Editorial: Information Security Solutions for Telemedicine Applications

Amit Kumar Singh, Zhihan Lv, Seungmin Rho, Sanjay Kumar Singh, Xiaojun Chang, William Puech

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of current version December 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2885256

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: INFORMATION SECURITY SOLUTIONS FOR TELEMEDICINE APPLICATIONS

Implementing telemedicine solutions has recently become a trend among various research teams at an international level. Telemedicine refers to the use of modern information and communication technologies to meet the needs of citizens, patients, healthcare professionals, and healthcare providers, as well as policy makers. Telemedicine applications are very promising and have great potential; they can play a very important role in service provision by improving access, equity and quality through connecting healthcare facilities and healthcare professionals, and diminishing geographical and physical barriers. However, the transmission and access technologies of medical information raise critical issues that urgently need to be addressed, especially those related to security. Further, medical identity theft is a growing and dangerous crime. Stolen personal information can have a negative financial impact, but stolen medical information cuts to the very core of personal privacy. Medical identity theft already costs billions of dollars each year, and altered medical information can put a person's health at risk through misdiagnosis, delayed treatment or incorrect prescriptions. Yet, the use of hand devices to store, access, and transmit medical information is outpacing the privacy and security protection on those devices. Therefore, the authenticity of the information and related medical images is of prime concern as they form the basis of inference for diagnostic purposes. In such applications, tamper proofing and guaranteed originality of medical data/information is achieved by embedding some kind of watermark(s) which must be secure and robust against malicious attacks. Robustness and security of medical data/information against attacks is an interesting, challenging area for researchers. Potential researchers are using watermarking and cryptography to disseminate security to the medical data. Further, noted researchers are using watermarking techniques in the field of healthcare to address health data management issues, including source and data authentication, efficient image archiving and retrieval, optimizing bandwidth required to transmit the data, and highlighting diagnostically significant regions.

The objective of this Special Section in IEEE ACCESS is to present a snapshot of the state-of-the-art security techniques in the field of telemedicine.

Our Call for Papers received an enthusiastic response with 49 high-quality submissions. Per IEEE policy, it was ensured that handling editors did not have any potential conflict of interest with authors of submitted articles. All articles were reviewed by at least two independent potential referees. The articles were evaluated for their rigor and quality, and also for their relevance to the theme of our Special Section. After a rigorous review process, we accepted 15 articles to form the Special Section. The brief summary about each paper is presented as follows.

1) The invited article "SBPG: secure better portable graphics for trustworthy media communications in the IoT," by Saraju P. Mohanty *et al.*, first introduced some major challenges faced in the Internet of Things (IoT) infrastructure, specifically secure communication and user authentication in the context of automated analysis of biomedical images and communication of the analysis results and related metadata in a smart healthcare framework. Further, authors proposed hardware architecture for a secure digital camera integrated with the secure better portable graphics (SBPG) compression algorithm, which is very useful for image communications in IoT. The performance of proposed BPG method with respect to compression quality and size of the compressed file is found superior than traditional JPEG method.
2) In the article "Nucleosome positioning with fractal entropy increment of diversity in telemedicine", by Mengye Lu *et al.* proposed a fractal entropy increment of diversity-based nucleosome positioning technique. Core DNA of human, worm, fly and yeast were recognized by their sequences. The authors evaluate the model's quality, and different nucleosome positioning methods were compared with the same existingbenchmark datasets. Extensive experimental results showed that the provided model was an effective nucleosome positioning method. Further, the authors analyzed the importance of all factors which were thought to play roles in nucleosome structure.
3) The article "Prediction of lung motion from four-dimensional computer tomography (4DCT) images

using bayesian registration and trajectory modelling,'' by Min Li *et al.*,presented an approach for modeling lung motion based on Bayesian registration and trajectory simulations. In the registration process, the neighborhood information is combined with a similarity metric such that an initial displacement field is generated, which is smoothed and refined via the displacement regularization. The dense displacement fields are then used to describe the lung motion. The experimental results indicated that any point in the lungs at any given time is accurately predicted, which provides another method of determining the lung and tumor motions for radiation therapy. In addition, the experiments provided promising results compared to some similar state-of-the-art image registration methods.

4) In the article ''A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application,'' Qikun Zhang *et al.* proposed a dynamic and cross-domain authenticated asymmetric group key agreement for telemedicine. The method using the group keys also has been implemented efficiently in cryptographic systems to provide confidential and privacy. It supports that the members leave one group or join another group frequently. Extensive analysis of the method makes it suitable for security group communication in telemedicine applications.
5) In the article ''Hybrid predictor based four-phase adaptive reversible watermarking,'' Muhammad Ishtiaq *et al.* presented a prediction error expansion based reversible watermarking technique. The method uses four phases for embedding a watermark to provide authentication of both an image and source of origin. Further, the authors have compared the performance of the proposed method with three interesting state-of-the-art techniques and found very promising results.
6) The article ''Secure and robust digital image watermarking using coefficient differencing and chaotic encryption,'' authored by Nazir A. Loan *et al.* proposed a DCT based watermarking scheme, which is secure and blind in nature. The method uses Arnold transform and chaotic encryption to add dual level security to the watermark. The proposed embedding technique is based on the difference between the coefficients of adjacent blocks. The performance of various variants of the method was tested for many attacks. Further, the comparison results depict that the proposed scheme outperforms many state-of-the-art schemes. Authors believe that the proposed method will be beneficial for secure telemedicine.
7) The article ''A short linearly homomorphic proxy signature scheme,'' authored by Qun Lin *et al.*, introduced a concept and security model of linearly homomorphic proxy signature (LHPS) method, and designed a novel LHPS method from bilinear pairings. Further, the authors prove that the method is secure under consideration. Due to the short length of signature, the method is suitable for any low-bandwidth communication environments.
8) In the article ''Eye recognition with mixed convolutional and residual network (MiCoRe-Net)'', Zi Wang *et al.* proposed a deep learning based Eye Recognition system to improve the accuracy of other similar deep learning based methods. The method uses deep learning architecture called mixed convolutional and residual network (MiCoRe-Net), which inserts a plain convolutional layer between every two residual layers. The MiCoRe-Net takes advantage of fast learning from convolutional neural network, and nonsaturation features from residual network. The performance of the proposed method is tested for different datasets and results show the superiority in accuracy to previously published research.
9) The article ''Whole brain fMRI pattern analysis based on tensor neural network,'' authored by Xiaowen Xu *et al.*, proposed a framework to more efficiently and accurately extract features and improve the performance of functional magnetic resonance imaging (fMRI) classification. The method uses tensor neural network (TensorNet) to extract the essential and discriminative features from the whole-brain fMRI data. Authors confirmed that the proposed method performed better than SVM classifier based similar method for multi-class fMRI data.
10) The article ''Secure medical data transmission model for IoT-based healthcare systems,'' authored by Mohamed Elhoseny *et al.*, proposed a method to provide secure transmission of patient data through the combination of watermarking and cryptography in an IoT environment. The method uses hybrid encryption (AES and RSA) to encrypt the secret information and then hides the results in the cover gray/color images through DWT. The authors presented a detailed evaluation and demonstrated superior performance of the proposed method.
11) The article ''Efficient quantum information hiding for remote medical image sharing,'' authored by Ahmed A. Abd El-Latif *et al.* proposed two quantum information hiding approaches based on least and most significant qubits for healthcare applications. The first method uses controlled-NOT gate to encrypt quantum images and hide encrypted results into quantum cover image. However, the second method uses Arnold's cat map to scramble the secret quantum watermark image. The authors hide the scrambled result into the quantum cover image. The authors presented a detailed evaluation and demonstrated the method has excellent visual quality and high embedding capacity.
12) The article ''Secure delegation-based authentication for telecare medicine information systems,'' authored by Zuowen Tan, proposed a secure delegation-based authentication protocol for wireless roaming service using identity based-cryptography. Experimental

security analysis under Random Oracle model and Burrows-Abadi-Needham (BAN) logic shows that the proposed technique provides communication confidentiality at low computational cost. .

13) The article "Anonymous data sharing scheme in public cloud and its application in e-Health record," authored by Huaqun Wang, developed a data sharing scheme for the security of the outsourced cloud information. The method uses symmetric encryption, searchable encryption and attribute-based encryption techniques to provide confidentiality in public clouds. The security and efficiency analysis demonstrate that the designed scheme is feasible and efficient. The author further discussed the suitability of the scheme for secure e-health records.
14) In the article "A practical public key encryption scheme based on learning parity with noise," Zhimin Yu *et al.* proposed a single-bit public key encryption method based on a variant of learning parity with noise (LPN) and extended it to a multi-bit public key encryption technique. Experimental demonstration efficiently proved the correctness and chosen plaintext attack security of the proposed method. Further, the method solved encoding error rate issues of the previous LPN based public key technique, while the encoding error rate in the proposed is negligible.
15) Finally, the article entitled "Privacy-preserving protocol for sink node location in telemedicine networks," authored by Ting Li *et al.*, presented a privacy-preserving protocol for sink node location for telemedicine networks. The method uses fake sink nodes and data packets to make it difficult to determine the location of the real sink node at low delivery time. The extensive experimental results show the significant improvement in safe time of the sink node and reduction in the data delivery time.

To conclude, we would like to sincerely thank all the authors for submitting their high quality articles to this Special Section, and the large number of reviewers who have participated in the review process, and provided helpful comments and suggestions to the authors to improve their article. We especially thank the IEEE ACCESS Editor-in-Chief, Professor Michael Pecht, and other staff members of IEEE ACCESS for their continuous support and great guidance. We believe that our Special Section will be helpful to the senior undergraduate and graduate students, researchers, industry professionals, healthcare professionals and providers working in the area of telemedicine as well as other emerging applications demanding state-of-the-art information security solutions.

AMIT KUMAR SINGH, *Guest Editor*
Department of Computer Science and Engineering
National Institute of Technology at Patna
Patna 800005, India
E-mail: amit_245singh@yahoo.com

ZHIHAN LV, *Guest Editor*
School of Data Science and Software Engineering
Qingdao University
Qingdao 266071, China
E-mail: lvzhihan@gmail.com

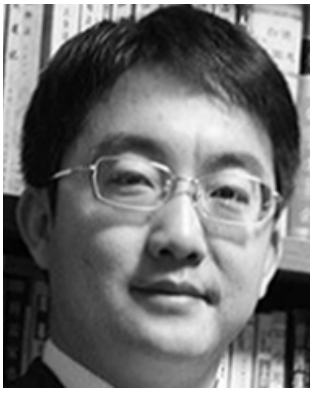
SEUNGMIN RHO, *Guest Editor*
Department of Media Software
Sungkyul University
Anyang 14097, South Korea
E-mail: smrho@sungkyul.edu

SANJAY KUMAR SINGH, *Guest Editor*
Department of Computer Science and Engineering
Indian Institute of Technology (BHU)
Varanasi 221005, India
E-mail: sks.cse@iitbhu.ac.in

XIAOJUN CHANG, *Guest Editor*
Faculty of Information Technology
Monash University
Melbourne, VIC 3800, Australia
E-mail: cxj273@gmail.com

WILLIAM PUECH, *Guest Editor*
ICAR Team
Laboratory of Computer Science, Robotics, and Microelectronics
University of Montpellier
34095 Montpellier, France
E-mail: william.puech@lirmm.fr

AMIT KUMAR SINGH received the bachelor's degree in computer science and engineering from the Institute of Engineering, Veer Bahadur Singh Purvanchal University, Jaunpur, India, in 2005, the M.Tech. degree in computer science and engineering from the Jaypee University of Information Technology, Waknaghat, India, in 2010, and the Ph.D. degree in computer engineering from the National Institute of Technology, Kurukshetra, India, in 2015. He was with the Computer Science and Engineering Department, Jaypee University of Information Technology, from 2008 to 2018. He is currently an Assistant Professor with the Computer Science and Engineering Department, National Institute of Technology at Patna (An Institute of National Importance), Patna, India. He has authored over 70 peer-reviewed journal, conference publications, and book chapters. He has authored two books entitled *Medical Image Watermarking: Techniques and Applications*, in 2017, and *Animal Biometrics: Techniques and Applications*, in 2018 (Springer International Publishing). He has also edited the book *Security in Smart Cities: Models, Applications, and Challenges* (Springer International Publishing, 2019), the Proceedings of 4th IEEE International Conference on Parallel, Distributed and Grid Computing in 2016 and the Proceedings of 4th International Conference on Image Information Processing in 2017. He currently serves on the Editorial Board of two peer-reviewed international journals, including the IEEE ACCESS and *Multimedia Tools and Applications* (Springer). His research interests include data hiding, biometrics, and cryptography.



ZHIHAN LV received the joint Ph.D. degree from Paris Diderot University and the Ocean University of China, in 2012. He was a Research Associate at University College London. He has also been an Assistant Professor with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, since 2012. He was with CNRS, France, as a Research Engineer, with Umeå University/KTH Royal Institute of Technology, Sweden, as a Post-Doctoral Research Fellow, and with Fundación FIVAN, Spain, as an experienced Researcher. He is currently an Associate Professor with Qingdao University, China. He was a Marie Curie Fellow at the European Union's Seventh Framework Programme LANPERCEPT. He has completed several projects successfully on PC, website, smartphone, and smart glasses. His research mainly focuses on multimedia, augmented reality, virtual reality, computer vision, 3-D visualization and graphics, serious game, HCI, bigdata, and GIS. His research application fields widely range from everyday life to traditional research fields (i.e., geography, biology, and medicine). He is a Programme Committee Member of ACM IUI 2015, ACM IUI 2016, the IEEE BIGDATA4HEALTH Workshop 2016, the IEEE/CIC WIN Workshop 2016, IIKI2016, and WASA2016. He received the memberships from several international academic organizations, such as ACM, the IEEE, and Eurographics. He has been an Associate Editor of *PLOS One* (since 2016), the IEEE ACCESS (since 2016), *Neurocomputing* (since 2016), and *IET Image Processing* (since 2017). He is also the Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Multimedia Tools and Applications*, *Neurocomputing*, and the *Journal of Intelligent and Fuzzy Systems*.

SEUNGMIN RHO received the M.S. and Ph.D. degrees in computer science from Ajou University, South Korea, in 2003 and 2008, respectively. He visited Multimedia Systems and Networking Laboratory, The University of Texas at Dallas, from 2003 to 2004. Before he joined the Computer Sciences Department, Ajou University, he spent two years in the industry. From 2008 to 2009, he was a Post-Doctoral Research Fellow with the Computer Music Lab, School of Computer Science, Carnegie Mellon University. He was a Research Professor with the School of Electrical Engineering, Korea University, from 2009 to 2011. In 2012, he was an Assistant Professor with the Division of Information and Communication, Baekseok University. He is currently an Assistant Professor with the Department of Media Software, Sungkyul University. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management, and computational intelligence. He has published about 100 papers in refereed journals and conference proceedings in these areas. He has received a few awards including Who's Who in America, Who's Who in Science and Engineering, and Who's Who in the World in 2007 and 2008, respectively. He has been involved in over 20 conferences and workshops as various Chairs and over 30 conferences/workshops as a Program Committee Member. He has edited a number of international journal special issues as a Guest Editor, such as *Multimedia Systems*, *Information Fusion*, *Engineering Applications of Artificial Intelligence*, *New Review of Hypermedia and Multimedia*, *Multimedia Tools and Applications*, *Personal and Ubiquitous Computing*, *Telecommunication Systems*, *Ad Hoc & Sensor Wireless Networks*, and so on.

SANJAY KUMAR SINGH received the B.Tech. degree in computer engineering, the M.Tech. degree in computer applications, and the Ph.D. degree in computer science and engineering. He is currently a Professor with the Department of Computer Science and Engineering, IIT BHU, Varanasi. He is also a Certified Novell Engineer and a Certified Novell Administrator with Novell Netware, USA. He has published over 100 national and international journal publications, book chapters, and conference papers. His research areas include biometrics, computer vision, image and video processing, pattern recognition, and artificial intelligence. He is a member of the Computer Society of India and the Association for Computing Machinery. He has served as a guest editor, a TPC member, and a Reviewer for various conferences and reputed journals. He is a Guest Editorial Board Member of *Multimedia Application and Tools* (Springer), the *International Journal of Information and Computer Security* (Inderscience), and the *EURASIP Journal of Image and Vision Processing* (Springer).

XIAOJUN CHANG received the Ph.D. degree in computer science from the Centre for Quantum Computation and Intelligent Systems, University of Technology Sydney, Australia, in 2016. He held a post-doctoral position at the Language Technology Institute, Carnegie Mellon University. He is currently an Assistant Professor with Monash University, Australia. His main research interests include machine learning, data mining, and computer vision. He is especially interested in the topic of video analysis. Eight of his papers have been recognized as the 2018 Thomson Reuters Highly Cited Paper. He has served as an Area Chair for ICPR 2017 and as a PC member for top-tier conferences.

WILLIAM PUECH received the Diploma degree in electrical engineering from the University of Montpellier, France, in 1991, and the Ph.D. degree in signal-image-speech from the Polytechnic National Institute of Grenoble, France, in 1997, with research activities in image processing and computer vision. He served as a Visiting Research Associate with the University of Thessaloniki, Greece. From 1997 to 2008, he was an Associate Professor with the University of Montpellier, where he has been a Full Professor in image processing, since 2009. He is currently the Head of the ICAR Team (Image & Interaction), LIRMM. He has published over 40 journal papers and 120 conference papers and is an Associate Editor of five journals (JASP, SPIC, SP, JVCIR, and IEEE TDSC) in the areas of image forensics and security. His current interests include image forensics and security for safe transfer, storage and visualization by combining data hiding, compression, and cryptography. Since 2018, he has been a member of the IEEE Information Forensics and Security. Since 2017, he has been a General Chair of the IEEE Signal Processing French Chapter.