Editorial:
Special Issue on Multimedia Information System Security

1 Introduction

With the rapid progress in information technology and an enormous amount of media (e.g. text, audio, speech, music, image and video) appearing over networks, guaranteeing multimedia information system security is becoming increasing important. Several pivotal challenges include copyright protection, integrity verification, authentication, access control, privacy protection, etc. As a consequence, the subject of multimedia information system security has attracted intensive research activities in academy, industry and also government.

With the recent advances in network and multimedia technology, the applications in commercial scenario become increasing crucial. There is an increasing trend in multimedia systems including multimedia distributed computing, multimedia databases, multimedia communications, etc. For example, in multimedia distributed computing, the multimedia content is delivered from the central service provider to the individuals using various techniques/applications such as video-on-demand, IPTV and P2P content distribution. In these applications, piracy is becoming a critical issue. Solutions are needed to protect the copyright of multimedia content. During the past decades, various techniques have been reported for secure multimedia information system such as key management, multimedia encryption, authentication, digital watermarking, digital fingerprinting, secure data mining, access control and digital rights management. These techniques are able to protect multimedia content's confidentiality, integrity, ownership, traitor traceability. In addition, in different networks such as Internet, 3G wireless, DVB-H and P2P, different secure protocols and algorithms are required to provide the system's security. All these topics are in active development.

This special issue of the Informatica Journal invited authors to submit their original work that communicates current research on multimedia information system security regarding both the novel solutions and future trends in the field. In this special issue, we have 7 papers, which can demonstrate advanced works in the field including covert communication in multimedia carriers, secret information analysis from multimedia content, copyright protection, multimedia content encryption, secure mobile multimedia communication, and secure multimedia content indexing or retrieval.

2 The papers in this special issue

In the first paper, entitled "Recent advances in multimedia information system security" we survey techniques and tools used for multimedia information system security. In addition, we present the latest research progress in the field as well as hot research topics such as Trusted Computing, security in network, and security of content sharing in social networks, privacy-preserving data processing, multimedia forensics, intelligent surveillance and steganography.

Steganography is a hot topic belonging to covert communication techniques, which hides secret information into multimedia content and thus sends it to receivers. Only the receiver partnered with the sender can extract the secret information from multimedia carrier. The third party can only detect whether the multimedia content is suspicious and then decide whether to remove it. Steganography faces two threats, i.e., steganalysis and unstable transmission. The former one denotes the technique to detect the presence of secret information based on statistical abnormality caused by information hiding. The latter one means the unstable transmission that causes transmission errors or losses to multimedia content. Although some steganalysis techniques have been proposed, their detection performances are still not satisfied. One important reason is that the methods can only detect certain statistical abnormality, such as the changes in histogram or pixel correlation.

In the second paper, S. Geetha, Siva S. Sivatha Sindhu and N. Kamaraj propose a method to distinguish the plain media and stego media by detecting content independent statistical features. In particular, they designed a feature classification technique, which is composed of two steps: training step and detection step. In the training step, the feature classifier is trained by the database composed of both plain images and stego images (generated by using different information hiding methods). Then, in the detection step, the given image is decided by the classifier automatically. Compared with existing schemes, their scheme does not depend on the steganographic methods.

For steganography, it is a challenge to resist the unstable transmission. Since the transmission errors or losses often make the secret information unrecoverable.

In the third paper, X. Zhang, S. Wang and W. Zhang present a new steganography method that aims to resist the active warden or poor channel conditions. In their method, the secret information is decomposed into a number of shares, and then embedded into different cover images respectively. The embedding efficiency and imperceptibility are improved by the proposed share embedding method. Thus, even a part of stego images are lost during transmission, most of the shares can still be extracted from the remaining stego images, and the shares can be used to recover the secret information. The experiments and analysis show the scheme's practicability.

Digital watermarking is regarded as a potential solution for copyright protection, which embeds such copyright information as content producer, content owner or content receiver into multimedia content. Visible watermarking denotes the watermarking technique that

embeds copyright information imperceptibly. Since it does not affect the commercial value of multimedia content, visible watermarking is preferred. However, watermark detection is still a challenging topic when the original multimedia content is not accessible and the marked content is degraded.

The fourth paper by H. Malik proposes a blind watermark detection method for spread spectrum watermarking. This method regards the problem of watermark detection as a blind source separation problem, and thus uses independent component analysis to estimate the embedded watermark. Since in spread spectrum watermarking, the embedded watermark and the multimedia content are mutually independent and obey non-Gaussian distribution, the proposed detection method outperforms existing correlation-based blind detection methods. The experiments on audio clips are given to show the proposed method's good detection performances.

Multimedia encryption has being emphasized with the popular applications of multimedia content in human being's daily life. Due to such properties as large volumes and real time interaction, selective encryption is preferred for multimedia encryption, which encrypts only some significant parameters in the compressed multimedia stream while leaves other parameters unchanged. Additionally, some synchronization information, e.g., syntax information in the compressed stream, is not encrypted in order to keep the stream's error resistance. Generally, the multimedia content encrypted by selective encryption is still playable. Thus, the intelligibility of the played content is in close relation with the encryption method's security. Till now, few works have been done to assess the quality of the encrypted multimedia content.

In the fifth paper, Y. Yao, Z. Xu and S. Liu propose an assessment method based on neighborhood similarity. Firstly, the neighborhood similarity is defined and cipher images' features are analyzed. Then, the objective visual security metric is defined based on the neighborhood similarity. In experiments, the cipher videos encrypted by different algorithms are assessed with the objective metric. The experimental results show that the objective metric is consistent with the human perception, and can be used to assess the encryption method's visual security automatically.

Digital rights management (DRM) becomes more and more important for protecting the usage of multimedia content. Generally, for a multimedia service system, certain business model is firstly defined, then, the protection means are proposed to support the model. Till now, some practical DRM systems have been reported for securing applications in Internet, wireless mobile network or broadcasting network. However, more and more new applications arise with the development of network technology and multimedia technology, and the corresponding DRM solutions are expected.

In the sixth paper, M. Furini proposes a secure solution for the pervasive video lectures. In this solution, the video chapters are partitioned into two parts, i.e., the pre-defined lesson and the other lesson. The videos in the former one are in clear, while the videos in the latter one are encrypted and the corresponding encryption key is hidden in the videos in the former one. Thus, only the mobile player being able to extract the encryption key correctly can play the videos in the second part successfully. The prototype implementation shows the scheme's feasibility.

In decentralized and distributed system as peer-to-peer multimedia sharing, there are some security issues. Among them, secure multimedia indexing and retrieval is a challenge. In the last paper, W. Allasia, F. Gallo, M. Milanesio and R. Schifanella propose a decentralized, distributed and secure communication infrastructure for indexing and retrieval of multimedia contents with associated digital rights. Firstly, the existing works about Distributed Hash Table (DHT) is introduced, and some security threats are pointed out. Then, the secure DHT layer is presented, and the secure protocols are proposed. Additionally, the feasibility of proposed architecture is shown with a prototype implementation. This scheme is based on structured P2P networks and allows complex queries using standard MPEG-7 and MPEG-21 multimedia metadata. This scheme is expected to attract more researchers in this field.

The list of the papers follows:

- S. Lian, D. Kanellopoulos and G. Ruffo. Recent advances in multimedia information system security.
- S. Geetha, Siva S. Sivatha Sindhu and N. Kamaraj. Detection of stego anomalies in images exploiting the content independent statistical footprints of the steganograms.
- X. Zhang, S. Wang and W. Zhang. Steganography combining data decomposition mechanism and stego-coding method.
- H. Malik. Blind watermark estimation attack for spread spectrum watermarking.
- Y. Yao, Z. Xu and J. Sun. Visual security assessment for cipher-images based on neighborhood similarity.
- M. Furini. Secure, portable, and customizable video lectures for e-learning on the move.
- W. Allasia, F. Gallo, M. Milanesio and R. Schifanella. Indexing and retrieval of multimedia metadata on a secure DHT.

Acknowledgments

The guest editors wish to thank Prof. Anton P. Zeleznikar (Editor-in-Chief of the Informatica Journal) and Prof. Matjaz Gams (Managing Editor) for providing the opportunity to edit this special issue on Multimedia Information System Security. We would also like to thank the authors for submitting their works as well as the referees who have critically evaluated the papers within the short stipulated time. Finally, we hope the reader will share our joy and find this special issue very useful.

S. Lian, D. Kanellopoulos and G. Ruffo
Guest Editors