International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.147-156
http://dx.doi.org/10.14257/ijsia.2016.10.5.14

A New Collusion Attack Using Interpolation for Multimedia Fingerprinting

Conghuan Ye, Zenggang Xiong*, Yaoming Ding, Xuemin Zhang, Guangwei Wang, Fang Xu

Hubei Engineering University, School of Computer and Information Science, Xiaogan, Hubei, China
jkxxzg@163.com

Abstract

Digital fingerprinting is a special digital watermarking technology that can deter legal user to redistribute multimedia content to others. With traitor tracing, it can detect illegal users who use multimedia content illegally. However, collusion attack can avoid some illegal users being detected. With different fingerprinted copies, collusion attack can produce a new colluded fingerprinted copy for get rid of the fingerprint information from the colluded copy, so digital fingerprinting technique should deter collusion attacks. In order to improve the performance of new digital fingerprinting technique in future, this paper presents a new collusion attack approach based on interpolation. The proposed interpolation collusion attack scheme comes from the idea of image fusion. The experimental results demonstrate that the proposed interpolation collusion attack method outperform average attack and maximum attack.

Keywords*: multimedia fingerprinting; interpolation collusion attack; average collusion attack; maximum attack*

1. Introduction

With the rapid development of multimedia communication technology and cloud computing technology recently, multimedia content sharing is becoming more and more convenient. Prevail of smart phone make it very easy to access multimedia content. User with smart phone can share multimedia content anytime and anywhere. The ease of multimedia content sharing will cause illegal misuse which will bring threat of security and privacy. Concerned about the threat of security and privacy, multimedia owners protect their content from illegal use with some multimedia security techniques such as digital watermarking, copy detection, copyright authentication, and digital fingerprinting [1], multimedia encryption.[1]

Both digital watermarking and copy detection are a useful technique for multimedia copyright authentication with information hiding method. It is necessary for digital watermarking to embed copyright information into original multimedia content; on the contrary, copy detection can authenticate multimedia copyright with content feature comparison. Digital watermarking and copy detection should robust to attack [2], however, neither digital watermarking nor copy detection can track illegal users that distribute multimedia content to other users again. In this case, tracing should be applied to deter redistribution, as a special application of digital watermarking; digital fingerprinting can provide tracing [3].

Digital fingerprinting system assigns unique fingerprint information for every user; the fingerprint information is embedded into multimedia content before the multimedia content is distributed to the corresponding user. If the suspicious multimedia content is

Zenggang Xiong is the corresponding author.

ISSN: 1738-9976 IJSIA

detected, the fingerprint information is extracted from the fingerprinted content. The fingerprint information will be used to trace those who redistribute fingerprinted multimedia content to others. Digital fingerprinting is different from digital watermarking, where fingerprints are not same, but watermarks are same for all users. Unique fingerprint for every user can provide tracing.

Although digital fingerprinting can guarantee tracing, the pirates who want to redistribute multimedia content to others will take a way to escape from tracing. Collusion attack is often used to avoid to be detected, and the method for collusion attack is very simple, where only if serval pirates combine their fingerprinted copies to produce a new colluded copy, fingerprint information in the colluded copy may be removed. Collusion attack is very effective to attack digital fingerprinting system. In [4], Kiyavash *et al*. proved that order statistic collusion attack can maximize the error probability for Gaussian fingerprints. Moreover, the average collusion attack is a perfect attack because the colluded copy has good visual quality, and the fingerprint information may be attenuated. Zhao *et al*. [5] verified the visual quality of the colluded copy when non-linear collusion attacks and linear collusion attacks are performed. Results demonstrated that several non-linear collusion attacks can be modeled with average collusion attack superposing Gaussian noise.

Collusion attack is a serious security threat to digital system, therefore, it is very important to research some new collusion attacks, and then the digital fingerprinting system can design robust digital fingerprinting technique to deter all kinds of collusion attack. In this paper, we propose a new collusion attack approach based on image interpolation. Section 2 reviews the key technologies of fingerprinting system. The proposed interpolation collusion attack approach is introduced in section 3. In section 4, we highlight the simulation results. The conclusion is given in section 5.

2. Fingerprinting System

2.1. Framework of Digital Fingerprinting

To protect proprietary rights, digital watermarking technique is used to embed watermarks into the digital multimedia content. For getting proper watermark information, digital watermarking should resist signal processing attack and noise attack. As a major application of digital watermarking, digital fingerprinting technique embeds fingerprint information into multimedia content with digital watermarking scheme. Although they can be used to authenticate copyright, digital can realize traitor tracing further. Different from digital watermarking, digital fingerprinting embeds a unique fingerprint information, that marks the identity of the corresponding user, into multimedia copy. When a similar multimedia copy is detected later, the fingerprint will be detect to decide who is the traitor. The whole fingerprinting process is as follows. An owner of multimedia, who sells the work, wishes to protect his/her copyright and deter illegal use of his/her content. He/She will embed a unique fingerprint to each multimedia copy with watermarking technology to produce a fingerprinted copy, and then distribute the fingerprinted copy to related user [6-8].

In this paper, we assume the total number of subscribers is M. There are K colluders in the multimedia fingerprinting system. We use a vector X to represent the digital multimedia content that will be protected. For a subscriber u^i, the owner of multimedia assigns a unique fingerprint W^i to a subscriber u^i. The mark of the fingerprint codeword W^i is embedded into digital content. The fingerprinted content, which is transmitted to u^i, is

$$Y^i = X + \alpha \cdot W^i \tag{1}$$

Y^i denotes the fingerprinted content related to subscriber u^i. α is a scale factor which is used to control the strength of fingerprint information. The unique fingerprint make every fingerprinted copy is different from each other, and the identify information is hidden in the fingerprinted copy, namely, the fingerprint can be used to identified traitor.

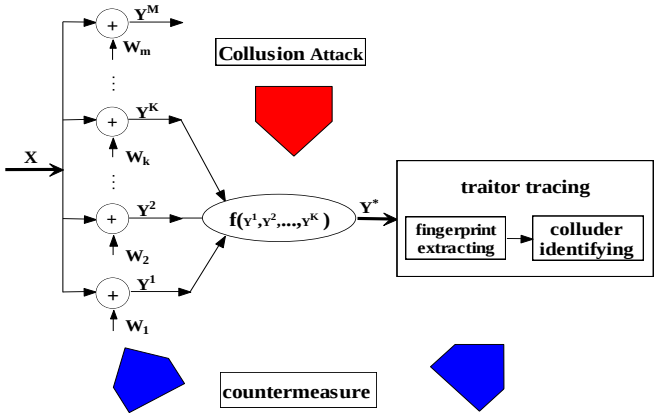

Figure 1. Digital Fingerprinting System

Multimedia fingerprinting system can trace pirates as it is shown in Fig.1. If a similar copy is found in multimedia public network, the owner will take measures to authenticate whether the similar copy is a redistributed copy or not. Then the detector will be used to extract mark information to verify who the traitor is. However, just as shown in Fig.1, several pirates will combine their own fingerprinted copies to generate a new colluded copy. They wish there is little fingerprint information in the colluded copy, then they may escape from being caught.

2.2. Common Collusion Attacks

It is very common that the multimedia content is redistributed in multimedia public network illegally, and the redistribution has bring heavy security and privacy problems. Digital fingerprinting is known to a potential technique to solve the redistribution problem, because it can provide tracing.

But the existing fingerprinting scheme can not resist all kinds of collusion attacks at all, where some pirates would combine their fingerprinted copies to produce a new colluded copy. Fingerprint information in the colluded copy would be attenuated, which will result in the detector can not catch a right pirate with high probability. A fingerprinting system is robust only if it can resist all kinds of collusion attacks. The colluded copy is generated by two kinds of methods, one is the non-linear collusion attack, with which the colluded copy is produced randomly when the pirates combine their fingerprinted copies. There is no rule to generate the new colluded copy. And another is linear collusion attack, where pirates generate a new colluded copy through combining the K fingerprinted copies linearly. Linear collusion attack is a very popular collusion attack, where every pirate will take the same profit and risk. Nonlinear attack includes all kinds of collusion attacks which are not linear attack. For example, the minimum collusion attack, the maximum collusion attack, the mid-value collusion attack, and the gradient collusion attack are non-linear collusion attacks.

Some common collusion attacks will be introduced in the following, in order to model new collusion attack, the fingerprinted copy is divided into $M \times N$ units, and each unit is a block of the original fingerprinted copy. For simplicity, the collusion attack model is just as shown in Fig.1, where every unit is used to produce a new colluded unit by K

pirates, therefore, the uniform collusion attack model can be denoted as the following equation.

$$\begin{cases} Y_{ij}^{C} = \sum_{m=1}^{K} \lambda_{ij}(m) \cdot Y_{ij}(m) \\ \sum_{m=1}^{K} \lambda_{ij}(m) = 1 \end{cases} \quad (2)$$

where the unit of block (i, j) is represented by $Y_{ij}(m)$, which is the signal of the m-th pirate's fingerprinted copy, and $\lambda_{ij}(m)$ is the calculation factor of it, and the three-dimensional matrix λ which is composed of $\lambda_{ij}(m)$ is denoted as calculation factors matrix. At last, a sequence m_1, m_2, … , m_k is used to denote the indices of pirates, which is an ascending sequence with order of $Y_{ij}(m)$, $m = 1, 2, ..., K$. We directly have $Y_{ij}(m_1)$ < $Y_{ij}(m_2)$ < … < $Y_{ij}(m_k)$.

It can be observed that all kinds of collusion attacks including linear and most of non-linear collusion attacks can be represented with the given model, and any single collusion attack is just a special instance of this model. A new collusion attack can be obtained when the calculation factors matrix is changed. There, we can create average attack, minimum attack, maximum attack, and median attack which are denoted by S_1, S_2, S_3, and S_4 respectively according to equation (3).

$$\begin{aligned} S_1 &= \{\lambda_{ij}(m) = 1/K, m = 1, 2, ..., K\} \\ S_2 &= \{\lambda_{ij}(m = m_1) = 1, \lambda_{ij}(m \neq m_1) = 0\} \\ S_3 &= \{\lambda_{ij}(m = m_K) = 1, \lambda_{ij}(m \neq m_K) = 0\} \\ S_4 &= \{\lambda_{ij}(m = m_{(K+1)/2}) = 1, \lambda_{ij}(m \neq m_{(K+1)/2}) = 0\} \end{aligned} \quad (3)$$

2.3. Traitor Tracing and PerformanceCcriteria

Both of blind detection and non-blind detection can be used to extract the fingerprint information from the fingerprinted copy in multimedia fingerprinting systems. For non-blind detection, we assume the original multimedia content is X, and it is available to detect the fingerprint information from the from the forgery copy Y^* to get the extracted vector C. The real fingerprint vector W_m in the extracted vector C can be identify by correlation statistics analysis. In this paper, we consider T statistic of

$$T_m = \frac{\langle \mathbf{C}, \mathbf{W}_m \rangle}{\sqrt{\|\mathbf{W}_m\|^2}} = \frac{\sum_{i=1}^{N} C(i) W_m(i)}{\sqrt{\|\mathbf{W}_m\|^2}} \quad (4)$$

Without loss of generality, we assume that the fingerprint vector extracted from the forgy copy follow i.i.d. common Gaussian distribution with variance of σ and mean 0. The detector determines the colluder according to the threshold value h as the equation (5) shows.

$$H_0 : T_m < h, \quad H_1 : T_m \geq h. \quad (5)$$

where H_0 and H_1 are the two kinds of assumption which represent innocent users and colluders respectively. In this paper, we use the detector to trace at least one pirate, so

the legal user would be detected with low probability. The pirate that redistributes the fingerprinted copy to other users is determined by equation (6)

$$User_m = \arg\max_{m\in[1,2,...,M]} T_m \tag{6}$$

The effectiveness of the collusion attack and the performance of the detector could be evaluated by two kinds of main performance criteria: P_d denotes the probability that at least a real pirate is traced, and P_{fp} is the probability which a legal user is caught. In our evaluation, the performance criteria is the probability, denoted with P_d, of successfully catching at least one colluder based on maximum correlation detector as equation (6) shows. Equation (7) shows the success probability of catching at least one colluder, on the contrary, equation (8) determines the probability of falsely accusing one innocent user.

$$P_d = P\{\max_{m\in S_c} T_m > h\}) \tag{7}$$

$$P_{fp} = P\{\max_{m\notin S_c} T_m > h\} \tag{8}$$

3. Collusion Attack based on Interpolation

3.1. Interpolation

Image interpolation is equivalent to methods of constructing a new image from a corresponding original image sequence. The interpolation using with multiple images, which usually involves in resampling process, will result in a high-resolution image. The resolution of image is increased by expanding original images produced by low-resolution devices. Image interpolation can be applied in the areas including: (1) super resolution, and (2) image compression, (3) image display, and (4) computer graphics and (5) reversible watermarking. Common interpolative techniques are the spline interpolation, the linear image interpolation and the cubic image interpolation, these common image interpolations have low time complexity and produce image with moderate visual quality. However, the fidelity must be kept according to the human visual system (HVS) which could forgive small estimation errors from reasonable linear, spatial domain filters.

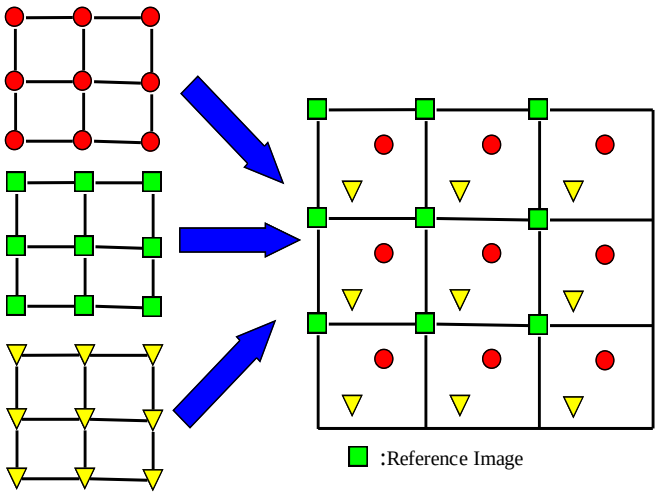

Figure 2. Collusion Framework based on Interpolation

Image interpolation is also regarded as the problem of fitting discrete data samples with a continuously specific model. In order to fit the data correctly, the model must be defined. The possibility of fulfilling this objective lies in the belief that missing information in the new signal is highly correlated with that in the original images. In this case, the relationship between estimated data information and adopted interpolation is inseparably. According to the types of images to be interpolated, the interpolation techniques could be generally grouped into three categories: single image frame interpolation, multi frame image interpolation and video frames interpolation. In this paper, we focus on the multi frame image interpolation according the collusion attack model. Usually, the multi frame image interpolation using some low-resolution image frames can restructure a new image which includes more details.

The single frame image interpolation deals only with the spatial information of the original low-resolution image. The multi frame image interpolation technique can produce a high-resolution image with a number of similar images that have the same scene with different motion blur and noises to reproduce a new image with the same scene. Similarly the video frames interpolation could estimate both the miss spatial and temporal information to produce high-resolution image frame. Inspired by these image interpolation methods, we present a new collusion attack using image interpolation with multiple images.

3.2. Collusion Attack using Image Interpolation

In order to disturb fingerprints information of the fingerprinted image without degrade the metric of fingerprinted image, By expanding the difference between the two neighboring pixels of pixel pairs multiple fingerprinted images could be fused based on multiple image frame interpolation. This approach is from relation of colluded fingerprints detected with original individual fingerprints in fingerprints database. The process is shown in Fig. 2.

In Fig.2, there are three fingerprinted images which are used to collude to get a new colluded image by three colluders. One of the original fingerprinted images is regarded as a reference image colored in green. This new collusion algorithm is different from the previous collusion methods such as average attack, minimum attack, maximum attack, and median attack. The process of image interpolation aims at disturbing the dependence of pixels in original fingerprinted images. So estimating pixels from non-reference images which have much difference from the original known pixel in reference image would take the place of the latter, and let its neighbors remain unchanged.

4. Experimental Results

In this section, we evaluate the effect of the proposed collusion attack based on image interpolation. A set of collusion attack experiments are conducted, and the performance of the proposed collusion attack is analyzed. In order to verify the performance, orthogonal fingerprint code which has 10^4 fingerprint codewords is used to accommodate 10^4 users. We use spread-spectrum method to embed the fingerprint codeword into test images, then we select several fingerprinted images to produce colluded images with maximum collusion attack, average collusion attack, and the proposed interpolation collusion attack.

Fig. 3 shows the experimental results of the probability of at least one pirate detected. The success probabilities against average attack and maximum attack are 1 when the number of pirates is less than 6, while the probability is about 0.72 with only two fingerprinted copies. With the increase of coalition size, the success rate of the proposed approach decreases more rapidly than those of the other two attacks. We can also observe that collusion of less than four marked copies can sufficiently disturb the fingerprints of all the colluders.

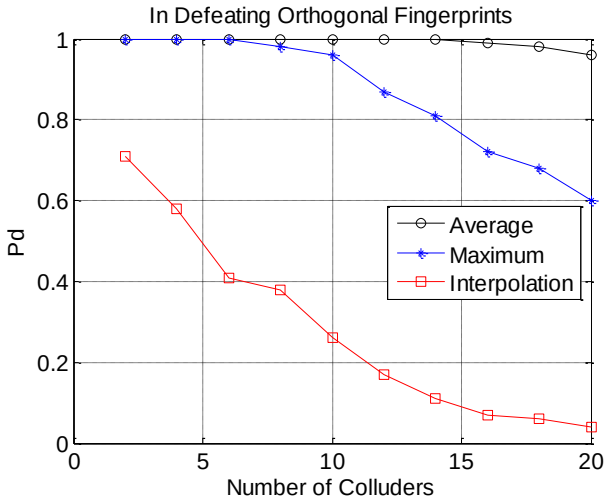

Fig.3 Performance Comparison of the Proposed Interpolation Collusion Attack, the Maximum Collusion Attack , and Average Collusion Attack, in Terms of the Success Probability vs. the Number of Pirates

5. Conclusion

Collusion attack is a heavy threat to digital fingerprinting system; however, a robust digital fingerprinting system should resist all kinds of collusion attack. A new interpolation collusion attack is proposed in this paper. The performance of the proposed attack scheme outperforms that of maximum collusion attack and average collusion attack, and the proposed attack scheme can produce a colluded copy with a good perceptual quality. With the proposed interpolation collusion attack scheme, one is able to design a robust digital fingerprinting system.

Acknowledgements

This work is supported by NSF of Hubei Province of China (No.2015CFB236), and Youth innovation team project in Hubei Provincial Department of Education (No.T201410), and NSF of China Grants (61502154, 61370092, 61370223).

References

[1] KANG Shou-qiang, ZHENG Jian-yu, WANG Yu-jing, JI Bin, LAN Chao-feng, GAO 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, 2015,20(4), 109-115.
[2] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," Journal of Visual Communication and Image Representation, vol. 30, pp. 125-135, 2015.
[3] Cox IJ, Kilian J, Leighton FT, Shamoon T, “Secure spread spectrum watermarking for multimedia”, IEEE TRANSACTIONS ON IMAGE PROCESSING. vol: 6 issue: 12 pp: 1673-1687, DEC 1997
[4] N. Kiyavash, and P. Moulin, “A Framework for Optimizing Nonlinear Collusion Attacks on Fingerprinting Systems,” Information Sciences and Systems, 2006 40th Annual Conference on, pp. 1170-1175, 2006
[5] Zhao HV, Wu M, Wang ZJ, *et al.*, “Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting”, IEEE TRANSACTIONS ON IMAGE PROCESSING. vol:14,issue: 5,pp: 646-661, MAY 2005
[6] 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, pp. 658-666, 2014.
[7] 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.

[8] C. Ye, H. Ling, F. Zou, Z. Lu, A new fingerprinting scheme using social network analysis for majority attack, Telecommunication Systems, 54 (2013) 315-331.

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.