Security Scheme for Digital Watermarking

Xiao Jun, Wang Ying, Li Dengyu, Zhang Ying, Zhu Li

School of Engineering Science, University of the Chinese Academy of Sciences

No.19A Yuquan Road, Beijing 100049, China

xiaojun@ucas.ac.cn

Keywords: Digital Watermark; Security Scheme; Cryptography; Side Information

Abstract. Digital watermarking technology is one of the main means to realize the copyright protection and authentication of digital works in the information age, and many excellent watermarking algorithms have been proposed to achieve different performances in different application. But, attackers also can make use of the design fault of these algorithms to realize their illegal purpose, such as embedding without authorization, detecting without authorization or removing without authorization, and the security problem of watermarking system is becoming more and more serious. In this paper, the security problems of digital watermarking algorithms are summarized, the research status of the watermarking security is analyzed, and many typical security schemes are studied, and then a useful scheme based on side information theory and cryptology technique is proposed, including three feasible strategies in different stages of the watermarking system.

Introduction

As it is known to all, fidelity, robustness and capacity are the main performance index of digital watermarking, while the security had always been an aspect of robustness, but in practical use, security is entirely different from robustness. When only robustness is considered, the watermarking algorithm may not ensure the safety of the watermarking system. If the algorithm or the key are leaked, even if only partial information leaked, attackers can obtain part of the watermark information, and this is an imperfect security, even can be considered completely insecure, and in this situation, the watermark will not achieve the desired effect.

With the development of computer and network, digital watermark is becoming more and more widely used, as an important performance, security is becoming more and more important [1-7], and watermarking security worth more research.

In this paper, the existing security strategies for watermarking are studied, and the scheme for improving security is proposed.

Typical strategies for watermark security and its analysis

More and more watermarking algorithms are being proposed, and the security strategies are mainly considered from the following two aspects: the structure of the watermark information and the embedding scheme. Most of the researchers put their main energy on the embedding scheme, such as the Least Significant Bit (LSB) algorithm proposed by Tirkel [8], the Patchwork algorithm proposed by Pitas [9], the Secure Spread Spectrum Watermarking algorithm proposed by Cox [10]. While, the research on the structure of the watermark information mainly focus on the use of scrambling method or cryptographic algorithm, and its objective is to change the watermark information to be a pseudo-random sequence.

1) scheme based on encryption of embedding positions

In 2002, a watermarking method based on chaos theory was proposed [11], then some similar algorithms are proposed [12,13].

For example, Logistic mapping is a usually used scheme, which can be represented using the following formula:

$$x_{k+1} = \mu x_k (1 - x_k) \qquad 0 < \mu \le 4,\ 0 < x < 1 \tag{1}$$

Where, k represents the time, and μ is an adjustable parameter.

In these algorithms, the embedding positions are controlled by a key, and the embedding orders are dislocated, so it is more secure than the common algorithms with fixed embedding positions. When attack occurs, even exhaustive attack occurs, it is difficult to find the accurate embedding positions.

But the encryption process is independent of the embedding process, and the information from the cover and attack are not fully used. What's more, the information of different embedding positions is independent of each other.

2) scheme based on encryption of the watermark content to be embedded

When watermark content is encrypted, two methods can be used: the content is scrambled by some mathematical model, or the content is encrypted by conventional cryptographic algorithms.

(1) scrambling technology based method

Digital image scrambling technology is mainly used for digital image preprocessing and postprocessing, its purpose is to put the original watermark information into a disordered form, and this disorder lays a good foundation for the following encryption or data embedding in watermarking system.

At present, the common digital image scrambling algorithms include Arnold transform, [14,15], Hilbert transform [16], Fibonacci and Fibonacci-Q transform [14], Orthogonal-Latin-Square transform [17], affine transformation [18], etc.

Arnold transformation is also called the cat face transform [14,15], it was proposed by Russian mathematician Vladimir. Arnold when he researched the ergodic theory. The implementation of Arnold transform is simple, since only the matrix is used to transform the coordinates of the original image points, and with the increase of the number of iterations, the image will be confused. But, when a certain number of iterations achieved, which is called the Arnold algorithm cycle, the original image will be restored, and the Arnold algorithm cycle is the key of transform.

Arnold transformation of n dimension can be described as the following formula (2), where L is the size of image, x and x' represent the positions before and after Arnold transformation. In 2007, this method began to be used in watermarking embedding by researchers [19].

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_n' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 2 & \cdots & 2 & 2 \\ 1 & 2 & 3 & \cdots & 3 & 3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2 & 3 & \cdots & n-1 & n-1 \\ 1 & 2 & 3 & \ldots & n-1 & n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \bmod L \tag{2}$$

Hilbert Curve was proposed by a German mathematician in 1981, and its source is the FASS cure proposed by Samile [13]. If search traversal method is used according to the Hilbert cure, and rearrange all the pixel points in accordance with the order of search traversal, a scrambled image will be obtained, which is different from the original image.

In both Fibonacci transformation and Fibonacci-Q transformation, Fibonacci transformation is use to search through all the pixel points of the image. In Fibonacci transformation, the following formula (3) is used, where (x, y) and (x', y') represent the pixel coordinates before and after Fibonacci transformation.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{3}$$

In the orthogonal Latin square transformation [17], the space position of the image is scrambled by using the orthogonal Latin square, and the method also can be used to set the color space.

In affine transformation, the operations of rotation, translation and scaling are applied to the coordinates of the image to get new coordinates, which can be represented as formula (4), where

a, b, c, d, e and f are the transformation parameters.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \quad (4)$$

It is worth mentioning that affine transformation can be repeatedly used to get a better scrambling effect.

In digital watermarking, these scrambling methods are just used to do preprocessing of the watermark information, and the preprocessing result is embedded into the cover image as a whole, then if attack happens, attackers may obtain the whole scrambled watermark information, and this may lead to the recovery of the original watermark information. That is to say, these methods may not be safe enough.

(2) cryptographic algorithm based method

The use of cryptography algorithm to encrypt the content of the watermark information has the same effect as the scrambling technology based method. In cryptographic algorithm based method, cryptographic algorithm is used to encrypt the watermark information to be embedded into the cover image before embedding, such as the algorithms proposed by zhang [7].

These methods also have the same problems with the scrambling technology based methods, the encrypted watermark information will be embedded as new information, and the encryption process has nothing to do with the following embedding process. What's more, it is difficult to verify the overall security of the watermarking algorithm.

If the encryption process can be closely integrated with the watermark embedding process, digital watermarking technology will be integrated in the cryptography technology, then "unseen" and "don't understand" will work together to achieve higher security.

Secure watermarking scheme based on cryptography and side information theory

With the development of watermarking, many researchers found that if the whole process of digital watermarking is considered as a communication with side information [20,21], the theory of side information can be used to improve the performances of watermarking, such as the capacity, fidelity and robustness [21], and we also believe that the security of watermarking system can be effectively improved by making full use of network information theory and cryptography technology during the processes of watermark signal designing, watermark information coding, choosing embedding positions and embedding strength.

(1)Optimization scheme for watermarking preprocessing

During the watermarking preprocessing stage, don't simply disturbing the watermark information by scrambling or encryption, but make sure that the information of the carrier is associated with the watermark information, at the same time, both scrambling technology and encryption technology are used together, then the security must be improved.

(2)Optimization scheme for the watermark embedding position

Now, the embedding positions in watermarking algorithms are mainly depended by considering the balance between the robustness and fidelity.

If we can make the embedding positions associated with the watermark information and the carrier information, and when extracting or detecting the embedded watermark, all the following positions will be incorrect once one position information mistake occurs. This is meaningful for the security of watermarking system, and may lead to a high security level which may be the same as cryptography.

(3)Optimization scheme for security attack

Security attack is far different from the general robustness attack. If we can establish the mathematical models for security attacks according to the characteristics of embedding without authorization, detecting without authorization and removing without authorization, then we can get some useful side information from these attacks, and based on this information, we can get more and more methods and schemes combined with side information theory and cryptography resisting security attacks.

What's more, if all these optimization schemes described above are fully used in one watermarking system at the same time, many security problems can be resolved.

Conclusion

In this paper, the difference between robustness and security is described, and the importance of security is analyzed. Typical strategies for watermarking security are introduced, especially the method based on embedding content and the method based on embedding location. If the watermarking system is considered as a communication system with side information, and the theory of side information and cryptology are fully combined and used, then the watermarking system will be more secure.

Acknowledgement

In this paper, the research was sponsored by the National Natural Science Foundation of China (No. 61471338), the state password development fund (No.MMJJ201401010), President Fund of UCAS, and the Youth Innovation Promotion Association of CAS (2015361).

References

[1]Bianchi, Tiziano,Piva, Alessandro . Secure watermarking for multimedia content protection: A review of its benefits and open issues [J]. IEEE Signal Processing Magazine,2013, 30(2):87-96.

[2]Guo Jianting, Zheng Peijia, Huang Jiwu. Secure watermarking scheme against watermark attacks in the encrypted domain [J]. Journal of Visual Communication and Image Representation. 2015,30:125-135.

[3]Wang, Hong-Yang.A secure image watermarking using visual cryptography and discrete fractional fourier transform [J]. Applied Mechanics and Materials, 2014,577:754-757.

[4]Niu Shaozhang. Survey of digital watermarking security [J]. Journal of southeast university (Natural Science Edition).2007, vol37, sup(1):220-224.

[5]Cayre F, Fontaine C, Furon T. Watermarking security: theory and practice [J]. IEEE Transactions on Signal Processing,2005, 53 (10) : 3976-3987.

[6]Ba rniM, Ba rtolini F, Furon T. A general framework for robust watermarking security [J]. Signal Processing, 2003, 83(10) : 2069-2084.

[7]Zhang Tao, Tang Guangming, Sun Yifeng. Research of the Digital Watermarking Based on Encryption [J]. Computer Engineering and Applications , 2003:36(26):109-111.

[8]Tirkel A, Rankin G, Van Schyndel R, Ho W, Mee N and Osborne C. Electronic Watermark [C]. Proceedings of Digital Image Computing: Techniques and Applications. 1993. 12: 666-672.

[9]Pitas I. A Method for Signature Casting on Digital Images [C]. Proceedings of International Conference on Image Processing. 1996,3: P215-218.

[10]Ingemar J. Cox, Joe Kilian, Talal Shamoon. Secure Spread Spectrum Watermarking for Multimedia [J]. IEEE Trans. on Image Processing. 1997. 6(12):1673-1687.

[11]Weiwei Xiao, Zhen Ji, Xhong Zhang, Weiying Wu. A watermarking algorithm based on chaotic encryption [C]. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. 2002. 545-548.

[12]Zou Xiaoxiang, Li Jintao, Peng Cong. Research on Asymmetric Watermark [J]. Computer Engineering and Applications. 2002. 38(16):7-10

[13]Yang Degang, Chen Yonghong, Yang Huaqian, Wei Pengcheng. Research on Algorithm of

Embedding Muti-watermarking in Digital Image [J]. Computer Engineering and Applications. 2005, 41(21):41-44.

[14]Qi Dongxu, Zhou Jiancheng, Han, Xiaoyou. A new class of scrambling transformation and its application in the image information covering [J]. Science in China (Series E). 2000, 30(5)：440-447.

[15]Ding Wei, Yan Weiqi, Qi Dongxu. Digital image scrambling technology based on Arnold transformation [J]. Journal of computer-aided design & computer graphics. 2000. 13(4):338-341

[16]Lin Xuehui, Cai Lidong. Scrambling research of digital image based on Hilbert cure[J]. Chinese journal of stereology and image analysis. 2004. 9(4):224-227.

[17]Li Guofu. Image Scrambling method based on Orthogonal-Latin-Square[J]. J. North china univ. of tech. 2001. 13(l):14-16.

[18]Zhu Guibin, Cao Changxiu, Hu Zhongyu, He Shibiao, Bai Sheng. An Image Scrambling and Encryption Algorithm Based on Affine Transformation [J]. Journal of computer-aided design & computer graphics. 2003. 15(6): 711-715.

[19]Cheng Xinguo, Wang Xiang, Zeng Rong. Algorithm of Watermarks embedded in DC Components in DCT [J]. he modern electronic technology. 2007,3:57-59.

[20] Ingemar J. Cox, Matt L. Miller, Andrew L. Mckellips. Watermarking as Communications with Side Information [J]. Proceedings of the IEEE. 1999. 87(7): 1127-1141.

[21]Wang Ying, Xiao Jun, Wang Yunhong. Digital watermarking Principles and Techniques [M]. Beijing: Science Press, 2007.