Editorial

Peter Stavroulakis

Department of Electronics and Computer Engineering,
Technical University of Crete,
73100 Chania, Crete, Greece
E-mail pete_tsi@yahoo.gr

Biographical notes: Peter Stavroulakis received his BS and PhD from New York University in 1969 and 1973 respectively and his MS degree from California Institute of Technology in 1970. After a successful career in the USA working at Bell Labs, Oakland University, Rochester, Michigan and ATT/NYNEX, he joined the Technical University of Crete as a Professor in 1990 where he founded the Telecommunications Institute of Crete. He is the author/editor of 15 books, 100 research papers and has been on the Editorial Board of six international journals. His work influenced and changed international standards in satellite communications. He has presented a number of tutorials and organised more than ten international conferences.

This special issue is composed of eight-papers contributed by authors who responded to a special call for this issue. All these papers have been blind-reviewed by at least two-reviewers. They cover interesting topics in the general area of the multimedia intelligence security such as, a fingerprint images encryption process based on a chaotic true random bits generator, improved reversible steganography schemes based on dual cover images, transcoding resistant robust watermarking techniques using entropy-based selective spread spectrum, fast subscriber identification based on the zero-knowledge principle for the multimedia content distribution, estimation of the strength of DDoS attack using various regression models, adaptive background subtraction using fuzzy logic, a highly metamorphic virus generator and future security challenges in cloud computing.

In the first paper, 'Fingerprint images encryption process based on a chaotic true random bits generator', a fingerprint image encryption scheme, based on a chaotic true random bit generator (TRBG), is proposed. The chaotic generator is based on a non-linear electronic circuit, which produces double scroll chaotic attractors. The initial conditions and the values of the circuit parameters serve as the private key of the cryptographic scheme. Two-chaotic generators with different initial conditions are used, which produce the bits sequences that XOR-ed for generating the final bits sequence. A well-known statistical suite for testing the distribution of the bits sequence was adopted. This sequence has been used to encrypt and decrypt the fingerprint images. Also, the security analysis of the encrypted image demonstrates the high security of the proposed encryption scheme.

The second paper, 'An improved reversible steganography schemes based on dual cover images', investigates the problem of secure confidential message communication over the internet. A common solution to this problem is the usage of steganography which hides secret messages in cover images and only the intended recipient receives the contents of the image. An improved reversible data hiding scheme for grey-scale images using dual steganography images is presented. This scheme provides high security as the secret image cannot be extracted without the knowledge of two-steganoimages. Experimental results demonstrate that the scheme provides a higher embedding capacity without making noticeable distortion in the steganoimage.

In the third paper, 'Transcoding resistant robust watermarking technique using entropy-based selective spread spectrum', the need for efficient copyright protection mechanisms over internet transmission of multimedia information is investigated. Traditional encryption and access control techniques ensure protection of the content till it gets decrypted, but does not protect against unauthorised distribution of content after the content has been decrypted. Therefore, digital watermarking that embeds copyright information written in the content in an imperceptible manner and hence, deters unauthorised distribution has become a very active area of research. The future internet will have various heterogeneous devices like laptop, mobile and IPTV which require the data to be transcoded and delivered according to the capabilities of the end user devices. But the process of transcoding affects the embedded watermark and making it difficult to prove the ownership rights. The current scenario is to embed the watermark in the content after it has been transcoded for each end user device. This increases the overhead and is also a redundant process. This paper investigates the effects of transcoding on watermark and recommends a robust watermarking algorithm such that watermark can be embedded in the original content once and can be retrieved even after the content is transcoded for different end user devices.

The fourth paper 'Fast subscriber identification based on the zero knowledge principle for the multimedia content distribution' proposes an innovative method for the reduction of zero-knowledge subscriber identification schemes that is suitable for multimedia content distribution applications. The fundamental principle underlying the proposed method is the concept of using one-way Boolean functions as transformations for the zero-knowledge identification. This enables the increase of the speed of completion of the identification process by two to three-orders of magnitude, compared to the corresponding speed when using modular arithmetic with large numbers. A method for the establishment of one-way Boolean functions for zero-knowledge identification has been developed. Two-examples for the application of the proposed method are presented.

In the fifth paper, 'Estimating strength of DDoS attack using various regression models', the evaluation results of a proposed approach that utilises the extend of deviation from a detection threshold to estimate strength of DDoS attack is presented using various regression models. Various statistical performance measures, such as coefficient of determination (R2) coefficient of correlation (CR), sum of square error (SSE), mean square error (MSE), root MSE (RMSE), normalised MSE (NMSE), Nash-sutcliffe efficiency index and mean absolute error (MAE) are used to measure the performance of various regression models. Internet type topologies used for simulation are generated using Transit-Stub model of GT-ITM topology generator. NS-2 network simulator on Linux platform is used as simulation test bed for launching DDoS attacks with varied attack strength. A comparative study is performed using different regression models for estimating strength of a DDoS attack. The simulation results are promising since it is shown that the strength of DDoS attack can be estimated efficiently with very little error rate using various regression models.

The sixth paper, 'Adaptive background subtraction using fuzzy logic', studies the extraction of moving objects from an image sequence as a fundamental problem in dynamic image analysis. A novel fuzzy approach is used for background subtraction with a particular interest in the problem of silhouette detection. Experimental results demonstrated that a fuzzy system is much more efficient, robust and accurate than classical approaches. Features are extracted from image regions, the feature information over time is accumulated, high-level knowledge with low-level features is fused in order to build a time-varying background model. A problem with the system is that by adapting the background model, objects moved are difficult to handle. In order to reinsert them into the background, the risk of cutting part of the object is taken but the test results show the feasibility of the proposed algorithm.

In the seventh paper, ‘A highly metamorphic virus generator’, it is shown how metamorphic viruses modify their code to produce viral copies that are syntactically different from their parents. The viral copies have the same functionality as the parent but typically have no common signature. This makes signature-based virus scanners ineffective for detecting metamorphic viruses. A machine learning tool such as hidden Markov models (HMMs) have been proven effective at detecting metamorphic viruses. Previous research has shown that most metamorphic generators do not produce a significant degree of metamorphism. In this paper, a metamorphic engine is developed that yields highly diverse morphed copies of a base virus. It is shown that such metamorphic engine easily defeats commercial virus scanners and in turn is shown that, perhaps surprisingly, HMM-based detection is effective against highly metamorphic viruses. It is concluded with a discussion of possible improvements to the virus generator that might enable it to defeat statistical-based detection methods, such as those that rely on HMMs.

The eighth paper, ‘Future security challenges in cloud computing’ represents cloud computing as one of the most significant shifts in information technology. In cloud computing physical computer models (storage, processing power and services, including software platforms and applications) are abstracted in the way it enables the users to work and access their information and different computer services through multiple devices and networks. Cloud computing, therefore, is about virtualisation where pervasive users will be able to create, modify and distribute new machines very easily. Unfortunately, it can also undermine many assumptions that today’s relatively static security architectures rely on the number of hosts in a system, their mobility, connectivity, patch cycle, etc. Security challenges are one of the concerns about cloud computing, which is delaying its adoption. These challenges include lacking control over data, compliance risks, malicious insiders, access and identity management, secure virtualisation and many others. This paper gives an overview about cloud computing, describes general and security challenges and identifies future security research directions.