Multimedia Systems (2014) 20:101–103
DOI 10.1007/s00530-013-0339-8

EDITORIAL

Advances in digital media security and right management

Wojciech Mazurczyk · Krzysztof Szczypiorski

Published online: 6 September 2013

Abstract Digital media security and right management is an emerging research area that has attracted the attention of many security computer professionals, law enforcement experts and practitioners. It is a multidisciplinary research area that includes multiple fields, i.e., law, computer science, networking, data mining and criminal justice. We believe that the papers enclosed in this Special Issue will contribute to the development of the digital media security field and will further stimulate research in this area.

1 Introductory remarks

In the recent years, rapid development in digital technologies has been augmented by the progress in the field of multimedia standards and the mushrooming of digital media applications and services penetrating and changing the way people interact, communicate, work, entertain and relax. Multimedia services and digital content are becoming more significant, popular and they enrich humans' everyday life. Currently, the term multimedia information refers not only to text, image, video or audio content but also graphics, Flash, web, 3D data, etc. Multimedia information may be generated, processed, transmitted, retrieved, consumed or shared in various environments. The lower cost of reproduction, storage and distribution, however, also invites much motivation for large-scale commercial infringement.

The abovementioned issues have generated new challenges related to the protection of multimedia services, applications and digital content. Providing security for digital content is significantly different from providing typical computer information security since multimedia content usually involves large volumes of data and requires interactive operations and real-time responses. In addition, ensuring digital multimedia security must also signify safeguarding of the multimedia services. Different services require different methods for content distribution, payment, interaction, etc. Moreover, these services are also expected to be "smart" in the environment of converged networks, which means that they must adapt to different network conditions and types as multimedia information can be utilized in various networked environments, e.g., in fixed, wireless, mobile networks, etc. All of these make providing security for multimedia even harder to perform.

Digital media security and right management is an emerging research area, and it has attracted a lot of attention of computer security professionals, law enforcement experts and practitioners. It is a multidisciplinary area that includes multiple fields, i.e., law, computer science, networking, data mining and criminal justice. Despite this increased interest, this field still faces diverse challenges and issues, most commonly related to efficiency of the digital evidence processing and the resulting forensic procedures.

In this special issue, we are delighted to present a selection of eleven papers which, in our opinion, will contribute to the enhancement of knowledge in digital media security and right management. The collection of high-quality research papers provides a view on the latest research advances on secure multimedia transmission and distribution but also on multimedia content protection. Security of various digital media is covered starting from

W. Mazurczyk (✉) · K. Szczypiorski
Warsaw University of Technology, Warsaw, Poland
e-mail: wmazurczyk@tele.pw.edu.pl

K. Szczypiorski
e-mail: ksz@tele.pw.edu.pl

well-established security of digital images to more recently popular digital audio/speech and video contents protection.

In the first paper [1], Megías and Domingo-Ferrer introduce an interesting concept of a recombination fingerprinting mechanism for P2P content distribution. Its main innovation is that it allows redistributor tracing, while offering collusion resistance against dishonest buyers trying to create a forged copy without any of their fingerprints.

The authors of the paper [2], Thanh and Iwakiri, describe a novel digital right management (DRM) method which consists of an incomplete cryptography using invariant Huffman code length feature and user identification mechanism to control the quality of the digital content. They have also proposed a new watermarking technique in which the size of the digital content is not changed during the whole process and the disclosing of the original content problem is solved by using the encoder/decoder in the incomplete cryptography.

In [3] Tian et al. contribute by improving the security of quantization index modulation (QIM) steganography in low bit-rate speech streams. It is achieved by exploiting the characteristic of codebook division diversity in the complementary neighbour vertices algorithm to design a key-based codebook division strategy which follows Kerckhoff's principle. To resist the state-of-the-art steganalysis, authors introduce random position selection to dynamically adjust the embedding rate and matrix encoding strategy to enhance the embedding efficiency. The experimental results provided show that the proposed approach outperforms previous schemes in terms of steganographic transparency and steganalysis resistance.

In the next paper, Fallahpour and Megías [4] propose a novel audio watermarking algorithm in the logarithm domain based on the absolute threshold of hearing of the human auditory system. It utilizes the fact that the human ear requires more precise samples at low amplitudes (soft sounds)—this helps to design a logarithmic quantization algorithm. Adjusting the quantization level results in a very high-capacity, imperceptible distortion and robustness. The introduced scheme provides also three parameters (frequency band, scale factor and frame size) which can further facilitate the regulation of the watermarking properties.

The authors of the paper [5] present an efficient block-based encryption scheme for encrypting H.264/SVC (Scalable Video Coding) enhancement layers by taking advantage of the inter-layer prediction technique used in H.264/SVC. These properties make the proposed scheme highly suitable for perceptual/transparent encryption of H.264/SVC bitstreams in such applications like pay TV broadcasting.

In the sixth paper [6], Chen et al. also focus on H.264 by proposing a novel method for open-loop, robust watermarking of H.264/AVC bitstreams. In contrast to previous watermarking techniques that embed the information after the reconstruction loop and perform drift-compensation, authors propose a new approach by utilizing intra-drift-free watermarking algorithm. The resulting watermark is extremely runtime-efficiently embedded in the compressed domain after the reconstruction loop. Such approach also preserves average bit-rate, which leads to an increase in bit-rate of the watermarked video. The watermark remains detectable in the re-compressed videos, even in very low quality and highly distorted video sequences.

Song et al. [7] introduce a novel digital video watermarking algorithm based on intra prediction modes of Audio Video coding Standard (AVS). In the proposed scheme, watermark bits are embedded in intra prediction modes by modifying them based on the mapping between those modes and the watermark bits. Because the proposed algorithm keeps the features of encoded video stream and maintains the video quality both objectively and subjectively, it is highly transparent. In addition, watermark extraction is simple and fast and it requires neither original media nor a complete video decoding.

In the next paper, Bhatnagar and Wu [8] present a simple but efficient chaotic encryption framework for enhancing the security of biometric images during transmission. The proposed framework is based on the fractional wavelet packet transform (FrWPT), chaotic map and Hessenberg decomposition. To enhance the security, the transform orders of FrWPT are chaotically obtained and it results in a desired randomness of the process. The proposed framework is validated by a detailed discussion of the key sensitivity, space analysis, and edge distortion, randomness, statistical and numerical analyses. They confirm the high security of the proposed framework.

The authors of the paper [9] describe a data hiding method for digital images that is based on the combination of a secret sharing technique and a novel steganography method using integer wavelet transform. It consists of three phases: a cryptography phase using a secret sharing method, data hiding phase using a novel integer wavelet-based steganography method, and a data extraction phase. The provided experimental results prove that, considering all aspects, including the visual image quality and undetectability, the proposed method facilitates a very effective system and performs well under almost all of popular attack cases and scenarios when compared to the state-of-the-art techniques.

In [10] Liu et al. introduce an adaptive steganography algorithm based on block complexity and matrix embedding for digital images. The embedding strategy sets are defined for seven kinds of image blocks with different complexity. The corresponding embedding strategies are determined by resolving the embedding risk minimization problem. The adaption guarantees that the message bits are mainly embedded into the regions with higher complexity values. Experimental results prove that the proposed approach provides moderate capacity with lower distortion and has a higher resistance ability than state-of-the-art steganographic algorithms.

Finally, the last paper [11] focuses on categorization and evaluation of the robustness of wavelet-based image watermarking techniques against JPEG2000 compression. Authors propose a new modular framework for this purpose that incorporates algorithmic choices, wavelet kernel, subband or watermark selection. As most of the algorithms utilize a different set of parametric combinations, this analysis is particularly helpful to describe the various parameters' influence on the robustness on common platform. Such a framework can be especially useful while designing new algorithms of this type.

We believe that the papers presented in this Special Issue will stimulate further research in the important areas of information and network security.

Acknowledgments This work was partially supported by the Polish Ministry of Science and Higher Education and Polish National Science Centre under grants: 0349/IP2/2011/71 and 2011/01/D/ST7/05054.

References

1. Megías, D., Domingo-Ferrer, J.: Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints. Multimedia Syst. J. (2013, this issue)
2. Thanh, T.M., Iwakiri, M.: A proposal of digital rights management based on incomplete cryptography using invariant huffman code length feature. Multimedia Syst. J. (2013, this issue)
3. Tian, H., Liu, J., Li, S.: Improving security of quantization-index-modulation steganography in low bit-rate speech streams. Multimedia Syst. J. (2013, this issue)
4. Fallahpour, M., Megías, D.: Secure logarithmic audio watermarking scheme based on the human auditory system. Multimedia Syst. J. (2013, this issue)
5. Deng, R.H., Ding, X., Wu, Y., Wei, Z.: Efficient block-based transparent encryption for H.264/SVC bitstreams. Multimedia Syst. J. (2013, this issue)
6. Chen, W., Shahid, Z., Stutz, T., Autrusseau F., Le Callet, P.: Robust drift-free bitrate preserving H.264 watermarking. Multimedia Syst. J. (2013, this issue)
7. Song, X., Lian, S., Hu, W., Hu, Y.: Digital video watermarking based on intra prediction modes for Audio Video Coding Standard. Multimedia Syst. J. (2013, this issue)
8. Bhatnagar, G., Wu, Q.M.J.: Enhancing the transmission security of biometric images using chaotic encryption. Multimedia Syst. J. (2013, this issue)
9. Khosravi, M. J., Naghsh-Nilchi, A.R.: A Novel joint secret image sharing and robust steganography method using wavelet. Multimedia Syst. J. (2013, this issue)
10. Liu, G., Liu, W., Dai, Y., Lian, S.: Adaptive steganography based on block complexity and matrix embedding. Multimedia Syst. J. (2013, this issue)
11. Bhowmik, D., Abhayaratne, C.: On robustness against JPEG2000: a performance evaluation of wavelet-based watermarking techniques. Multimedia Syst. J. (2013, this issue)