Editorial

Amit Kumar Singh*, Pardeep Kumar and Satya Prakash Ghrera

Department of CSE and IT,
Jaypee University of Information Technology,
Waknaghat, Solan 173234, Himachal Pradesh, India
Email: amit_245singh@yahoo.com
Email: pardeepkumarkhokhar@gmail.com
Email: sp.ghrera@juit.ac.in
*Corresponding author

Basant Kumar

Department of Electronics Engineering,
MNIT Allahabad,
211004, Uttar Pradesh, India
Email: singhbasant@yahoo.com

Sanjay Kumar Singh

Department of Computer Science and Engineering,
IIT (BHU),
Varanasi 221005, Uttar Pradesh, India
Email: sks.cse@iitbhu.ac.in

Biographical notes: Amit Kumar Singh is currently working as an Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering at the Jaypee University of Information Technology (JUIT) Waknaghat, Solan, Himachal Pradesh-India since April 2008. He has completed his PhD degree from the Department of Computer Engineering, NIT Kurukshetra, Haryana in 2015. Recently, he appointed as an Associate Editor of IEEE Access and Multimedia Tools and Applications (MTAP), Springer. He has presented and published over 50 research papers in reputed journals and various national and international conferences. His research interests include multimedia security, data hiding, biometrics and cryptography.

Pardeep Kumar is currently working as an Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering at the Jaypee University of Information Technology (JUIT), Wakanaghat and he has ten years of extensive experience in academics. Prior to joining Jaypee Group, he has associated with Mody University of Technology and Science (formerly known as Mody Institute of Technology and Science) Laxmangarh, Sikar, Rajasthan. He has completed his PhD (Computer Science and Engineering, Noveber 2012) from the Uttarakhand Technical University, Dehradun. He is also serving as a professional member of ACM (Association for Computing Machinery), life member of IAENG (International Association of Engineers)

and IAENG Society of Computer Science and Society of Data Mining. He has published around 22 papers in peer reviewed journals and conferences of national and international repute.

Satya Prakash Ghrera completed 34 years of service in Corps of Electronics and Mechanical Engineers of the Indian Army, he joined Jaypee Institute of Engineering and Technology in January 2006, as an Associate Professor in the Department of Computer Science and Engineering. With effect from September 2006, he has taken over responsibilities of HOD (Computer Science Engg. and IT) at the Jaypee University of Information Technology Waknaghat, Distt. Solan HP. His research interests include information security and cryptography.

Basant Kumar is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad. He has more than 13 years of teaching and research experience. He obtained his BTech degree in Electronics and Instrumentation Engineering from the Bundelkhand Institute of Engineering and Technology, Jhansi, Uttar Pradesh, and ME degree in Communication Engineering from the Birla Institute of Technology and Science, Pilani, in 1999 and 2002, respectively. He received his PhD in Electronics Engineering from the Indian Institute of Technology, Banaras Hindu University, Varanasi, India (IIT-BHU) in 2011. His areas of research include telemedicine, data compression, data hiding, multimedia communication and medical image processing. He has published more than 30 research papers in reputed international journals/conferences.

Sanjay Kumar Singh is currently working as an Associated Professor at the Department of Computer Science and Engineering, IIT BHU, Varanasi. He has completed his BTech in Computer Engg., MTech in Computer Applications and PhD in Computer Science and Engineering. He is a Certified Novell Engineer (CNE) from the Novell Netware, USA and a Certified Novell Administrator (CNA) from the Novell Netware, USA. He is a member of LIMSTE, IEE, International Association of Engineers and ISCE. His research areas include biometrics, computer vision, image processing, video processing, pattern recognition and artificial intelligence. He has over 50 national and international journal publications, book chapters and conference papers. He is also a guest editorial board member of *Multimedia Application and Tools*, Springer, and the *EURASIP Journal of Image and Vision Processing* (Springer). He is a member of the Computer Society and the Association for Computing Machinery.

1 Introduction

In the digital information age, multimedia content such as text, image, audio, video and 3D computer graphics models can be easily copied, manipulated and distributed over the open channel. This makes copyright protection, ownership identification, content authentication, and identity theft challenging issues to the content owner and distributors. Recently, data hiding techniques have developed very fast and have applied to many applications, such as e-government, military, communication, medical/healthcare, privacy protection, identification, media file archiving, broadcast monitoring, remote education and insurance companies, secure e-voting systems, digital cinema, fingerprinting and so on. Digital watermarking is a data hiding technique for inserting multimedia information, also known as a watermark, into multimedia data, which can be later extracted or detected for a variety of purposes including identification and authentication. In addition to providing security, this technique can also be used to recognise the source, owner, distributor or creator of the data.

The objective of this special issue is to call for all future research aspects and directions, state-of-the-art approaches and methodologies, and most recent developments related to this specific area. This special issue has attracted 27 manuscripts and the submissions have been strictly reviewed by least three reviewers consisting of guest editors and external reviewers, with 11 high-quality articles accepted in the end.

2 Summary of the accepted papers

Below, we briefly summarise the highlights of each paper.

In 'WeChat traffic classification using machine learning algorithms and comparative analysis of datasets', Shafiq et al. extract 44 features from captured WeChat traffic in two different network environments. The method execute training testing method using six well-known machine learning (ML) classifiers to classify WeChat instant messaging, picture messaging, audio and video calling traffic. Further, the performance of the method is determined in term of training time, accuracy, recall and precision. Furthermore, compare the results of full instance of dataset and reduce instances of dataset to find out the effectiveness of both datasets as well as compare the ML classifiers result to show which classifiers gives high performance result.

In 'Node authentication algorithm for securing static wireless sensor networks from node clone attack', Mohindru and Singh propose an energy efficient algorithm for node authentication. Authors aim of the node authentication algorithm is to authenticate the sensor nodes before message communication within wireless sensor networks (WSN) so that cloned nodes are identified in the initial step of the communication. The proposed algorithm uses encryption decryption operations and also XOR, extraction, bitwise shift operations. Performance of the algorithm is analysed in terms of communication, storage, and computation overheads metrics and compare with other similar authentication algorithms.

In 'The research of reputation incentive mechanism of P2P network file sharing system', Li and Su establish the reputation incentive mechanism in P2P network file sharing system. The simulation result indicates that the mechanism can provide a good business environment for resource sharing and promotes a stable and reliable development of the whole file sharing system.

In 'Robust injection point-based framework for modern applications against XSS vulnerabilities in online social networks', Gupta and Gupta present XSS-Explorer, a server-side framework, which scrutinises the web applications for discovering XSS vulnerabilities in multimedia applications in an automated manner. The evaluation outcome reveals the efficiency of utilising XSS-Explorer in recognition of real as well as previously unknown vulnerabilities by examining all possible injection points of the web page. Verification injection method deployed in the framework compact the volume of checks on all possible injection points. Moreover, utilisation of field qualifiers improved the guarantee of the submission of multifaceted web forms. Further, method is evaluated the server-side framework on a suite of three real world tested web applications and noticed that the proposed XSS-Explorer is considered to be a worthy substitute to support the experts of cyber security in the competition against XSS vulnerabilities. The transformation from context-insensitive sanitisation to context-familiar sanitisation leads to an escalation in the performance of the web servers and precision rate of our proposed XSS defensive technique. The inclusion of new XSS attack vector repositories (apart from the conventional XSS cheat sheet) increases the robustness of the work and observed an acceptable rate of false positives and negatives, unlike in the existing work.

In ‘A nonlinear two dimensional logistic-tent map for secure image communication’, Rajendran and Doraipandian present innovative chaotic map for image cryptosystem by combining tent map and 2D logistic map in different form. The proposed 2D logistic-tent map (2DLT) generates two chaotic series. These chaotic series are used to perform the confusion and diffusion phases of image cryptosystem. A comparison between existing standard 2D logistic map and proposed 2D logistic-tent map shows that the proposed map has high random chaotic series than the existing one. In order to evaluate the strength of the proposed image cryptosystem, the developed chaos cryptosystem was subjected to different analysis such as differential, key size and sensitivity, chosen plain text and cipher text attack analyses. All the analysed results proved that the proposed cipher has good security level and can be used for different secure image communication applications.

In ‘A robust reversible image watermarking scheme in DCT domain using Arnold scrambling and histogram modification’, Roy and Pal develop a discrete cosine transform (DCT) and histogram shifting based robust reversible image watermarking scheme using Arnold scrambling. Initially, the image is decomposed into non-overlapping blocks and consequently DCT are applied to each block to embed a binary bit of watermark into each transformed block by modifying one pair of middle significant AC coefficients. In this initial step, location map is also generated for the cover image restoration purpose in the extracting side. Further, this location map is embedded in the cover image using histogram modification technique. In the receiver side, at first location map is generated from an image using histogram modification method and watermark is recovered from the corresponding image. Using location map reversible image is reversed in the following extracting phase of the proposed method. The proposed reversible watermarking scheme has also been experimented to verify the robustness property against several image processing attacks and satisfactory results are achieved.

In ‘Improved pixel relevance based on Mahalanobis distance for image segmentation’, Song and Zhang present an algorithm based on the novel pixel relevance, where non-local information can be incorporated into fuzzy clustering for image segmentation. The algorithm can improve the robustness of corresponding algorithms greatly. Experiments on different noisy images show that the proposed algorithm can retrieve better results than conventional algorithms.

In ‘3D reconstruction of human face from an input image under random lighting condition’, Sun et al. present an improved method to reconstruct the 3D shape of human face from a single captured image under random lighting condition. Based on an average face model, the lighting parameter of the input image is estimated firstly. Further, based on the original training database, a new training database has been built by relighting the surface normals of the training human faces. Furthermore, a coupled statistical model has been used based on the new training database to reconstruct the 3D face for a single input image under random lighting condition. The experiment results show the effectiveness of the proposed method.

In 'Reversible data hiding in absolute moment block truncation coding compressed images using adaptive multilevel histogram shifting technique', Amita et al. present a reversible histogram shifting method is used in the absolute moment block truncation coding (AMBTC)-compressed images with the addition of an adaptive block division scheme. The proposed method achieves high performance in terms of embedding capacity as well as PSNR value while maintaining the normalised correlation of the cover image after extraction. Further, the method offer good robustness for signal processing attacks.

In 'A new statistical attack resilient steganography scheme for hiding messages in audio files', Kar et al. present a novel technique for audio steganography that preserves first-order statistical properties of the cover audio after embedding a secret message in it to avoid detection by automated tools. Particularly, the technique preserves the frequency distribution of audio samples in the resultant audio in relation to the cover audio, i.e., the histogram of the resultant audio obtained after embedding a secret message is the same as the one of the original cover audio. As a result, the technique further avoids detection by any histogram based or similar statistical attacks. Particularly, the technique allows away to maintain a desired level of signal-to-noise ratio in the resultant stego audio while embedding a secret message. The technique applies a method of partitioning the audio samples in the cover audio, which is followed by a technique of rearranging or reordering of the audio samples in each partition through an encoding process for embedding the secret message bits in it. Partitioning of samples in the audio is governed by a specified error limit on each individual sample. Results show how this error limit can be determined from a signal-to-noise ratio that should be maintained in the stego audio to avoid detection.

In 'Physiological trait based biometrical authentication of human-face using LGXP and ANN techniques', Raja et al. develop a method is to handle the variability in human-face appearances due to changes in the viewing direction. Poses, illumination conditions, and expressions are considered as three main parameters, which are processed for the overall authentication process. For the overall processing, extensive feature set like texture, contrast, correlation and shape are extracted by employing modified region growing algorithm and texture feature by local Gabor XOR pattern (LGXP) and artificial neural network (ANN) technique. The present work has been analysed using the data of different subjects with varying ages.

3 Conclusions

Contributions of these 11 selected articles basically reflect the new achievements in the field of for multimedia watermarking and network security and we hope they can provide a solid foundation for future new approaches and applications. Finally, we would like to thank all authors for their contributions and the reviewers for reviewing these high quality papers for his support and guidance throughout the process.

Acknowledgements

We would like to express our gratitude to all the authors who have submitted their work for publication in this special issue. Finally, we would like to thank all authors for their contributions, the reviewers for reviewing these high quality papers, Honorary Editor-in-Chief Prof. Eldon Y. Li, Editor-in-Chief Prof. Xin (Robert) Luo and all the Editorial Staff of the *International Journal of Information and Computer Security* for his support and guidance throughout the process.