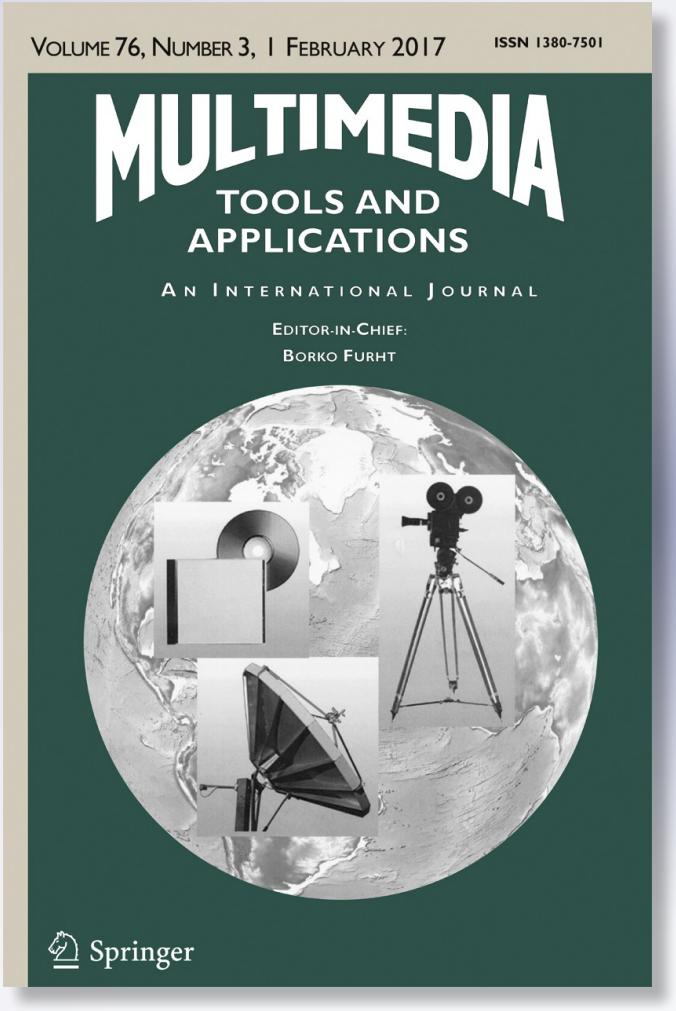
Guest Editorial: Multimedia Social Network Security and Applications

Zhiyong Zhang & Kim-Kwang Raymond Choo

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501
Volume 76
Number 3

Multimed Tools Appl (2017)
76:3163-3168
DOI 10.1007/s11042-016-4081-z



Springer

Multimed Tools Appl (2017) 76:3163–3168
DOI 10.1007/s11042-016-4081-z

GUEST EDITORIAL

Guest Editorial: Multimedia Social Network Security and Applications

Zhiyong Zhang[1,2] · **Kim-Kwang Raymond Choo**[3,4]

Published online: 1 December 2016

In the increasingly inter-connected society, multimedia social networks (MSN) have become a 'mainstream' tool used by online users to connect and share contents with other users 24/7 in real-time. It is, therefore, unsurprising that MSNs have become a salient area of inquiry by computer scientists and computer security researchers. For example, researchers need to design intelligent computing and soft computing technologies to improve multimedia system functions, efficiency and performance, as well as improving user's sharing experiences (e.g. using recommendation systems and more effective algorithms). Ensuring the security of users and data are also an ongoing topic of interest and importance due to the ease in producing and sharing user and multimedia content using MSNs. In recent years, we have seen advances in multimedia system security and soft computing for MSN applications, such as "hard" security mechanisms (e.g. protocols and methodologies) and "soft" computing methods (e.g. machine learning and rough set), as well as research efforts in trust assessment, risk management and social factors to understand the trade-off between the effectiveness and security in MSNs.

This special issue is dedicated to the reporting of state-of-the-art and recent advancements in this emerging area of enquiry. We received 26 submissions for this special issue, of which 12 were accepted for publication (i.e. 46 % acceptance rate). Each paper went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. A summary of the papers is categorized and presented below.

✉ Zhiyong Zhang
xidianzzy@126.com

Kim-Kwang Raymond Choo
raymond.choo@fulbrightmail.org

[1] Information Engineering College, Henan University of Science and Technology, Luoyang, Henan, People's Republic of China

[2] Department of Computer Science, Iowa State University, Ames, IA, USA

[3] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

[4] School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5095, Australia

1 Social networks

Due to the pervasiveness of social networks, the capability to measure and quantify the influence of users (e.g. influential users) has many applications, such as targeted marketing and advertising (e.g. pay influential users to advertise a particular product, in order to maximize exposure). Some studies on social network trust model and credential paths finding algorithms were done [24–26]. In this special issue, Zhuang et al. [27] presented a way of measuring the spread influence of users in microblog. In their approach, the authors considered user interaction features, retweet intervals, location of users in information cascades and other features relevant to the measurements.

While it is important to measure and quantify the influence of users, it is equally important for e-commerce businesses and review website providers to be able to identify and remove deceptive review spam (e.g. written by competing businesses or disgruntled employees). This is the area that Rout et al. [17] seek to contribute to in this special issue. Specifically, the authors demonstrated how the collective use of supervised and unsupervised techniques as well as sentiment analysis can be used to identify such review spam.

Identifying and removing compromised social networking accounts is a key solution to addressing disseminating of review spams and other spams, as well as malicious content. In this special issue, Barbon et al. [6] demonstrated that text mining approach of the posts' content can be used to determine whether an account has been compromised. The approach consisted of extracting the user's writing style, uses the k-Nearest Neighbors algorithm (k-NN) to evaluate the post content and identify the user, and uses a continuous updating of the user baseline to support existing trends and seasonality issues of the user's posts. The findings reported by the authors in this special issue, as well as those of Peng et al. [14]) and Peng et al. [15]) demonstrated the potential to identify users based on the textual contents of their postings on social media.

Niu et al. [13] also noted the inevitable fact that we will have malicious nodes or nodes with malicious intent or behaviour in any (mobile) social networks, where these nodes seek to disrupt the normal functioning of the networks (e.g. discarding and tampering network packets). Therefore, it is important to ensure the resilience of such networks by having a sufficiently robust service recovery mechanism. In this special issue, the authors present a service recovery method based on trust evaluation, which adopts the Dempster-Shafer (D-S) evidence theory.

2 Cryptographic solutions

For decades, Digital rights management has been still a burning issue [22]. The use of encryption is generally recognized as an effective tool in ensuring the confidentiality of data-at-rest and data-in-transit. In this special issue, Peng et al. [15]) present a selective encryption scheme designed to ensure the confidentiality of H.264/AVC video in multimedia social networks.

However, there are limitations in encryption-based solutions. For example when one wishes to share data such as multimedia content with different groups of users whose access rights may dynamically change. Therefore, to provide the scalability and flexibility of real-time multimedia data sharing, the fine-grained access control such as using delegation and secure sharing approaches are required (see [7, 18, 20, 25]).

Wang et al. [19] in this special issue present a social network delegation model, which allows delegators in the MSN to provide their delegation policies. The model, formalized using a behaviour sequence logic language, will attempt to resolve delegation conflicts, if any. The authors then evaluate their approach using a custom-built multimedia social network.

3 Forensics

Digital forensics, including multimedia forensics, is an increasingly important research focus due to the digitalization of our society [1, 9, 16]. This is also evidenced by the work of Yang et al. [21], and Azfar et al. [3] in this special issue.

Yang et al. [21] present an AVI carving technique to recover a fragmented video file using the frame size information in every frame and the index. They demonstrate the utility of their technique using a prototype on 16 camera shot AVI files.

Azfar et al. [3] extend their previous work [2, 4, 5] to 30 popular Android productivity apps. Based on the findings of the forensic examination of these apps, a two-dimensional taxonomy of the forensic artefacts of the productivity apps is presented.

4 Watermarking and data hiding

Unlike some of the topics examined in this issue (e.g. social networks and mobile apps), watermarking and data hiding have been extensively studied but there are still worthwhile contributions to be made in this area [12].

In this special issue, for example, Jeyhoon et al. [10] propose a blind audio watermarking algorithm which can be used to embed data as well as extracting the embedded data by changing the Discrete Cosine Transform (DCT) coefficients. Niu et al. [13] also present an image watermarking scheme designed to be resilient again desynchronization attacks, particularly for colour images. In their approach, the authors extract the steady colour image feature points using a new image feature point detector, based on the colour invariance model and the probability density. Then, the authors build the affine invariant local feature regions using a probability density, prior to using their watermarking algorithm to embed the digital watermark into the affine invariant local feature regions.

Lu et al. [11] studied the combination use of asymmetric-histogram shifting method with the gradient adjusted gap, median edge detect, and interpolation by neighboring pixel to generate prediction errors, in their attempts to embed secret data in images. The authors demonstrated that different methods have varying performance outcome on the types of images (e.g. complex images or images with smooth edges).

5 Mobile apps

Due to the increasingly popularity of mobile apps, they are the subject of ongoing research efforts, including mobile recommendation systems via apps examined by Hsieh et al. [8] in this special issue. The authors presented a collaborative filtering-based mobile app recommender system, which is designed to suggest movies to the users. In addition, the system collects data related to the movies from external open web APIs, and uses cluster-based matrix factorization

to capture the shared preferences between user clusters and apps clusters, and the relationship between (categorized) App and movie based on the number of the overlapping features.

6 Future research directions

Despite the significant amount of published research attempting to address the wide range of multimedia social network security and application issues (e.g. in this special issue), there are a number of challenges that remain to be addressed, including social media platform security and trustworthiness measurement and evaluation by the new computing paradigm of crowd computing [23], as well as risk management and social-factor considerations in multimedia social network applications, etc.

We give thanks to all international reviewers for their valuable comments and suggestions for authors. Finally, we show special gratitude to MTAP Journal Editor-in-Chief, Prof. Furht, and managing editor Jay-y Banua and production coordinator Razel Gerona-Avanzado for their kind help, guidance and instruction, with a result of successful publication of the special issue.

References

1. Ariffin A, Slay J, Choo KKR (2013) Data recovery from proprietary formatted CCTV hard disks. In: IFIP WG 11.9 international conference on digital forensics 2013. IFIP advances in information and communication technology 410. Springer, Heidelberg, pp. 213–223
2. Azfar A, Choo KKR, Liu, L (2015) Forensic Taxonomy of Popular Android mHealth Apps. In Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 13–15 August 2015, Association for Information Systems
3. Azfar A, Choo KKR, Liu L (2016a) Forensic taxonomy of android productivity apps. Multimed Tools Appl doi:10.1007/s11042-016-3718-2
4. Azfar A, Choo KKR, Liu L (2016b) An android communication app forensic taxonomy. J Forensic Sci 61(5):1337–1350
5. Azfar A, Choo KKR, Liu L (2017) Forensic taxonomy of android social apps. J Forensic Sci
6. Barbon S Jr, Igawa RA, Zarpelão BB (2016a) Authorship verification applied to detection of compromised accounts on online social networks: A continuous approach. Multimed Tools Appl. doi:10.1007/s11042–016–3899-8
7. Feng W, Zhang Z, Wang J, Han L (2016) A novel authorization delegation for multimedia social networks by using proxy Re-encryption. Multimed Tools Appl 75(21):13995–14014
8. Hsieh M-Y, Chou W-K, Li K-C (2016) Building a mobile movie recommendation service by user rating and APP usage with linked data on Hadoop. Multimed Tools Appl. doi:10.1007/S11042-016-3833-0
9. Jalilzadeh SZ, Peng J, Choo K-KR, Ashman H (2016) Bit-level N-Gram Based Forensic Authorship Analysis on Social Media: Identifying Individuals from Linguistic Profiles. J Netw Comput Appl 70: 171–182
10. Jeyhoon M, Asgari M, Ehsan L, Jalilzadeh SZ (2016) Blind audio watermarking algorithm based on DCT, linear regression and standard deviation. Multimed Tools Appl. doi:10.1007/s11042-016-3934-9
11. Lu T-C, Chen C-M, Lin M-C, Huang Y-H (2016) Multiple predictors hiding scheme using asymmetric histograms. Multimed Tools Appl. doi:10.1007/s11042-016-3960-7
12. Niu P-P, Wang X-Y, Liu Y-N, Yang H-Y (2016a) A robust color image watermarking using local invariant significant bitplane histogram. Multimed Tools Appls. doi:10.1007/s11042-016-3935-8
13. Niu D, Rui L, Huang H, Qiu X (2016b) A service recovery method based on trust evaluation in mobile social network. Multimed Tools Appl doi:10.1007/s11042-016-3963-4
14. Peng J, Detchon S, Choo, KKR, Ashman H (2016a) Astrofurfing detection in social media: a binary N-gram based approach. Concurrency and Computation: Practice and Experience
15. Peng F, Gong X-Q, Long M, Sun X-M (2016b) A selective encryption scheme for protecting H.264/AVC video in multimedia social network. Multimed Tools Appl. doi:10.1007/s11042–016-3710-x

16. Quick D, Martini B, Choo KKR (2013) Cloud storage forensics. Syngress, an Imprint of Elsevier
17. Rout JK, Singh S, Jena SK, Bakshi S (2016) Deceptive review detection using labeled and unlabelled data. Multimed Tools Appl doi:10.1007/s11042-016-3819-y
18. Sahai A, Seyalioglu H, Waters B (2012) Dynamic credentials and ciphertext delegation for attribute-based encryption. In: CRYPTO 2012. Lecture notes in computer science 7417. Springer, Heidelberg, pp. 199–217
19. Wang Y, Yang J, Qiu G, Feng W (2016) A formalized delegation model for multimedia social networks. Multimed Tools Appl. doi:10.1007/s11042-016-3715-5
20. Yang Y, Liu JK, Liang K, Choo KKR, Zhou J (2015) Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data. In: ESORICS 2015. Lecture notes in computer science 9327. Springer, Heidelberg, pp. 146–166
21. Yang Y, Xu Z, Liu L, Sun G (2016) A security carving approach for AVI video based on frame size and index. Multimed Tools Appl. doi:10.1007/s11042-016-3716-4
22. Zhang Z (2011) Digital rights management ecosystem and its usage controls: a survey. Intern J Digit Content Technol Appl 5(3):255–272
23. Zhang Z, Gupta BB (2016) Social Media Trustworthiness and Security: Overview and New Direction. Future Generation Computer Systems 10 (Online)
24. Zhang Z, Wang K (2013) A trust model for multimedia social networks [J]. Soc Netw Anal Min 3(4):969–979
25. Zhang Z, Wang K (2015) A formal analytic approach to credible potential path and mining algorithms for multimedia social networks. Comput J 58(4):668–678
26. Zhang Z, Wang Z, Niu D (2015) A novel approach to rights sharing-enabling digital rights management for mobile multimedia. Multimed Tools Appl 74(16):6255–6271
27. Kechen Zhuang, Haibo Shen, and Hong Zhang. User spread influence measurement in microblog. Multimedia Tools and Applications, 2016. doi:10.1007/10.1007/s11042-016-3818-z

Dr. Zhiyong Zhang is a Henan Province Distinguished Professor and Dean with Department of Computer Science, Henan University of Science & Technology. He is also a Visiting Professor of Computer Science Department of Iowa State University. His research interests include multimedia social networks, digital rights management, trusted computing and usage control. He published over 100 scientific papers and edited 5 books in the above research fields, and also holds 10 authorized patents. He is IEEE Senior Member (06'M, 11'S), ACM Senior Member (08'M, 13'S), IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee. And also, he is editorial board member and associate editor of Multimedia Tools and Applications (Springer), Neural Network World, EURASIP Journal on Information Security (Springer), Social Network Analysis and Mining (Springer), as well as leading guest editor or co-guest Editor of Applied Soft Computing (Elsevier), Computer Journal (Oxford) and Future Generation Computer Systems (Elsevier). And also, he is Chair/Co-Chair and TPC Member for numerous international conferences/ workshops on digital rights management and cloud computing security.

Dr. Kim-Kwang Raymond Choo is a Fulbright Scholar and Senior Researcher at the University of South Australia. His publications include a book in Springer's "Advances in Information Security" series and a book published by Elsevier (Forewords written by Australia's Chief Defence Scientist and Chair of the Electronic Evidence Specialist Advisory Group). His awards include the British Computer Society's Wilkes Award for the best paper published in the 2007 volume of Computer Journal. He is the editor of IEEE Cloud Computing Magazine's "Cloud and the Law" column and the Book Series Editor of Syngress/Elsevier's "Advanced Topics in Security, Privacy and Forensics".