With the rapid popularity of social network applications and advanced digital devices, we have witnessed the explosive growth of multimedia big data in terms of both scale and variety over the last few years. A large amount of multimedia data has been produced from different platforms, applications, and environments, including from social networking services, surveillance systems, Internet of Things (IoT) remote sensing, and entertainment applications. Such increases in multimedia big data are influencing communication through seamless network connections, enhanced user experiences, and free information sharing. At the same time, security issues related to such multimedia big data have arisen.

Emerging Cybersecurity Concerns

An urgent demand has emerged for novel technologies that deal with copyright protection, multimedia forgery detection, and cybersecurity—especially for cyber-enabled multimedia applications. This exciting research area has attracted extensive research, which reflects the significant role these topics play in the multimedia community. Recently, numerous promising solutions have been proposed, but it is still challenging for the multimedia community to effectively and efficiently handle these security challenges over large-scale multimedia data, especially when the scale reaches into the tens of millions or even billions.

This special issue brings together research efforts in cybersecurity for cyber-enabled multimedia applications to specifically deal with security challenges in the multimedia big data era. The five articles selected for this special issue cover a broad range of topics related to cybersecurity for cyber-enabled multimedia applications.

In This Issue

Multimedia big data not only evokes various innovative data-driven services and applications but also introduces privacy and security threats. The first article, “A Selective Privacy Preserving Approach for Multimedia Data,” by Huining Li, Kun Wang, Xiulong Liu, Yanfei Sun, and Song Guo, proposes a privacy
protection method in which the encryption complexity is selective according to time limitations and resource constraints. They focus on privacy leakage issues in multimedia systems and investigate how to maximize privacy and upgrade security levels given predefined time and resource constraints. They propose a selective privacy preserving method to adaptively allocate encryption resources according to the privacy weight and execution time of each data package—that is, selecting the encryption method with appropriate complexity and security level for each multimedia data package. Data is randomly divided into two parts and XOR operations are performed with a generated cipher key in different cloud storage servers to prevent users’ original information from being attacked by untrusted cloud operators. Extensive simulation results demonstrate the advantages and superiority of the proposed method over the prior schemes.

Mobile crowdsourcing (MCS) is emerging as an effective paradigm for large-scale cyber-enabled multimedia applications, with researchers exploring various sensing capabilities and multiple radios of mobile devices and how they might be combined with human power and intelligence. However, most MCS schemes use the direct mode (that is, crowdworkers passively or actively select tasks and contribute without interacting and collaborating with each other), which can hamper some time-constrained crowdsourced tasks. The second article “Word of Mouth Mobile Crowdsourcing: Increasing Awareness of Physical, Cyber, and Social Interactions,” is presented by Yufeng Wang, Wei Dai, Bo Zhang, Jianhua Ma, and Athanasios V. Vasilakos. After providing a system-level description of WoM-based mobile crowdsourcing and outlining the main challenges and future research directions in this research area, the authors explore WoM-based MCS, in which crowdsworkers, apart from executing tasks by themselves, actively recruit other appropriate individuals by exploiting their mobile social networks and/or physical encounters in the proximal area to conduct crowdsourced tasks. The authors review technical challenges, such as crowdworker recruitment, incentive design, security and privacy, and data quality control, and they compare available solutions and discuss practical system-level issues.

The next article, “Flow Watermarking for Antinoise and Multistream Tracing in Anonymous Networks,” by Ran Wang, Guangquan Xu, Bin Liu, Yan Cao, and Xiaohong Li, proposes an interval-packet-size-based spread spectrum network flow watermark (IPS3) scheme to solve the problems of noise interference and multistream tracing in anonymous networks, which adopts a new watermarking carrier based on the original direct sequence spread spectrum technology. IPS3 can not only solve the problem of multistream tracing through the operation of direct sequence spread spectrum for original watermarking but also the problem of network flow watermarking technology being subjected to the network stability. It tackles this issue by adjusting the carrier size in the process of watermarking modulation—that is, by taking the average packet size in a time interval as the watermarking carrier. Experiments demonstrate that the proposed IPS3 scheme outperforms the traditional network flow watermarking technology in terms of noise filtering and multistream tracing, and it achieves higher accuracy when it is used in anonymous network tracing.

With the rapid development of urbanization and industrialization in China, more and more children are coming to cities to study and live, and the complicated urban environment brings challenges to keeping children safe. It is important to keep parents and guardians informed of children’s whereabouts and activities through cyber-enabled technology and services. The article, “ChildGuard: A Child-Safety Monitoring System,” by Zhigang Gao, Hongyi Guo, Yunfeng Xie, Yanjun Luo, Huijuan Lu, and Ke Yan proposes a child monitoring system based on mobile devices. The system offers an in-path safety function and a region safety function. The in-path safety function monitors the real-time movement of children walking on a road. The region safety function restricts the activity scope of children by setting safety regions. Children can be reminded and warned about potential risks, and their guardians can check their children’s states (and abnormalities). Experiments show
that ChildGuard has higher positioning accuracy in real time than similar systems.

The last article is “Crowdsensing Multimodal Data: Security and Privacy Issues,” by Yan Li, Young-Sik Jeong, Byeong-Seok Shin, and Jong Hyuk Park. Smartphones are now equipped with various sensors, such as an accelerometer, GPS, and a gravity sensor, and they have high-performance wireless communication capabilities. Using the ubiquitous presence of powerful mobile devices, crowdsensing lets ordinary people collectively gather and share real-time multimedia data. Multimedia crowdsensing has made large-scale participatory sensing viable in a speedy and cost-efficient manner, but it also introduces security and privacy concerns. Personally identifiable information of participants can be exposed in the process of sharing individually owned sensor data. This article specifically identifies security and privacy issues in multimedia crowdsensing and describes existing solutions for protecting both data producers and consumers in the multimedia crowdsensing environment.

Cyberspace has become an integral part of our work and daily life. As cyber-physical systems are further integrated with social systems, cybersecurity will become increasingly important. Looking to the future, we envision the prediction, early detection, and proactive prevention of emerging cybersecurity problems. Such solutions will take human factors into account and will be enhanced by the advancement of data-driven and AI-enabled technologies. 

Acknowledgments
We express our gratitude to all the authors and reviewers for their fantastic effort to ensure the high quality of the articles appearing in this special issue. We thank the IEEE Computer Society Technical Committee on Multimedia Computing (TCMC) and Mei-Ling Shyu, the TC Chair, who first reviewed and recommended the proposal of this special issue. This special issue would not have been possible without the support of Yong Rui, Editor in Chief of IEEE Multimedia; Alan Hanjalic, Associate EIC; and Shani Murray and Andy Morton, who always provided prompt and appropriate help during the review and editing process.

Qun Jin is a professor in the Department of Human Informatics and Cognitive Sciences, Faculty of Human Sciences, at Waseda University, Japan. His research interests include human-centric ubiquitous computing, big data, personal analytics and individual modeling, cybersecurity, and cyber-enabled applications in healthcare. He seeks to exploit the rich interdependence between theory and practice in his work with interdisciplinary and integrated approaches. Jin received his PhD in computer science and electrical engineering from Nihon University, Japan. He is a senior member of IEEE and the Information Processing Society of Japan (IPSJ). Contact him at jin@waseda.jp.

Yong Xiang is a professor and the Director of the Artificial Intelligence and Data Analytics Research Cluster, School of Information Technology, at Deakin University, Australia. His research interests include information security and privacy, multimedia (speech/image/video) processing, wireless sensor networks and IoT, and biomedical signal processing. Xiang received his PhD in electrical and electronic engineering from the University of Melbourne, Australia. He is a senior member of IEEE. Contact him at yxiang@deakin.edu.au.

Guozi Sun is a professor in the School of Computer Science and Technology at Nanjing University of Posts and Telecommunications, China. His research interests include digital forensics, multimedia forensics, social network forensics, and digital investigation. Sun received his PhD in mechanical engineering and automation from Nanjing University of Aeronautics and Astronautics, China. He is a member of the IEEE Computer Society, ACM, China Computer Federation (CCF), Chinese Institute of Electronics (CIE), and Information Security and Forensics Society (ISFS), China. Contact him at sun@njupt.edu.cn.
Yao Liu is an assistant professor in the Department of Computer Science and Engineering at the University of South Florida. Her research is related to computer and network security, with an emphasis on designing and implementing defense approaches that protect emerging wireless technologies from being undermined by adversaries. Her research interest also lies in the security of cyber-physical systems, especially in smart grid security. Liu received her PhD in computer science from North Carolina State University. She is a recipient of the 2016 National Science Foundation CAREER Award. Contact her at yliu@cse.usf.edu.

Chin-Chen Chang is a chair professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taiwan. His research interests include data engineering, database systems, computer cryptography, and information security. Chang received his PhD in computer engineering from National Chiao Tung University, Taiwan. He is an IEEE and Institution of Engineering and Technology (IET) Fellow. Contact him at ccc@cs.ccu.edu.tw.