Editorial

Amit Kumar Singh*

Department of Computer Science and Engineering,
National Institute of Technology Patna,
Bihar, 800005, India
Email: amit_245singh@yahoo.com
*Corresponding author

Haoxiang Wang

GoPerception Laboratory,
Ithaca, NY 14850, USA
Email: hw496@goperception.com

Mohamed Elhoseny

Faculty of Computers and Information,
Mansoura University,
Mansoura, Dakahlia, 35516, Egypt
Email: mohamed_elhoseny@mans.edu.eg

S. Ramakrishnan

Department of Information Technology,
Dr. Mahalingam College of Engineering and Technology,
Pollachi, 642003, India
Email: ram_f77@yahoo.com

Biographical notes: Amit Kumar Singh is currently an Assistant Professor from the Computer Science and Engineering Department, National Institute of Technology at Patna (an Institute of National Importance), Patna, India. He has authored over 56 research papers in various reputed international journals, five books, 29 conference papers, five book chapters and edited various international journal special issues as a guest editor with international faculty members. His research interests include multimedia data hiding, biometrics and cryptograpy.

Haoxiang (Harry) Wang is currently the Director and lead executive faculty member of GoPerception Laboratory, NY, USA and has been the Research Associate at the Cornell University since 2014. His research interests include multimedia information processing, pattern recognition and machine learning, remote sensing image processing and data-driven business intelligence. He has co-authored over 30 journal and conference papers.

Mohamed Elhoseny is currently an Assistant Professor from the Faculty of Computers and Information, Mansoura University, Egypt, where he is also the Director of the Distributed Sensing and Intelligent Systems Lab. He has authored or co-authored over 100 ISI journal articles, conference proceedings, book chapters, and several books published by Springer and Taylor & Francis. His research interests include network security, cryptography, machine learning techniques, and intelligent systems. He serves as the Editor-in-Chief of the *International Journal of Smart Sensor Technologies and Applications*, and as an Associate Editor of several journals such as *IEEE Access*.

S. Ramakrishnan is a Professor and Head of the Department of Information Technology, Dr. Mahalingam College of Engineering and Technology, Pollachi, India. He is an Associate Editor for *IEEE Access* and reviewer of 24 international journals including *IEEE Transactions*, IET, Elsevier and Springer journals. He is a guest editor of special issues in three international journals including *Telecommunication Systems Journal* of Springer. He has published 160 papers and nine books. He has guided three PhD scholars and guiding seven scholars. His areas of research include digital image processing, soft computing, cryptography, wireless sensor network and cognitive radio.

1 Introduction

Recently, social networks are used by most of people for exchanging/sharing the personal information in the form of multimedia over unsecured channel in day-to-day life. The information and communication technology (ICT) has proved an indispensible and cost effective technique for dissemination of the multimedia documents. However, prevention of copyright violation, authenticity, confidentiality and ownership identity theft are the potential issues due to attempts of malicious attacks/hacking of transmitted information on the networks. It includes criminal offences ranging from ownership identity theft to copyright violation and personal information exposures to medical history disclosure are being made every day. To tackle these drawbacks, nowadays, potential researchers are developing advanced techniques to analyse, prevent and detect the potential issues.

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 54 manuscripts and the submissions have been strictly reviewed by three reviewers consisting of guest editors and external reviewers, with 12 high-quality articles accepted in the end.

2 Summary of the accepted papers

Below, we briefly summarise the highlights of each paper.

In 'A secured modular exponentiation for RSA and CRT-RSA with dual blinding to resist power analysis attacks', Mahanta and Khan developed a secured approach for modular exponentiation in RSA and CRT-RSA cryptosystems with dual blinding. Further, method have injected two ineffectual instructions between the fundamental operations and blinded the intermediate results to felicitate hiding and resist simple power analysis. The implementation results shows that with a nominal penalty, RSA and

CRT-RSA with dual blinding can effectively resist some popular simple power analysis and differential power analysis attacks to a significant extent.

In ‘Eight neighbour bits swap encryption-based image steganography using arithmetic progression technique’, Mukherjee and Sanyal described a steganographic approach of concealing the secret data so as to facilitate secure communication. Eight neighbour bits swap (ENBS) encryption has been used on the chosen cover image in the first stage. This results in the scrambling of the data bits, thereby disrupting the normal pixel orientation. Finally, data bits from the secret image are embedded within the scrambled cover using the technique of arithmetic progression. Several quantitative and qualitative benchmarks analysis pertaining to this approach is made. Experimental results have shown that the imperceptibility is well maintained at high payload with negligible distortion produced in the image.

In ‘Nested context-aware sanitisation and feature injection in clustered templates of JavaScript worms on the cloud-based OSN’, Gupta et al. proposed an enhanced JavaScript feature-injection-based framework that obstructs the execution of cross-site scripting (XSS) worms from the virtual machines of cloud-based online social network (OSN). It calculates the features of clustered-sanitised compressed templates of JavaScript attack vectors embedded in the HTTP response messages and inject them on the OSN server in the form of comment statements in such code. It further re-executes the feature calculation procedure of JavaScript code on the generation of HTTP response in online phase. The experimental evaluation of the framework was performed on the platform of OSN-based web applications deployed in the cloud platform. The performance analysis done (using F-score and F-test) revealed that the framework detects the injection of malicious JavaScript code with low false negative rate and acceptable performance overhead. The novelty of the method lies in the fact that it optimises the JavaScript feature calculation procedure by executing it on clustered templates of JavaScript attack payloads, unless its execution on redundant injected JavaScript code adopted by the existing state-of-art.

In ‘Fault prediction for distributed computing Hadoop clusters using real-time higher order differential inputs to SVM: Zedacross’, Pinto et al. suggested a model that uses the resource usage statistics of a normally functioning Hadoop cluster to create a machine learning model that can then be used to predict and detect faults in real time. Further, the paper explains the novel idea of using higher order differentials as inputs to support vector machine (SVM) for highly accurate fault predictions. The results obtained after running the system on various test cases demonstrate that the proposed method is accurate and effective.

In ‘A coupled map lattice-based image encryption approach using DNA and bi-objective genetic algorithm’, Suri and Vijay proposed coupled map lattice (CML) and deoxyribonucleic acid (DNA)-based image encryption algorithm that uses genetic algorithm (GA) to get the optimised results. The algorithm uses the chaotic method CML and DNA to create an initial population of DNA masks in its first stage. The GA is applied in the second stage to obtain the best mask for encrypting the given plain image. In addition, the results have shown that bi-objective optimisation of the proposed algorithm given balanced results with respect to the selected fitness functions.

In ‘Securing wireless sensor networks from node clone attack: a lightweight message authentication algorithm’, Mohindru et al. proposed a lightweight message authentication algorithm for securing message communication in WSNs. The algorithm uses Mod and XOR operations to compute fixed size hash value or message digest. The scheme is robust as a slight change in the message will affect the hash value extensively. The comparative analysis of the proposed algorithm is done with authentication algorithms available in the literature with the help of various metrics.

In ‘Blind noise estimation-based CT image denoising in tetrolet domain’, Diwakar and Kumar proposed a method where, the noise of CT images is estimated using patch-based gradient approximation. Further, estimated noise is used to denoise the CT images in tetrolet domain. The PSNR and visual quality of experimental results indicate that the proposed scheme gives excellent outcomes in compare to existing schemes.

In ‘A hybrid generative-discriminative model for abnormal event detection in surveillance video scenes’, Kumar et al. proposed hybrid generative-discriminative framework for detecting and localising the anomalous events of illegal vehicles present in the scene. This paper introduces a novelty in the application of hybrid usage of latent Dirichlet allocation (HLDA) and SVMs over dynamic texture at sub-region level. The proposed HLDA-SVM model is validated on UCSD dataset and is compared with mixture of dynamic texture and motion context technique. Experimental results show that the HLDA-SVM approach performs well in par with current algorithms for anomaly detection.

In ‘Scrutinising internet banking security solutions’, Khan et al. introduced the security mechanisms in online banking and the significance of online as well as the emerging mobile banking has been discussed. Furthermore, the pros and con of solutions based on OTP as well as other non-OTP solutions have been presented. At last, the prominence of open issues in the present subject of study has been elucidated.

In ‘Fake profile detection in multimedia big data on online social networks’, Sahoo and Gupta proposed a machine learning-based approach for detecting suspicious profiles for tapping and tainting multimedia big data on Facebook. The experimental result of the work using content-based and profile-based features delivers first rate performance as compared to other approaches.

In ‘Unconstrained face recognition using deep convolution neural network’, Agrawal and Singh developed a convolution neural network (CNN)-based architecture for face recognition in unconstrained environment. The proposed architecture is based on a standard architecture of ResNet50. The recognition performance has shown that the proposed framework of CNN achieves the state-of-art performance on publically available challenging datasets.

In ‘CSL: FPGA implementation of lightweight block cipher for power-constrained devices’, Lamkuche and Pramod proposed a unique lightweight block cipher. It operates on 64-bit block size and key size varies from 64-bit to 128-bit key for encryption and decryption. The hardware implementation of CSL algorithm was developed using field programmable gate array (FPGA) architecture. A pipelined architecture of compact S-boxes was implemented on Digilent Nexys 4 DDR Artix-7 FPGA Xilinx.

3 Conclusions

Contributions of these 12 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 their support and guidance throughout the process.