International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.209-220
http://dx.doi.org/10.14257/ijsia.2016.10.4.20

A Secure Fingerprinted Multimedia Distribution Using Social Network Analysis

Cong-huan Ye, Zeng-gang Xiong*, Yao-ming Ding,
Xueming Zhang, Guangwei Wang and Fang Xu

College of Computer and Information Science,
Hubei Engineering University, Xiaogan, Hubei, China
xzg@hbeu.edu.cn

Abstract

Collusion attack is a very effective attack for digital fingerprinting system. In order to remove or attenuate the fingerprint information hidden in fingerprinted content, a number of users produce a new colluded copy through their own fingerprinted copies. In this paper, we address a novel collusion-resisting desynchronization fingerprinting approach using social network analysis. The novelty of this paper is that collusion attack occurred in a multimedia social network community with high probability. Different from all existing works, with desynchronization model constructed upon social network, the original image is desynchronized to get many similar copies which are different from each other, and then they are assigned and distributed to subscribers according to social network analysis. Theory analysis shows that the presented desynchronization distribution method has significantly better performance than those existing distribution schemes. The experimental results also show that the average colluded images even with only two desynchronized copies have poor visual quality. And the visual quality of colluded images does not improve apparently with the increase of the number of copies.

Keywords*: multimedia fingerprinting, average collusion attack, social network, digital watermarking*

1. Introduction

With the fast development of multimedia processing and mobile network communication technology recently, it becomes more and more efficient to share content in multimedia social network. Concerned about security and privacy, content owners usually protect their content with digital fingerprinting [1]. There are other measures such as image encryption, image hash, copy detection, and information hiding to protect multimedia content from illegal use. Encryption schemes of multimedia have been proposed in many articles[1-9], in most of these paper, the chaotic map was generalized to design secure encryption schemes, which thereby significantly increased the resistance to misuse of multimedia. Encryption [41-43] may ensure secure multimedia transmission through communication networks; however, if the encrypted content is decrypted, there are no other ways to protect content anymore. But copy detection techniques may be used to provide copyright protection successively.

Multimedia copy detection, which could apply to multimedia content circulated, is critical to preventing copyright violations and enforcing intellectual property rights (IPR). If the similar image, which is suspected as the illegal distributed copy, is being illegally shared in multimedia social network, the owner can query the copy detection system.

* Corresponding Author

ISSN: 1738-9976 IJSIA

The copy detector then extract feature of the suspected one, and then compares the image feature with the original image feature stored in the index database [10]. Different copy detections to the illegal distribution have been proposed in the past few years [9-15].

Information hiding is another technology to protect copyright. Digital multimedia is increasingly popular in multimedia social network. With watermark embedding technology, mark information, which can help to prevent unauthorized distribution directly [16]. The embedded marks are known as digital watermarking academically. Digital watermarking, which is alternative approach to copyright enforcement, must be inserted into the original content as copyright marking before copies are made. On the other hand, due to the wide popularity of sharing multimedia in social networks, security and privacy protection has become very important. Digital watermarking can be used to protect ownership, copyright authentication, and digital fingerprinting [17]. For copyright authentication, various digital watermarking techniques [16-22] have been adopted to deter misuse of multimedia data in multimedia social network. Now the usage of digital watermarking should robust to resist common geometric transformations and some signal processing operations [18], which should not damage the watermark information. Even if the most robust digital watermark can not trace the pirate who shares the multimedia content illegally in social network, in order to provide solution, a special watermarking scheme, fingerprinting, could be applied.

Digital fingerprinting is a technology which can be used to trace the illegal redistribution in fingerprinting system, where digital fingerprints are embedded into the multimedia content as the ID. However, collusion attack is the main challenge that digital fingerprinting technology has to face, because a set of users can produce a new copy with their own fingerprinted copy, the fingerprint information hidden in the colluded copy can be removed, in this case, the detector will not detect the users who redistributed the copy in social network. As we know, these colluders must know each other or come from a same social network, so they could format a special crime unit. Inspired by this scenario, our multimedia fingerprinting will protect the multimedia content from redistribution based on social network analysis. In multimedia social network, those who take part in collusion attack must be having some social relationship. The community structure can be identified with social network analysis [27]. Therefore, colluders must come from the same community, and they will decide to choose which collusion attack to get the max profit. Digital fingerprinting should resist collusion attack to prevent redistributing of the fingerprinted copy [35].

In this work, we address a novel desynchronization fingerprinted multimedia distribution scheme using social network analysis to combat average collusion attack. This is the first time the desynchronized fingerprinted content is distributed with social network analysis. The related works are introduced in section 2, and followed by explain of social network in section 3. In section 4, we show the desynchronization distribution method and the performance of the scheme. In Section 5, we show the experimental results. Section 6 concludes this paper and show the future research.

2. Related Works

Considered about the possible collusion attack scenario, the owner has to embed fingerprints into original multimedia content, the fingerprint should be secure against collusion attacks. With collusion attack a set of users can generate a colluded version in order to disturb their fingerprint information, which makes the server fail to trace traitor [32]. In [35], Kiyavash *et al*. proved that order statistic collusion attack can minimize the probability of success of the detector. Zhao *et al*. [36] analyzed a number of collusion attack and show their effect. In order to resist collusion attack, some digital fingerprinting technologies are proposed in [33]. Cha *et al*. addressed a fingerprinting system which is

based on MC-CDMA, and the performance resisting time-varying collusion attack is analyzed in [34].

Fingerprinting code technologies, used by many researchers, may try to improve performance of fingerprinting system. The c-secure fingerprint code is secure against collusion attack of c pirates with ε-error [22-24]. In [25, 26, 31], a short random fingerprint code has been addressed. The rapid development of telecommunication systems makes multimedia distribution in social networks very easy. Users usually share multimedia content in social network [28-31]. In the meantime, the increase of unauthorized use will happen because of this ease of sharing. In order to maximize their own payoff, and minimize the risk of being traced, they communicate with each other to generate the colluded copy. The paper [37] collectively addresses security and broadcast efficiency for network-centric entertainment systems of educational medical videos. Lian SG *et al*. proposed a combined scheme include watermarking, encryption, fingerprinting, and encoding, to distribute multimedia content via network and protect data from illegal use in [38].

In this paper, we aim to resist average collusion attack. Different from these related works, the multimedia fingerprinting focuses on that some users in digital system may only need the lower resolution copy of original high-valued super resolution image and the social relationships of these users, our fingerprinted multimedia distribution based on users' social network, which is inspired by the coalition occurred in social network community with high probability. Multimedia content distribution aims at efficiently and effectively deterring the illegal collusion of traitors belonging to social network communities.

3. Analysis of Social Networks

Social networks can be social relationship network in which a set of entities interact with each other. In colluders' social networks, a group of traitors, who club together to perform collusion attack, wish to destroy fingerprinting system. Social network analysis mainly analyzes the social relationships between members. Graph can be used model social network. The nodes in graph are the members in social network, while the links in graph show social relationships between the members in social network. Social network analysis can provide a mathematical analysis of human social relationships. Many mathematical methods, especially graph theories, are available to measure networks. We will also show how to use these graph metrics to analysize colluders' social networks for fingerprinted multimedia distribution. In this paper, we focus on colluders' collaboration relationship, which is inspired by the collaboration network of film actors, networks of coauthorship among academics, and terrorist networks.

Given the graph $G = (V, E)$. The elements of $V \equiv \{v_1, v_2, \ldots, v_n\}$ are the nodes of the graph G, while the elements of $E \equiv \{e_1, e_2, \ldots, e_n\}$ are its links (or edges). A graph $G'=(V', E')$ is a subgraph of $G = (V, E)$ when $V' \subseteq V$ and $E' \subseteq E$. $\delta(v_i)$ denotes the degree of a node v_i which can be represented by the number of neighbors of the node. Assume A is the adjacency matrix of graph G, we have

$$\delta(v_i)= \sum_{v_j \in V} A_{ij} = \sum j A_{ij} \quad (1)$$

Community is one of important properties for social network. The subgroups are used to name communities in this paper. Community detection means the decomposition of a set of actors into just different subgroups. In the following, we will discuss community structures within a social network.

In general, entities have a high density of edges within community; on the contrary, the number of edges between groups is less. Communities based on numerous ties require that their members have ties to many others within them. Some cohesive community

structure ideas are concerned with the linkages that are established among individuals by virtue of their common membership in collectivities. The communities are known as groups or clusters. Communities can be demonstrated visually by a network map, as shown in Figure 1.

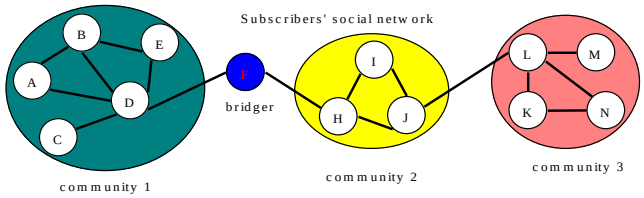


Figure 1. Community Structure with 3 Communities

Given a graph $G = (V, E)$ with N nodes, the algorithms for community detection can be regarded as finding a partition $P_C = \{C_1, C_2, \ldots, C_c\}$ if the following quantifications

$$C_i \cap C_j = \varnothing \quad (i, j = 1,2, \ldots, c \text{ and } i \neq j) \tag{2}$$

$$\cup_i C_i = V \ (i = 1, 2, \ldots, c) \tag{3}$$

are true. where C_i ($_i$ = 1, 2, … , $_c$) is subset of V, c is the number of communities of a social network. In order to evaluate with which communities are found in social networks, Newman and Girvan [39] used the modularity Q to measure the performance of the community detection algorithms:

$$Q = \sum_i (e_{ii} - a_i^2) \ (i = 1, 2, \ldots, c) \tag{4}$$

For the total weights of all edges in whole social, considered community i, e_{ii} is the fraction of weights of edges within the community, and a_i is the fraction of weights of edges connecting the community with other communities. The edge weight equals 1 if the graph of the complex network is unweighted.

4. Proposed Fingerprinted Multimedia Distribution Scheme

The tiny geometric transform to the original high resolution image does not significantly affect the perceived quality. In this research, we focus on that sometimes the users in fingerprinting system want to buy lower resolution version mapping to original valued high-resolution image because of some personal reasons. According to these needs of user-specific, the original image is distorted via geometric process which include warping and cropping suffered the limit of human visual model, then the geometric processed image is subsampled to a lower resolution image which meets the need of user-specific. We call these processes preprocessing in this article.

In this paper, we mainly focus on deterring average collusion attack and how to distribute desynchronized images. First, we produce an user-specific resolution image according to the request of user through image warping, image cropping and sub-sampling. Then, every preprocessed desynchronized image assigned for each particular user according to their social relationships. Finally, fingerprint is then embedded into the desynchronized copy, and the fingerprinted desynchronized images are distributed to user with social network analysis.

4.1. Image Preprocessing for Desynchronization

In social network, the method of preprocessing poses a tradeoff for a large number of subscribers. Preprocessing must not introduce apparently visual distortion while keeping desynchronization to resist average collusion attack. In this paper, we resort to social network analysis distributing a small number of desynchronizated images.

Assume that there is an original image $G_{original}$ with high resolution, the size of this image is $M_G \times N_G$. In the original image, there is an image pixel point at the corresponding coordinate. The value between 0 and *K-1* of this pixel point denotes When receive the request of user, this image $G_{original}$ is preprocessed to get a small size image with resolution $M_G' \times N_G'$, and the preprocessed desynchronized image will be embedded with a fingerprint mark for subscriber *i* before the preprocessed image is delivered to subscriber *i*. Figure.2 shows the process of the image preprocess.

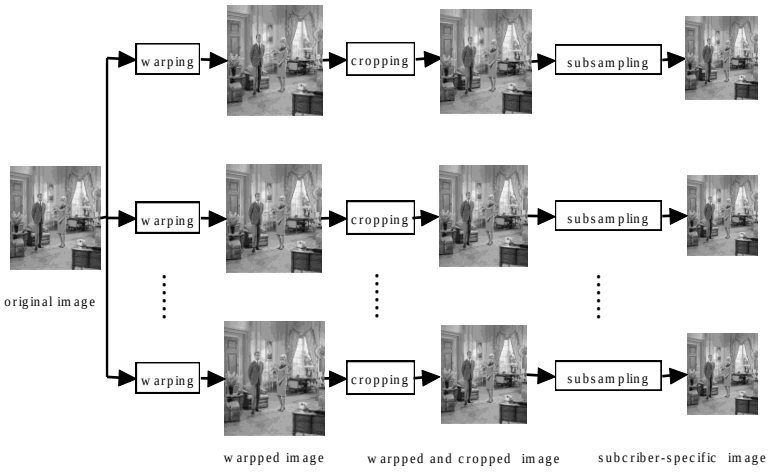


Figure 2. The Framework of Generation of Subscriber-Specific Images

First, original image is warped according to human visual system. The set of warping functions is denoted by F_w. The cardinality of F_w is denoted by $|F_w|$, which represents the number of functions in the set, however, because of distortion limit, $|F_w|$ could not be too large. In this paper, we fix $|F_w|$, but the element of F_w is adapted to multimedia content in order to get good desynchronization effect with Human Visual Model. An original image warped by $|F_w|$ warping functions, so we can get $|F_w|$ analogous desynchronized images. These images together with the original one with high resolution are regarded as $|F_w| + 1$ benchmark images. Figure.3. shows that the PSNR of different warped images with different warping functions, and the preprocessed images are shown in Figure.5. Compared to the original, there is no clear difference with human visual model.

Assume that the most important information is in the central area of images. Then, we can crop the margin part of the warped high resolution image accordingly. So these benchmark images will be cropped and keep the most centre area in which the important information is. However, the cropped image border should be limit. For the original image with resolution $M_G \times N_G$, there is a cropping function with three different parameters which are the size of cropped image, the location *(x,y)* of the upper left corner of reserved area in the original image. For every subscriber, a sole combination of three parameters is assigned to the cropping function. However, the location *(x,y)*,which lie in some region in original image, is limit by the size of cropped image in order to meet the request of subscribers.

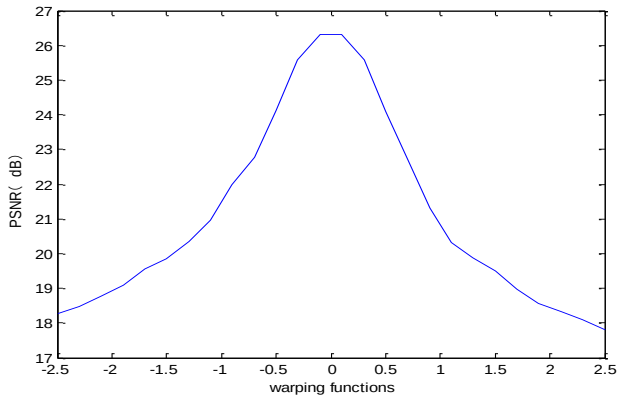


Figure 3. PSNR （Warped Images）

The preprocessed images are finally down sampled to subscriber-specific images with low resolution $M^{(i)}{}_G' \times N^{(i)}{}_G'$. For $G_{subsample,}$ and pixels $i,j, 0 \leq i < N_G', 0 \leq j < M_G'$

$$G_{subsample} = \sum_{m=-1}^{1} \sum_{n=-1}^{1} w(m,n) G_{original} \quad (2i+m, 2j+n) \tag{5}$$

where $w(m,n)$ is a 3-by-3 window.

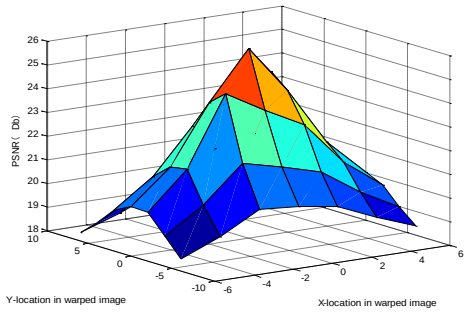
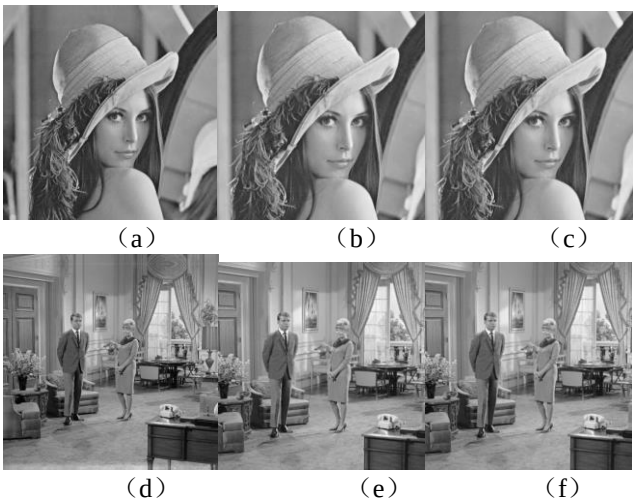


Figure 4. PSNR （User-Specific Images）

4.2. Fingerprints Embedding and Detection

In this paper, the fingerprints will be embedded in the DWT domain. After the preprocessed images are produced, we employ 2-level DWT. An image is split into *LL* subband, *LH* subband, *HL* subband, and *HH* subband. The coefficients of *LL* subband are then transformed by DWT. After decomposition, the coefficients of all 2nd-level subbands are used to embed fingerprint related subscriber. In this paper, we consider orthogonal fingerprint embedding. Because of the social relationships of subscribers, the fingerprints assigned to subscribers are composed of two parts: community *id* to which subscriber belongs and the inner fingerprint code for subscriber. The coefficients in the 2nd-level *HH* subband are used to embed the community *id*, and the coefficients in other 2nd-level subband are embedded with inner fingerprint code related to subscriber. Suppose N_c and N_u are two orthogonal vectors, which are regarded as community outer code segment and user inner code. We choose the $|N_c|$ coefficients in the 2nd- level *LH* and *HL* subbands to combine a vector, $X_c=(x_1, x_2, \ldots, x_{|Nc|})$, to imbed community code, and the largest $|N_u|$ coefficients in the 2nd- level LL subband, as a vector $X_u=(x_1, x_2, \ldots, x_{|Nu|})$, to hide inner fingerprint codeward related subscriber.



(a) and (d) Are Original Lena, Couple, (b) and (e) Are the Corresponding User-Specific Images, (c) and (f) Are the Fingerprinted Ones

Figure 5. Images Comparison

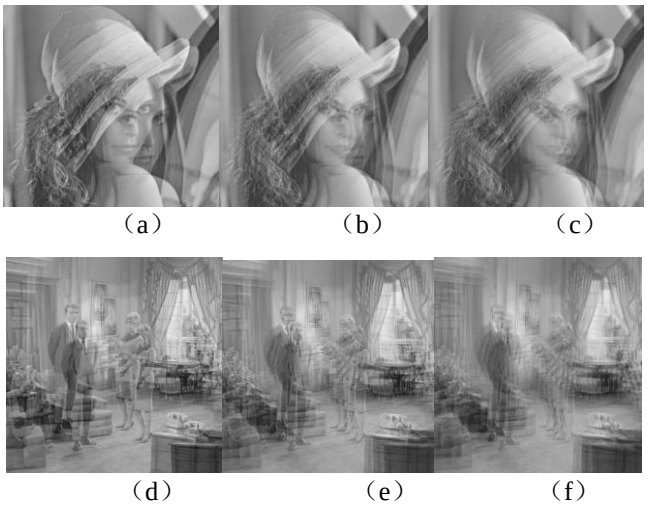
After fingerprinting in discrete wavelet transform domain based on subscribers' social network. The preprocessed images are similar to original ones in human visual model according to Figure.5. From Figure.5, we also know that the fingerprinting method has a perfect vision effect under allowance of human sight. In order to trace traitor, the owner should extract the fingerprint information in the suspected copy, the detector should decompose the fingerprinted image using the wavelet technique so that the coefficients of all 2-level subbands are produced. Two $|Nc|$ and $|Nu|$ coefficient series, which compose a long vector z, where the length of z is $|Nc|+|Nu|$, are extracted from the 2nd-level subbands, the minimum distance is used to identify traitor.

5. Experimental Results

We apply preprocessing to desynchronize image, then the desynchronized images are assigned to users according to social network analysis, finally, fingerprint information is embedded into the DWT domain. Detection is performed using equation (10) to trace the traitor. In these experiments, we mainly focus on the visual effect of average collusion attack. Figure.5 shows the original images and the preprocessed images. The average PSNR of the average PSNR of colluded copy is demonstrated in Figure.6, from which it can be seen that the change of the average PSNR of colluded copy with the increase of the number of colluders. Compared to the original images in Figure.5, the visual quality of desynchronized images is not apparently degradation in comparison with the original images, it also can be found that the fingerprint information embedded into the desynchronized copy do not reduce the visual quality according to the human visual model. However, the average collusion attack can reduce the visual quality of the colluded images, from which there exists blurry effect in Figure.6. Average collusion attacks using two, three, and four fingerprinted images are used to generate colluded images. From Figure.6, the image is very blurred and the detail information can not be observed in these images, and the perceptual quality is more and more degraded with the increase of number of colluded copies.

Figure.7 displays PSNR of the attacked signals. For image without preprocessing, namely, the classical fingerprinting scheme, the PSNR of the colluded copy does not large change with the increasing number of desynchronized fingerprinted copy. Without preprocessing, this means a non-quality decrease (almost 50 dB in PSNR). In the presence

of preprocessing, the PSNR metric is decreased rapidly with the increase of number of fingerprinted desynchronized copy because of the desynchronization of the colluded copies. However, compare to assignment scheme based on social network analysis, the PSNR is higher than that of latter once the number of colluders is small.



(a), (b), and (c), are Average Colluded Lena with 2, 3, and 4 Copies Respectively, so do the Couple

Figure 6. Colluded Images

So the proposed multimedia fingerprinting scheme based on social network analysis could reduce visual quality of the average colluded copy even small number of colluder. According to Figure.6 and Figure.7, the proposed scheme is more effective to generate blurred image by averaging desynchronized image with assignment based on social network analysis.

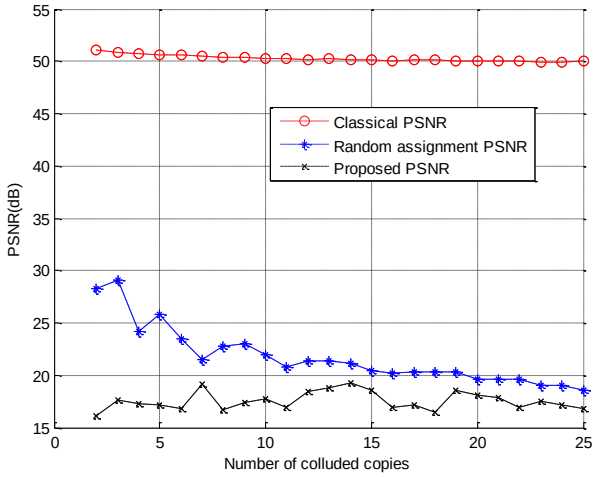


Figure 7. Average PSNR of Colluded Copy Versus Number of Colluders

5. Conclusion and Future Research

In this paper, we have addressed a desynchronization multimedia fingerprinting scheme. This paper has two main contributions: (1) a new image desynchronization can produce user-specific images, such as the lower resolution version of original high resolution image; (2) a scheme assigns desynchronized images to users using social

network analysis. Our approach is based on the subscriber-specific need of image and social network analysis. Each uniquely preprocessed copy of the host-signal prior to be assigned according social network analysis. The proposed scheme can be applied to multimedia social network, in which the proposed scheme can resist average collusion attack even if there is a large number of users in social network.

Acknowledgments

This work is supported by the NSF of China under Grant No. 61502154, 61370092 and 61370223, Natural Science Foundation of Hubei Province of China (No. 2015CFB236, 2014CFB188), and Youth innovation team project in Hubei Provincial Department of Education (No. T201410).

References

[1] E.T. Lin, Eskicioglu AM, Lagendijk RL. ,‘‘Advances in digital video content protection’’, Proceedings of the EEE, vol. 93, no. 1, **(2005)**, pp. 171-183.
[2] G.R. Chen, Y.B. Mao, C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps”, Chaos Solitons and Fractals, vol. 21, no. 3, **(2004)**, pp. 749-761.
[3] H. Cheng, X.B. Li, “Partial encryption of compressed images and videos », IEEE Transactions on Signal Processinh, vol. 48, no. 8, (**2000)**, pp. 2439-2451.
[4] K. Shou-qiang, Z Jian-yu, W Yu-jing, J Bin, L Chao-feng, G Hua-qiang. «A Streaming Media Secure Communication Method Combined by Dynamic Key of Dual Chaotic Systems and RSA. Journal of Harbin University of Science and Technology, vol. 20, no. 4, **(2015)**, pp. 09-115.
[5] Q.A. Zhang, Q.A Wang, X.P. Wei, “A Novel Image Encryption Scheme Based on DNA Coding and Multi-Chaotic Maps”, Advanced Science Letters, vol. 3, no. 4, **(2010)**, pp. 447-451.
[6] Y. Wang, K.W. Wong, X.F. Liao, “A new chaos-based fast image encryption algorithm”. Applied Soft Computing, vol. 11, no. 1, **(2011)**, pp. 514-522.
[7] L. CQ, L. SJ, M. Asim, “On the security defects of an image encryption scheme”, Image and Vision Computing, vol. 27, no. 9, **(2009)**, pp. 1371-1381.
[8] F. Huang, Y. Feng, X.H. Yu. “A symmetric image encryption scheme based on a simple novel two-dimensional map”, International Journal of Innovative Computing Information and Control, vol. 3, no. 6B, **(2007)**, pp. 1593-1602 .
[9] C. Kim, “Content-based image copy detection”, Signal Processing-image Communication”, , vol. 18, no. 3, **(2003)**, pp. 169-184.
[10] M-N Wub, C-Ch Linc, and C-Chen. “Novel image copy detection with rotating tolerance” ,Journal of Systems and Software. vol. 80, no. 7, **(2007)**, pp. 1057-1069.
[11] M Douze , H Jegou, C Schmid, “An Image-Based Approach to Video Copy Detection With Spatio-Temporal Post-Filtering”, IEEE Transactions on multimedia, vol. 12, no. (4), **(2010)**, pp. 257-266.
[12] Z Xu, H Ling, F Zou, et al. “A novel image copy detection scheme based on the local multi-resolution histogram descriptor”. Multimedia Tools and Applications, **(2010)**.
[13] H. Ling, L. Wang, F. Zou, “Fine-search for image copy detection based on local affine-invariant descriptor and spatial dependent matching”. Multimedia Tools and Applications, **(2010)**.
[14] D.N. Bhat, S.K. Nayar, “Ordinal measures for image correspondence”. IEEE Trans Pattern Anal Mach Intell, vol. 20, no. 4, **(1998)**, pp. 415–423.
[15] J.H. Hsiao, C.S. Chen, L.F. Chien, M.S. Chen, “A new approach to image copy detection based on extended feature sets”, IEEE Trans Image Process,vol. 16, no. 8, **(2007)**, pp. 2069–2079.
[16] Petitcolas FAP, Anderson RJ, Kuhn MG, “Information hiding - A survey”. PROCEEDINGS OF THE IEEE. vol. 87, no. 7, **(1999)**, pp. 1062-1078.
[17] M. Saikia, S. Majumder, and T.S Das,. Coded Fingerprinting Based Watermarking to Resist Collusion Attacks and Trace Colluders. Advances in Computer Engineering (ACE), 2010 International Conference on, **(2010)**, pp.120 – 124.
[18] IJ Cox, J. Kilian, FT Leighton, “Secure spread spectrum watermarking for multimedia”, IEEE Transactions on Image Processing, vol. 6, no. 12, **(1997)**, pp. 1673-1687.
[19] B Chen, GW Wornell. “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding”, IEEE Transactions on Information Theory, vol. 47, no. 4, **(2001)**, pp. 1423-1443.
[20] D Boneh, J. Shaw, “Collusion-secure fingerprinting for digital data”, IEEE Transactions on Information Theory, vol. 44, no. 5, **(1998)**, pp. 1897-1905.
[21] XY Luo, DS Wang, P Wang, et al. A review on blind detection for image steganography, Signal Processing, vol. 88, no. 9, **(2008)**, pp. 2138-2157.

[22] A. Barg, G. Blakley and G. Kabatiansky, "Digital fingerprinting codes: problem statements", constructions, Identification of traitors. IEEE Trans. on Information Theory, vol. 49, **(2003)**, pp.852–865.
[23] D. Boneh and J. Shaw, "Collusion-secure Fingerprinting for digital data. IEEE Trans. on Information Theory" , vol. 44, **(1998)**, pp.1987–1905.
[24] C. Ye, Z. Xiong, Y. Ding, X. Zhang, G. Wang, F. Xu, Joint Fingerprinting/Encryption for Medical Image Security, International Journal of Security and Its Applications, vol. 9, **(2015)**, pp. 409-418.
[25] C. Ye, Z. Xiong, Y. Ding, G. Wang, J. Li, K. Zhang, "Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks", Journal of Visual Languages & Computing, vol. 25, **(2014)**, pp. 658-666.
[26] D. Megias, "Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints" , Dependable and Secure Computing, IEEE Transactions on, vol. 12 , **(2015)**, pp. 179-189.
[27] A. Qureshi, D. Megías, H. Rifà-Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems" , Expert Systems with Applications, vol. 42, **(2015)**, pp. 1391-1408.
[28] C. Ye, H. Ling, F. Zou, Z. Lu, A new fingerprinting scheme using social network analysis for majority attack, Telecommunication Systems, vol. 54, **(2013)**, pp. 315-331.
[29] W.S., L Zhao H.V.and Liu, K.J.R, "Fairness dynamics in multimedia colluders' social networks". Image Processing, 2008(ICIP 2008), 15th IEEE International Conference on, **(2008)**, pp. 3132-3135.
[30] W.S. L Zhao H.V. and Liu, K.J.R. Behavior modeling and forensics for multimedia social networks :A case study in multimedia fingerprinting. Signal Processing Magazine, IEEE , vol. 26, no. 1, **(2009)**, pp. 118 - 139.
[31] B.-H. Cha, S.-I. Choi, "Continuous media fingerprinting against time-varying collusion attacks", Information Sciences, vol. 298, **(2015)** , pp. 66-79.
[32] H. Feng, H. Ling, F. Zou, W. Yan, M. Sarem, Z. Lu , A collusion attack optimization framework toward spread-spectrum fingerprinting, Applied Soft Computing, vol. 13, **(2013)**, pp. 3482-3493.
[33] C. Ye, J. Li, Z. Xiong, "A Secure Content Distribution Based on Chaotic Desynchronization", in: Computer, Consumer and Control (IS3C), 2012 International Symposium on, IEEE, **(2012)** ,pp. 906-909.
[34] B. H. Cha, and C. C. J. Kuo, "Robust MC-CDMA-Based Fingerprinting Against Time-Varying Collusion Attacks". Information Forensics and Security, IEEE Transactions on, vol. 4, no. 3, **(2009)**, pp. 302-317.
[35] N. Kiyavash, and P. Moulin.A Framework for Optimizing Nonlinear Collusion Attacks on Fingerprinting Systems, Information Sciences and Systems, 2006 40th Annual Conference on, **(2006)**, pp. 1170-1175.
[36] HV Zhao, M Wu, ZJ Wang, et al. (2005). Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting, IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 14, no. 5, **(2006)**, pp. 646-661.
[37] W Luh and D Kundur, "New Paradigms for Effective Multicasting and Fingerprinting of Entertainment Media". IEEE Communications Magazine , **(2005)**, pp:77-84 .
[38] SG Lian, ZX Liu, Z Ren, et al. "Secure advanced video coding based on selective encryption algorithms". IEEE Transactions on Consumer Electronics, vol. 52, no. 2, **(2006)**, pp. 621-629.
[39] M.E.J. Newman, M. Girvan. "Finding and evaluating community structure in networks". Phys. Rev. E 69 026113, **(2004)**.

Authors

Conghuan Ye, he received the B.S. and M.S. degree in computer science from Hubei Normal University, Hubei, China, in 2002, and University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2005, respectively. Now, his research interests include digital fingerprinting, digital right management, complex network, and cloud computing. Dr.Ye received the scholarship from UESTC from 2003 to 2004.

He has co-authored over 40 publications including book chapters, journal and conference papers. He received the Ph.D. degree in computer science and technology, Huazhong University of Science and Technology (HUST) in 2013, Wuhan, Hubei, China. Since 2013, he has been an associate professor with the college of computer science and technology, HBEU.

Zenggang Xiong, he received the MA degree from Hubei University, China, in 2005, and the PhD degree in computer science from Beijing University of Science and Technology, China, in 2009. He is now a professor in Hubei Engineering University. His research interests are in the areas of peer-to-peer computing, Cloud computing, distributed systems and big data.

Yaoming Ding, he received the MA degree from Huazhong Normal University, China, in 2000, and the PhD degree in education from Huazhong Normal University, China, in 2011. He is now a professor in Hubei Engineering University. His research interests are in the areas of optical communication technology and cloud computing.

Xuemin Zhang, She received the Bachelor degree in computer science from Hubei Normal University, China, in 2001, and the MA degree in computer science from Wuhan University of Technology, China, in 2009. She is now an associate professor in Hubei Engineering University. Her research interests are in the areas of Cloud computing, distributed systems, Service Computing. She is a member of the IEEE and the ACM.

Guangwei Wang, he received the B.S. and M.S. degree in computer science from Huazhong Normal University, Wuhan, China, in 2005 and 2008, respectively. He received the Ph.D. degree from Huazhong University of Science and Technology in 2012. Now, He works in School of Computer and Information Science, Hubei Engineering University and his research interests include Computer vision and video analysis. He has co-authored more than 10 papers published in various journals.

Fang Xu, he received the B.S. and M.S. degree in computer science from Hubei Engineering University, Hubei, China, in 2003, and Wuhan University, Wuhan, Hubei, China, in 2009, respectively.

Now, his research interests include Mobile Social Networks, digital fingerprinting, Machine Learning, and cloud computing.

Dr. Xu has co-authored over 20 publications including journal and conference papers. He is currently a Ph.D. student in the Wuhan University at Wuhan, majoring in computer science and technology.