Multimed Tools Appl (2011) 52:257–261
DOI 10.1007/s11042-011-0741-1

GUEST EDITORIAL

Research advances in data hiding for multimedia security

Muhammad Khurram Khan

Published online: 28 January 2011

The digital information revolution has brought profound changes in our daily lives and the advantages of digital information have also generated new challenges and opportunities for their protection. Due to the tremendous advances in signal processing and transmission techniques, it is easy to acquire, tamper and duplicate multimedia data. The wide spread use of internet in business, research and security has necessitated to protect the data and preserve the identity of its true owner.

For the last two decades, digital data hiding has received a great deal of attention from the scientific community. Remarkable research efforts have been invested in recent years, trying to export novel and applied real world engineering applications. Data hiding embeds information into digital media for the purpose of identification, authentication, and copyright protection. Data hiding represents a class of processes used to embed data, such as copyright information, into various forms of media e.g. video, image, audio, and text with a minimum amount of perceivable degradation to the "host" signal; i.e., the hidden data should be invisible and inaudible to an observer.

This special issue is intended to bring together diversity of international researchers, experts and practitioners who are currently working in the area of digital data hiding and its applications. This special issue is a collection of original papers that cover a wide range of topics from design, implementation, security, and application of data hiding systems for multimedia security. As a whole, this special issue contains a diverse collection of high-quality papers authored by eminent researchers in the field. There were total 49 submissions from several countries around the world and through a rigorous peer-review process, only 20 submissions got final acceptance for the publication.

The first paper by Liu et al. presents an adaptive DE-based reversible steganographic scheme with bilinear interpolation and simplified location map. Authors apply kernel of bilinear interpolation to effectively improve the number of the embeddable location. Also, it is used for the existing adaptive embedding rule to improve the embedding payload control

M. K. Khan (✉)
Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia, Riyadh, Saudi Arabia
e-mail: mkhurram@ksu.edu.sa
URL: http://faculty.ksu.edu.sa/khurram

capability in single layer embedding. Their proposed scheme presents better visual quality of the stego-image and carries larger embedding payload than some other DE schemes published in the current literature.

The second paper by Zhao et al. confirms the truth that the current reversible data hiding algorithms are detectable. Authors show that the horizontal difference histogram of natural image is significantly altered after being embedded secret message. Furthermore, the difference between the horizontal and the vertical difference histogram of natural image is much less than that of the watermarked image. Experimental analysis demonstrates that the approach of Zhao et al. is effective and more efficient than the already published schemes.

The third paper by Yan et al. presents a MPEG-1 Layer III (MP3) audio CODEC based steganographic method to embed secret message during encoding. Their method is designed under the restrictions of the MP3 compression standard without any modifications or additions to the existing standard. The authors experimentally show that their method can provide much higher capacity than other approaches, while satisfying the low distortion and security requirements for steganography on MP3 audios.

The fourth paper by He et al. proposes a neighborhood characteristic based detection model for statistical fragile watermarking to lift the constraints of the tampered area from 4% to 14% of the host image. He et al. demonstrate experimentally and analytically that the neighborhood characteristic based detection model effectively reduces the total number of false decisions and detects the tampered pixels with high probability.

The next paper by Tan et al. proposes a lexicographical-structured framework to generate image hashes. Their system consists of two parts: dictionary construction and maintenance, and hash generation. The authors implement a hashing scheme using discrete cosine transform (DCT) and non-negative matrix factorization (NMF). They also show that their scheme is resistant to normal content-preserving manipulations, and has a very low collision probability.

The sixth paper by Min-Jen Tsai presents application of chaotic systems to strengthen the security of wavelet tree quantization (WTQ) technique for digital watermarking, especially against cryptanalysis attack. This enhancement in robustness of WTQ is achieved by dividing the digital image into various blocks and that are scrambled using chaotic system technique and then WTQ is implemented. According to the results, this enhancement is not only for WTQ but also for other advanced wavelet tree based algorithms like wavelet tree group modulation (WTGM) and dynamic energy enabled differentiation (called DEED) watermarking techniques.

The seventh paper by Vivekananda et al. proposes a new audio watermarking algorithm based on singular value decomposition and dither-modulation quantization. The watermarks produced by this algorithm are highly imperceptible that can be blindly extracted and have low error probability rates. The results show its robustness against attacks like additive white Gaussian noise, MP3 compression, resampling, etc.

The eighth paper by Min-Jen Tsai presents a new non-blind watermarking algorithm based on the wavelet tree classification and human visual system (HVS)—dynamic energy enabled differentiation (DEED). The algorithm works by dividing the wavelet coefficients of the image into disjoint trees and embeds one watermark bit into one wavelet tree along with contrast sensitive function (CSF) of human visual system. Author further proposes that this may be enhanced to truly blind watermarking technique by introducing a random direction differentiator that he calls DEEDR. The results show that DEED not only has low complexity but it performs better than other tree energy differentiation based techniques like WTGM and WTQ in terms of robustness and imperceptibility of watermarking.

The ninth paper by Luo et al. proposes a secure steganography technique based on a content adaptive scheme where a cover image is divided into small squares, which are

rotated by a random multiple of 90 degree to produce a new image that is divided into non-overlapping embedding units with three consecutive pixels. The data is embedded in the middle pixel based on the difference among the three pixels such that their sort order is not changed so as to preserve the local statistical features. Experimental results show that their scheme performs better than the existing Pixel-value differencing (PVD) based methods.

In the tenth paper, Liu et al. propose a low complexity coding scheme named Minority codes for improving watermarking embedding efficiency for large payloads. By exploiting the property that the positions of the minority bit in two complementing sequences are the same, where the minority bit is the bit with least number of occurrences in an odd number long binary sequence, Minority codes are generated. Using the codebook based on minority codes composed of a pair of complementing sequences combined with the watermarking algorithm such codewords are identified that causes fewer embedding changes according to the host image and the watermarking method, thus providing a better efficiency for large payloads.

The next paper by Xu et al. describes a copy image detection technique that can resist various kinds of image attacks. In the first phase, large sized circular patches are constructed by using Scale Invariant Feature Transform (SIFT) detector and then a Multi-resolution Histogram Descriptor (MHD) is deployed to produce the discriminative attributes. The proposed scheme is compared to global and local feature extraction techniques. An experimental evaluation from benchmark attacks has been performed and the better performance of the proposed technique to the existing methodologies is reported.

In the twelfth paper, Zeng et al. propose a lossless drift compensation scheme to restrain the distortion issues in reversible video data hiding. In their work, the drift compensation signals are merged in the quantized DCT (Discrete Cosine Transform) coefficients of P-frames and the corresponding recovery mechanism is presented. The scheme solves the spreading and accumulation problem of traditional reversible schemes. Experimental results show that their proposed method improves the video quality and the original data can be recovered by removing the hidden data.

In the next paper, Fallahpour and Megias present an audio watermarking algorithm by incorporating the high frequency band of the wavelet decomposition. In their work, the high frequency band is divided into frames to alter the wavelet samples. The results of their study show that their technique has a very high capacity and is robust against common audio signal processing methods.

The fourteenth paper by Lien and Lin proposes a reversible data hiding method for ordered dithered halftone images. In this method, the data hiding is obtained by sub image-swapping operation and by decomposing ordered dithered halftone into a maximal number of sub images. The major advantage of this scheme is that it preserves good visual quality and offers a high capacity. The authors also propose a reversible authentication watermarking system based on reversible watermarking method. Their work shows better visual quality compared to an existing method.

The next paper by Fallahpour et al. proposes a data hiding method within the image prediction errors by using the median edge detector (MED), gradient adjacent prediction (GAP) and Jiang prediction algorithms. The histogram of the prediction errors of images is computed and higher frequencies values are shifted to attain require capacity for data hiding. The experimental results show better performance of the image prediction error histogram over the conventional image histogram. The authors also develop an adaptive method for hiding data where subjective quality is traded for data hiding capacity by choosing the sum of frequencies of positive and negative error values on the histogram.

The sixteenth paper by Su et al. combines the methodologies of selective encryption and fingerprinting for effective DRM of H.264/AVC streaming videos. A selective encryption

scheme is first presented and then a fingerprinting scheme is introduced to provide further protection. The feasibility of the solution is also studied through the experimental results.

In the seventeenth paper, Ling et al. attempt to propose a fine-search scheme to further refine the results from a rough query set. A local affine-invariant descriptor based on polar-mapping and discrete Fourier transform is used as the first step. Second and final step is to propose a spatial dependent matching method. Robustness, distinction and suitability parameters are used as performance metrics in the paper by Ling et al.

In the next paper, Natthawut et al. design a scheme to covertly send secret message to multiple receivers via a stream of running short text messages. Thai language is used as case study but it can be applied to many other languages. Authenticity and privacy against active attacks is also discussed in the paper.

The second last paper of this special issue is contributed by Hsieh et al., in which they develop a solution to identify the source and to detect the image tampering. They present an image authentication scheme that can verify the origin of the received image and detect if the image has been tampered with. Their experimental results prove that using different strength values increases the robustness of the watermark with little sacrifice in image quality.

The last paper by Bhatnagar and Raman segments host image into non-overlapping blocks by the means of Hilbert space filling curve. As a result, a reference image is formed by considering Human visual system. An extraction scheme by keeping reliability in focus is also proposed in the paper. Their analysis demonstrates better visual imperceptibility and resiliency against intentional or un-intentional variety of attacks.

Acknowledgements I would like to express my heartfelt thanks to all the people who have contributed their time and efforts in making this special issue a success. I thank all the authors who contributed their papers for this special issue. I am also full of gratitude to the reviewers who scrutinized the submitted manuscripts and recommended modifications and revisions in enhancing the quality of the accepted papers. Last, but certainly not the least, I would like to pay my special thanks to the Editor-in-Chief, Prof. Borko Furht, for his encouragement and strong support during the preparation of this special issue.

Dr. Muhammad Khurram Khan is currently working as associate professor and R&D Manager at Center of Excellence in Information Assurance (CoEIA), King Saud University, Kingdom of Saudi Arabia.

He is the Founding Editor of 'Bahria University Journal of Information & Communication Technology (BUJICT)'. He is on the editorial board of several international journals e.g. Journal of Network & Computer

Applications (Elsevier), Journal of Security of Communication Networks (Wiley), Computers & Electrical Engineering (Elsevier), Journal of Information Hiding and Multimedia Signal Processing (JIHMSP), International Journal of Biometrics (Inderscience), Journal of Physical & Information Sciences, and Journal of Independent Studies and Research-Computing (JISR). He has also played role of guest editor of several international journals of Springer-Verlag and Elsevier Science, etc. He is an active reviewer of many international journals. In addition, he is on the organizing and technical committees of dozens of international conferences.

Dr. Khurram is an honorary Professor at IIIRC, Shenzhen Graduate School, China. He has been included in the Marquis Who's Who in the World 2010 edition. He was recently awarded a certificate of appreciation for outstanding contributions in Biometrics & Information Security Research, AIT Conference, June 2010 at Japan. He has also secured an outstanding leadership award at IEEE international conference on Networks and Systems Security 2009, Australia. He has published more than 90 research papers in the journals and conferences of international repute and has two US patents pending. His areas of interest are biometrics, multimedia security, digital data hiding, and authentication protocols.

The research interests, academic and professional activities of Dr. Khurram can be found in detail at http://faculty.ksu.edu.sa/khurram