A COMBINED PIXEL IN BLOCK HIDING METHOD AND HILL CIPHER FOR SECURE STENOGRAPHY TECHNIQUE

H.M. Abdul-kader, K. A. Moustafa, and A. B. Elsis

Faculty of computers and Information, Menofyia University, Shebin Elkom 32511, Egypt,
(hatem6803@yahoo.com, kaaly2006@yahoo.com and ashrafelsisi@hotmail.com)

Abstract

In this paper a secure stenography technique is proposed and developed. This technique uses the well known hill substation cipher. The proposed method is based on a modified spatial domain hiding method for images. The cover image is partitioned into number of squares blocks of equal sizes completely covering the image. The hided image is divided into pixels then the pixels are encrypted using hill cipher. Each encrypted pixel of the hided image is embedded into a block in the cover image. The selection is based on the nearest RGB value of the cover block to the value of the embedded image pixel. A certain deviation between the RBG value and the embedded pixel is allowed. The proposed technique is demonstrated using different examples. The perceptual transparency using PSNR is evaluated. The simulation results give satisfying hiding results which include secure and fast performance.

Data at Rest Security Model for Cloud Computing

Abstract

From the perspective of data security, which has always been an important aspect of quality of service, Cloud computing focuses a new challenging security threats. Therefore, a data security model must solve the most challenges of cloud computing security. The proposed data security model provides a single default gateway as a platform. It used to secure sensitive user data across multiple public and private cloud applications, including salesforce, Chatter, Gmail, and Amazon Web Services, without influencing functionality or performance. Default gateway platform encrypts sensitive data automatically in a real time before sending to the cloud storage without breaking cloud application. It did not effect on user functionality and visibility. If an unauthorized person gets data from cloud storage, he only sees encrypted data. If authorized person accesses successfully in his cloud, the data is decrypted in real time for your use. The default gateway platform must contain strong and fast encryption algorithm, file integrity, malware detection, firewall, tokenization and more. This thesis interested about authentication, stronger and faster encryption algorithm, and file integrity

Fuzzy Knowledge Base System for Fault Tracing of Marine Diesel Engine

Abstract

Marine diesel engine provides the prime mover for the majority of ship propulsion systems and as such plays a fundamental role in ship operational and economy. Ship owners and operators focuses to the development of improved method of analysis, operation, fault condition diagnosis, performance monitoring, performance optimization, and recently emission analysis and control. Information technology can be used to raise the technological level of diesel engine automation and control to enable a new generation of engines with high level of safety and friendly use for the operators. Fuzzy knowledge base systems are practically suitable for these problems and will inevitably become an essential element in marine technology.

   The main objective of this paper is designing a prototype fuzzy knowledge base system (FKBS) to improve the capabilities of fault tracing for a ship diesel engine. Such system can be used by non-experts to improve their problem solving skills. Also it can be used as a training tool for new staff. For implementing the Knowledge base system, a special software package has been proposed. This software package has been designed for building the prototype knowledge base system shell. The developed system has a friendly user interface and does not require any special programming skills to encourage all operators to use it

Evaluation of Differential Evolution and Particle Swarm Optimization Algorithms at Training of Neural Network for Stock Prediction

.

Abstract

This paper presents the comparison of two meta-heuristic approaches: Differential Evolution (DE) and Particle Swarm Optimization (PSO) in the training of feed-forward neural network to predict the daily stock prices. Stock market prediction is the act of trying to determine the future value of a company stock or other financial instrument traded on a financial exchange. The successful prediction of a stock's future price could yield significant profit. The feasibility, effectiveness and generic nature of both DE and PSO approaches investigated are exemplarily demonstrated. Comparisons will be performed between the two approaches in terms of the prediction accuracy and convergence characteristics. The proposed model is based on the study of historical data, technical indicators and the application of Neural Networks trained with DE and PSO algorithms. Results presented in this paper show the potential of both algorithms applications for the decision making in the stock markets, but DE gives better accuracy compared with PSO.

Performance of Encryption Techniques for Real Time Video Streaming

Abstract

Recently, multimedia security is becoming more important with the continuous increase of digital communications on the internet. Moreover, special and reliable security is needed in many digital applications (such as video conferencing and medical imaging systems). The classical techniques for data security are not appropriate for the current multimedia usage. As a result, we need to develop new security protocols or adapt the available security protocols to be applicable for securing the multimedia applications. In this paper, three different symmetric encryption techniques are studied namely; AES, RC4 and XOR. . The performance of these algorithms was evaluated for three data types (text, audio and video). Simulations were performed to indicate the performance of the selected encryption algorithms for the different data type given. The results showed the effectiveness of the AES encryption technique in such application.