International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.7 (2016), pp.311-320
http://dx.doi.org/10.14257/ijmue.2016.11.7.31

Recursive Chaotic Desynchronized Fingerprint for Large Scale 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
E-mail: xzg@hbeu.edu.cn

Abstract

Average collusion attack is a very effective attack for digital fingerprinting system. Moreover, the commercial value of the colluded content is often time-sensitive. The more profit the colluder will make from it when the colluded copy is distributed earlier. This paper presents a new collusion-resilience approach with recursive chaotic desynchronization and social network. It has processed chaotic transformations due to random image grid based on chaos. The experimental results show that collusion even with only two copies results in degradation of the image metric, even if those traitors try to resynchronization using image registration technology. However, it will take expensive computational cost to do that, and the visual quality is degraded expensively with the increase of the number of fingerprinted copies.

Keywords*: fingerprinting, collusion attack, chaos, social network, multimedia distribution*

1. Introduction

With the fast advance of mobile multimedia communication technology and the dramatic penetration of embedded devices, including IPads, PCs, mobile terminals, IPTVs, *etc.* For content security and privacy protection in multimedia communication, digital rights management technologies are used for deter content redistribution [1]. Fingerprinting [1-2] is one of the technologies used to deter the illegal redistribution by embedding a digital ID information into the original content. The paper [3] discussed how to assign different codeword to different user for tracing multimedia copy. B Czaplewski addressed the problem of unauthorized redistribution of multimedia content in [4]. Continuous media fingerprinting [5] was proposed by BH Cha to against time-varying collusion attacks. Digital fingerprinting can deter illegal use of multimedia copy, however, the fingerprinting will be invalid if there are enough users to attack the fingerprinted copy [6], furthermore, it will be more difficult for digital fingerprinting system to trace illegal user when pirates using many different collusion attacks together [7].

Human vision system (hvs) can not perceive the tiny geometric transform of multimedia content. A secure streaming media distribution method is addressed in [8]. Similar schemes are proposed in [7, 9-10] to deter average collusion attack. With these schemes, the quality of colluded copy will be degraded.

ISSN: 1975-0080 IJMUE

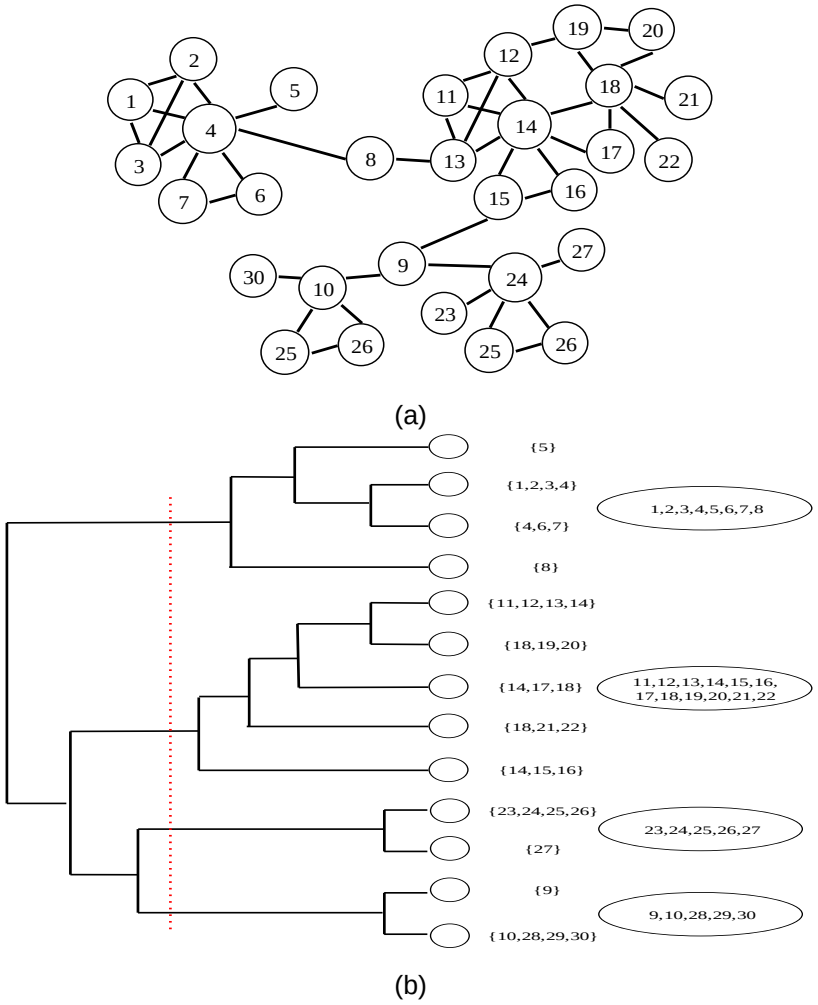

Figure 1. The Dendrogram of Social Network (a) the Social Network, and (b) the Community Structure of the Network

For desynchronization fingerprint [11] in such applications, there are two important issues to be resolved: one is that exist schemes can not deter collusion attack completely. Another is that these proposed schemes do not consider the number of desynchronized copies for very large scale fingerprinting system [12]. For the former problem, resynchronization can be used to desynchronized copies. For the later, a professional photo of some star can be used by Tens of millions of fans (such as downloading from the homepage), these proposed desynchronized schemes cannot guarantee the enough difference between any two copies of desynchronized images. In [13-14], the authors proposed P2P multimedia distribution schemes respectively. Inspired by P2P multimedia distribution scheme, we represent a valid social multimedia distribution strategy according to social network analysis to deter average collusion attack. When they produce the colluded copy, the desynchronization will be discovered; therefore they will use all kinds of technologies to resynchronization.

On one hand, colluders always communicate with each other deciding how to produce the colluded copy through social network, and sometimes they use resynchronization scheme to undo the desynchronization. On the other hand, the advantage of chaos lies in its disorderly and unsystematic character. The chaotic change will be very difficult to realize image registration. For the joint chaotic desynchronization and social network analysis for secure content distribution, there's no other researcher who do the related research work until now.

In this research, we represent a new chaotic desynchronization strategy for the possible resynchronization. The complex chaotic desynchronization method can deter resynchronization effectively, and with social network analysis, the distribution system is more secure than the known desynchronization schemes. In Section 2, we discuss our novel chaotic desynchronization distribution method with social network analysis, and followed by the security evaluation in Section 3. Section 4 concludes this paper.

2. Desynchronized Content Distribution

2.1. Community detection

Given a users' multimedia social network, we detect community structure. In real social networks, there is a hierarchical and overlapping community structure. Overlapping structure indicates that some nodes belong to multiple communities; these overlapping nodes are hubs between groups.

In this subsection, we will get the community structure of multimedia social network with the method used in [15-16]. The method has two stages. First, a dendrogram is generated. Then, an appropriate cut is used to break the dendrogram into communities. The community detection scheme is presented as Figure1 shows.

2.2. The Desynchronization Framework

The image desynchronization framework is shown in Figure 2. The desynchronization method consists of four stages. First, we generate global warped images based on the max community of social network. Second, the random grids for these warped images are produced based on chaos as Figure 3 shows. Third, different warping functions are generated by chaos to transform corresponding patches in the random image grids. Fourth, repeat the second and third stages.

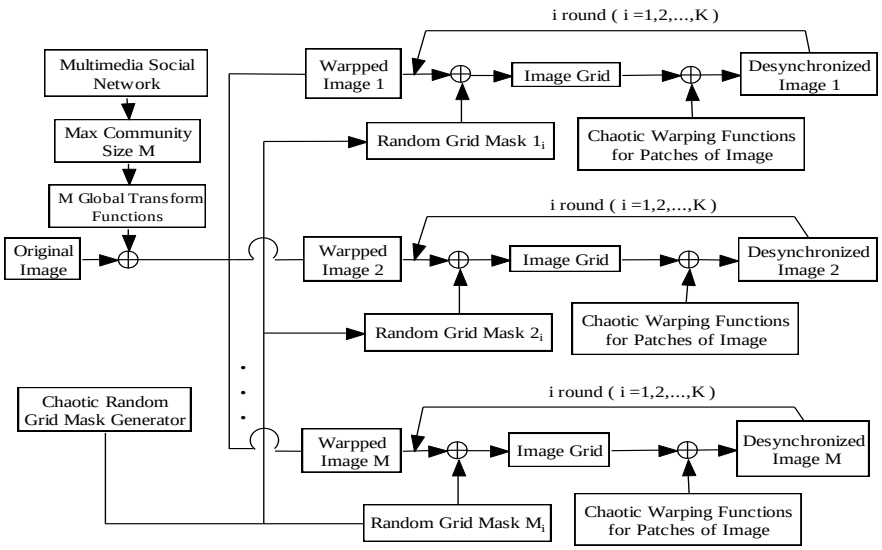

Figure 2. Parallel Chaotic Desynchronization Based on Social Network

2.3. Chaotic Desynchronization Based on Random Grid

The image desynchronization is to find a perceptually admissible subset of the possible transform functions that introduce small or no perceptual change. For an original image, we produce *M* random grid template every round, and then the image will be partitioned by a set of non-overlapping rectangle areas which are patches with

different size. Two random grid templates are shown in Figure3. The warping functions are produced randomly, which means the transform functions are chosen to warp the corresponding patches at random [9].

In this research, all the geometric transforms are performed for change the location of pixels in every single local rectangle patches. For simplicity, we change the horizontal location of a pixel, and the max horizontal displacement distance is decided by the image visual perception quality. For every pixel, the displacement place will be produced by the geometric transform function, and then in the vertical direction, each pixel in a rectangle block is transformed with the similar method. For an image *I*, $\partial_i(I)$ is the transformed image which is identical to the original image *I*, but the total Euclidean distance of all corresponding pixels between the original image and the transformed one is very large. By mapping the pixel coordinates in the original two-dimensional image to the corresponding coordinates in the chaotic geometric transformed two-dimensional image, the mathematical expressions can be different for each particular patch [17].

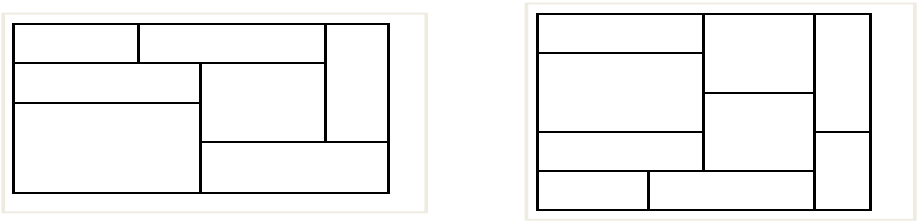

Figure 3. Two Random Image Grid Templates for Partition

The geometrid transform of a patch P is a mapping F: $P \to P$ of the form:

$$F(X) = AX + d = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix} \quad (1)$$

Namely, the transformed coordinate is

$$(x', y') = (x + \partial_x(x), y + \partial_y(y)) \quad (2)$$

where (x, y) and (x', y') are location of the original pixel and the transformed pixel respectively, $\partial_x(x)$ and $\partial_y(y)$, which are sequences of i.i.d integer random variables uniformly distributed in the interval $[-\Delta_{\max}, \Delta_{\max}]$, $\Delta_{\max}$, which controls perceptual distortion, is maximum transplant of x-coordinate and y-coordinate.

2.4. Distribution Based on Collusion Probability

Before we fingerprinted multimedia content, we assign the desynchronized content to users according to the users' social network. Those, who are in same community, will get different preprocessed multimedia copies. In order to introduce more blur of colluded image when colluders take part in collusion, we distribute the random geometrically distorted fingerprinted images for users based on the similarity metric between them. The more similar the metrics are, the more chaotic the distortions are. First, users in same community will get different global warped image as Figure2 shows; Second, the more high the metric value, the more chaotic the change of the point-wise relative displacement between the two images.

We use the similarity between nodes to measure the cooperation probability between two members, in graph theory, the members are denoted by nodes. Consider two users i and j, the similarity between them can be calculated by the following equation:

$$S_{ij} = \sum_{k \in N(i) \cap N(j)} \frac{1}{d(k)} \text{ if user } i \text{ and user } j \text{ are connected} \quad (3)$$

where S_{ij} equals to 0, if user i and user j are not connected, $N(i)$ and $N(j)$ are the set of friends of i and j respectively, $N(i) \bigcap N(j)$ are the common friends of users i and j, and $d(k)$ is the degree of node k.

3. Security and Performance Analysis

3.1. Visual Security

The chaotic transformed images are shown in Figure 4(a) and Figure5 (a). The visual quality of transformed images is not degraded obviously, because the perceptual quality of the image can be controlled by the max displacement distance.

3.2. The Security of Distribution

The proposed desynchronization scheme has three main stages: global geometrical transform according to the number of communities, and then followed by the production of different random image grid templates, in the final, random functions are produced according to chaotic map. The image random grid template for each user in multimedia fingerprinting is different. The differences among random grid templates are really chaotic. The transform function warps the pixel in a block at random, in this case, the number of chaotic functions is extremely large. As Table 1 shows that the number of desynchronized copies is large enough to assign each user a different fingerprinted copy. In the end, the warped and fingerprinted images will be distributed based on user's social network, that is, the more close the relationship between users, the more chaotic the warping changes between images corresponding to the users.

Table 1. Desynchronization Operations

Desynchronization Operation	Operation Range	Parameter Space
Global Rotation	-2.5～2.5(degree)	51(step-0.1 degree)
Translation,horizontal	-10～10(pixel)	21(step-1 pixel)
Translation,vertical	-10～10(pixel)	21(step-1 pixel)
Random frame grid	the whole frame	$2^{97(m+1)}$ (step-1 pixel), where m is the patches in the image as Figure 3 shows
Warping for local patch	-2～2(degree)	41(step-0.1 degree)

3.3. Image Registration Analysis

After pirates perform average collusion attack, the low quality of the colluded image will make them realize the desynchronization among the fingerprinted copies. They will try all kinds of methods to resynchronization before they perform the average collusion attack. Although they will find the difference among the fingerprinted copy with exhaustive attack, it will increase the computation overhead, which will decrease the

commercial value. On the other hand, they will produce a colluded image, of which the visual quality will be decreased apparently with the increase of the number of pirates. The experimental results are presented in Figure5.

Resynchronization analysis between warped images, we assume that we have a pair of images: one is denoted by f (x, y), and the other is a distorted image f (d) (x, y) underwent a geometric distortion from f (x, y). We want to characterize the point-wise relative displacement between the two images.

$$F(x,y,t) = F(m_1x + m_2y + m_5, m_3x + m_4y + m_6, t-1) \quad (4)$$

where $F(x,y,t)$ and $F(x,y,t-1)$ represent the original image and the transformed image respectively. To estimate the coefficients, we minimize the following function:

$$E(\vec{m}) = \sum_{x,y \in P} \left[F(x,y,t) - F(m_1x + m_2y + m_5, m_3x + m_4y + m_6, t-1) \right]^2 \quad (5)$$

(a) (b) (c)

Figure 4. Experimental Results: (a), (b), and (c), are Geometrical Transformed Images, Colluded Images Using Average Collusion Attack after Image Register, and Average Colluded Images Respectively

To make the scheme security, a large number of chaotic functions will be produced according to social network analysis and chaotic map. The distorted difference is chaotic because of the chaotic transform can be performed *K* rounds with a set of variable grid templates, in the end, the pirates have to process a brute-force search the desynchronization among the different fingerprinted images. The colluded images are shown in Figure4 (b). Even if the pirates use image registration to undo the desynchronization, the visual quality of these colluded images does not show apparently visual metric improvement compared to those images which do not undo the desynchronization. Because the image desynchronization is chaotic, the computational cost of image register will be very large.

3.4. Robustness

The visual quality of the average colluded images is shown in Figure5, where the warped image, colluded image with two fingerprinted copies, and colluded images with four fingerprinted copies are shown from left to right. According to the visual metric, we know that the proposed chaotic desynchronization is very effective to deter average collusion attack.

(a) (b) (c)

Figure 5. Average Colluded Images: (a), (b), and (c), are Warped Lena, Average Colluded Lena with 2, and 4 Copies Respectively

Digital fingerprinting can be used to identify devices which use multimedia copy for illegal purposes. An owner of digital work, who sells the work, wishes to protect his/her copyright and discourage illegal redistribution of his/her products. To this end, he uses watermarking technology to embed a unique ID number to every copy of the original before it is delivered.

We assume the total number of devices (or devices) in multimedia fingerprinting system is M. For the digital media represented by a vector X, and for every device who want to receive the content, the owner generates a sole fingerprint for the device. The fingerprint is embedded into digital media. The watermarked media is delivered to the device. This makes each copy unique and therefore if a dishonest device illegally redistributes his copy, he can be unambiguously identified by traitor tracing scheme. Digital fingerprinting system could realize traitor tracing as Figure4 shows. Once a pirated copy is detected, the owner extracts the fingerprint of the pirated copy and carries out traitor tracing algorithms to identify the colluders.

4. Conclusion

In this paper, we have presented a novel chaotic desynchronized content distribution scheme based on social network analysis. The method can be applied to large fingerprinting system, and the experimental results show that it can resist average collusion attack. The desynchronization scheme shows good performance even if the pirates try to resynchronization the desynchronized image. Therefore, the proposed chaotic scheme can be used for content protection in the multimedia social network.

Acknowledgements

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] C. Liu, H. Ling, F. Zou, L. Yan, Y. Wang, H. Feng and X. Ou, "Kernelized Neighborhood Preserving Hashing for Social-Network-Oriented Digital Fingerprints, Information Forensics and Security", IEEE Transactions on, vol. 9, **(2014)**, pp. 2232-2247.
[2] T. Bianchi, A. Piva and D. Shullani, "Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding", EURASIP Journal on Information Security, vol. 2015, **(2015)**, pp. 1-17.
[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data", IEEE Transactions on Information Theory, vol. 44, **(1998)**, pp. 1897-1905.
[4] B. Czaplewski and R. Rykaczewski, "Matrix-based robust joint fingerprinting and decryption method for multicast distribution of multimedia", Signal Processing, vol. 111, **(2015)**, pp. 150-164.
[5] B. H. Cha and S. I. Choi, "Continuous media fingerprinting against time-varying collusion attacks", Information Sciences, vol. 298, **(2015)**, pp. 66-79.
[6] H. Feng, H. Ling, F. Zou, W. Yan, M. Sarem and Z. Lu, "A collusion attack optimization framework toward spread-spectrum fingerprinting", Applied Soft Computing, vol. 13, **(2013)**, pp. 3482-3493.
[7] Z. X. Liu, S. G. Lian, Y. Dong and H. L. Wang, "IEEE, Desynchronized Image Fingerprint for Large Scale Distribution", in: 2008 15th Ieee International Conference on Image Processing, IEEE, New York, vols. 1-5, **(2008)**, pp. 409-412.
[8] K. S. Qiang, Z. J. Yu, W. Y. Jing, J. Bin, L. C. Feng and G. H. 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. 109-115.
[9] M. U. Celik, G. Sharma and A. M. Tekalp, "Collusion-resilient fingerprinting by random pre-warping", IEEE Signal Processing Letters, vol. 11, **(2004)**, pp. 831-835.
[10] Z. X. Liu, S. G. Lian and Z. Ren, "Image desynchronization for secure collusion-resilient fingerprint in compression domain", in: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.) Advances in Multimedia Information Processing - PCM 2006, Proceedings, **(2006)**, pp. 56-63.
[11] C. Ye, J. Li and 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.
[12] C. Ye, Z. Xiong, Y. Ding, G. Wang, J. Li and 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.
[13] 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.
[14] A. Qureshi, D. Megías and H. R. Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems", Expert Systems with Applications, vol. 42, **(2015)**, pp. 1391-1408.
[15] H. Shen, X. Cheng, K. Cai and M. B. Hu, "Detect overlapping and hierarchical community structure in networks", Physica A: Statistical Mechanics and its Applications, vol. 388, **(2009)**, pp. 1706-1712.
[16] C. Ye, H. Ling, F. Zou and Z. Lu, "A new fingerprinting scheme using social network analysis for majority attack", Telecommunication Systems, vol. 54, **(2013)**, pp. 315-331.
[17] M. Kutter and F.A.P. Petitcolas, "A fair benchmark for image watermarking systems", Electronic Imaging, vol. 3657, **(1999)**, pp. 87-90.

Authors

Conghuan Ye, 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.

Dr. Ye has co-authored over 50 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, 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, 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, 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, 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, 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.