separate chips are to integrated into one chip. Of non-recurrent engineering (NRE) cost, verification takes a main part during entire design flow. Basically, there are two major problems in current verification procedure. This paper describes a new verification environment that cooperates assertion-based technique and firmware to provide a system level verification. Cores of this verification environment are bus functional models, bus protocol monitors, firmware layer software, and a set of checker implemented with TestWizard. We develop a platform to verify the behavior of PCI and PCI-Express devices efficiently. A set of performance evaluation tools are also be developed at the same time. By applying these performances tools, the verification environment helps designers not only verify the circuit function but evaluate the performance.

Design of Automatic Database Schema Generator based on XML Schema

Abstract With the recent expansion of e-commerce, B2B has surfaced as an area of substantial interest to the corporate world. B2B refers to economic transactions created among businesses through various networks, including the Internet. Currently, XML documents are partially used in e-commerce for exchanging information among businesses, and the core corporate systems are expected to be based on XML as webservice becomes more prevalent. In turn, many companies are becoming competitively involved in developing XML DBMS. Conventional XML DBMS studies use XML DTD to express the XML document structure. Since XML DTD defines simple format expressions, there are numerous difficulties in defining the XML document structure. In order to overcome such issues, this paper proposes an automatic conversion mechanism and algorithm for the relational database schema using the XML schema, which was selected as the W3C standard, in order to store XML data in the relational database generally used in data content storage based on the XML schema. Furthermore, a module will be developed for converting the XML schema design based on this approach into a relational database schema. This should allow efficient management of the XML data through the relational database.

Application of Least Squares-Support Vector Machine for Measurement of Soluble Solids Content of Rice Vinegars Using Vis/NIR Spectroscopy
Fei Liu, Yong He*, Li Wang
College of Biosystems Engineering and Food Science
Zhejiang University
268 Kaixuan Road, Hangzhou, 310029, China
yhe@zju.edu.cn

Abstract Visible and near infrared (Vis/NIR) spectroscopy was investigated to predict soluble solids content (SSC) of rice vinegars based on least squares-support vector machine (LS-SVM). Five varieties of rice vinegars and 300 samples were prepared. After some preprocessing, PLS was implemented for calibration as well as the extraction of principal components (PCs). Wavelet transform (WT) was used to compress the variables. These selected PCs and compressed variables were applied as the inputs to develop PC-LS-SVM and WT-LS-SVM models. The correlation coefficient (r), root mean square error of prediction (RMSEP) and bias for prediction were 0.958, 1216, and -0.310 for PLS, 0.997, 0.357 and 0.121 for PC-LS-SVM, whereas 0.999, 0.199 and 0.030 for WT-LS-SVM, respectively. A highand excellent precision was achieved by LS-SVM models. The results indicated that Vis/NIR spectroscopy could be successfully applied as a fast and high precision method for the measurement of SSC of rice vinegars.

Test Case automate Generation from UML Sequence diagram and OCL
Abstract
A new test cases generation approach is presented which based on UML sequence diagrams and Object Constraint Language (OCL). In this approach, a tree representation of sequence diagrams is constructed. Firstly traversal of the constructed tree for selecting conditional predicates from the sequence diagram is carried out. Then, post- and precondition is described by OCL. We transform the conditional predicates on the sequence diagram and apply function minimization technique to generate the test data. The generated test cases achieve message paths coverage and constraint attribute coverage of all objects which relate to the message. Lastly, the results of experiments show that this method has a better performance.

A Novel Cluster-based Routing Algorithm in Ad hoc Networks

Abstract
Aimed at the stability of clusters and load balancing, a novel cluster-based routing algorithm is proposed in this paper. In order to maintain the stability of clusters, speed and energy of mobile nodes, but not the identity and connectivity, are taken as the basis of cluster-head election. Try to make all the nodes share the role of cluster-head, so as to balance the traffic loads of the network, and to avoid invalidity caused by certain nodes exhausting energy. Based on clustering, the backbone network composed by cluster-heads, gateways, and compound gateways is constructed, which reduces the complexity of maintaining routing information and topology information, and simplifies the routing process in large hierarchical ad hoc networks. Simulation results show that compared to the lowest ID and largest connectivity algorithms, it has better performance on network life duration, energy consumption, and signaling overhead.

Estimation of System Power Consumption on Mobile Computing Devices

Abstract
The relationship between power consumption and parameters of system state on mobile computing devices is studied in this paper, using genetic algorithm and artificial neural network. Then based on this relationship, a run-time power consumption model is proposed to estimate the energy used on a per process basis. This result can help us to design an intrusion detection system for battery exhaustion attacks or give some advice on how to design a less power consumption program on mobile computing devices.

Cluster-Based System-Level Fault Diagnosis in Hierarchical Ad-Hoc Networks

Abstract
Fault diagnosis plays a very important role to the security of networks. Cluster-Based Comparison Diagnosis Algorithm for ad hoc networks is presented in this paper. By making use of the concentrative control function of the cluster-heads in hierarchical ad-hoc networks, the diagnosis process is optimized, and correct diagnosis for all mobile hosts can be implemented as dynamic network topology is presented. The correctness of the algorithm is proved and its performance is analyzed. Simulation results indicate that comparing with the Comparison-Based Fault Diagnosis Algorithm, the Cluster-Based Comparison Diagnosis Algorithm results in smaller system overhead.

An Energy Efficient Directed Diffusion Routing Protocol
Abstract
Directed diffusion is a classic data-centric routing protocol in Wireless Sensor Networks (WSNs). Indirected diffusion based WSNs, data generated by sensor nodes is named by attribute-value pairs. A sink requests data by sending interests. The data that match the interests are then "drawn" down towards the sink. Intermediate nodes cache or transform data, and direct energy saving becomes the most important consideration in designing routing protocols. In the directed diffusion, the path reinforcement scheme is designed for minimum delay and maximum data received during a certain period of time. However, the communication cost and energy balance over the whole WSNs have not been paid enough attention. To address these issues, we propose a novel path reinforcement scheme. Our proposed protocol is simulated and compared with the directed diffusion. The simulation results show that the proposed protocol is outperform directed diffusion in energy efficiency, energy balance over WSNs, and network lifetime.