Secure Digital Watermarking Model with Side Information Theory and Cryptography

Xiao Jun, Li Dengyu, Wang Ying

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

No.19A Yuquan Road, Beijing 100049, China

xiaojun@ucas.ac.cn

Keywords: Secure Watermarking Model; Hostile attack; Cryptography; Side information

Abstract. The idea of side information is introduced into secure watermarking, and a secure watermarking model with side information theory and the idea of cryptography is proposed. In the proposed model, the side information from the cover work, the attack and the detector are considered and fully used in both the preprocessing stage and the embedding stage. With the guidance of the proposed model, we also give three security mechanisms resisting typical secure attacks, such as collusion attack, homology detection and copy attack, which belong to unauthorized removal, unauthorized detection and unauthorized embedding. The proposed security mechanisms show that the side information and encryption technology can be used to get good watermarking algorithms with higher security.

Introduction

With the development of computer and network, digital watermarking is becoming more and more widely used, and as an important factor, watermarking security worth more research [1-3]. There have been great achievements for secure watermarking algorithms [4-10] and security assessment models [11-14].

Both assessment model and performance index are very important tools to distinguish different algorithms, and as we know, security is a very special performance index different from robustness, so the assessment model for security is a research hotspot [11-13]. The analysis methods of watermarking security can be divided to three classes [14]: analysis method based on information theory proposed by Shanoon, analysis method based on Fisher information matrix and analysis method based on computation complexity.

In most of the existing secure watermarking algorithms, cryptography or scrambling is used, and these algorithms can be attributed to two categories, where one is encrypting the embedding positions [4, 5], and the other is encrypting the watermark [6-10]. In the algorithms with the scheme of encrypting the embedding positions, 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, 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. While in the algorithms with the scheme of encrypting the watermark content, two methods can be used: the content is scrambled by some mathematical model, or the content is encrypted by conventional cryptographic algorithms. In these algorithms, 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.

Besides, many other research works about the security of watermarking have been done by many researchers [17-22]. A watermarking preprocessing scheme of digital image aiming at the watermarking security was proposed in 2004 [17], in which, through chaotic map, random matrices are padded out with chaotic sequences, and the random matrices are turned into orthogonal matrices which are considered as transformed kerne1, and then a method is devised to satisfy Kerckhoffs

principle in cryptography，hence，it can enhance the security of the watermarking system．A new secure watermarking protocol based on digital signature was proposed through discussing about the attack over watermarking and the security leak of DHWM protocol in 2006 [18], this new protocol imports certificate，and embeds signature，timestamp，watermarking information into digital image, and can resist the middle-man attack and the interpreting attack.

But it's a pity that there are few models for secure watermarking used to guide the designing of secure watermarking algorithms, and we think this is one of the reasons that the security of digital watermarking system needs to be further promoted.

Some researchers have shown that side information theory can be used to improve the security of the watermarking system [20-22], but the proposed algorithms are just individual algorithms, haven't become a system, and so it is not enough.

In this paper, both side information theory and cryptography will be used for enhancing the watermarking security, and a preliminary secure watermarking model will be proposed, the side information from the cover work, the attack and the detector will be made full use of when the watermark is preprocessed, and also when the embedding positions and strength are selected.

Secure watermarking model with side information and encryption

Side-informed watermarking is developed under the elicitation of Costa's dirty paper model [15]. In side-informed watermarking, the correlation between the watermark and the cover work is used to improve the performances, and the watermark embedding process can be described as Fig.1, where m represents the watermark, Co represents the cover work, and Cw represents the watermarked cover work.

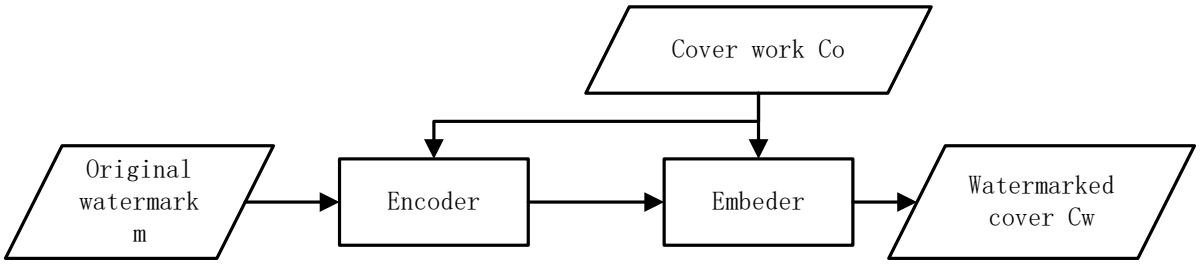

Fig. 1. Watermark embedding process of regular side-informed watermarking

In 1999, Cox and others considered watermark as communications with side information [16]. Now, the advantages of watermarking system with side information are accepted by more and more people [1]. But side information is seldom used in the researches of watermarking security.

In this section we will give a preliminary secure watermarking model with side information and encryption, as shown in Fig.2.

According to Fig.2, in the proposed model, encryption is used in both the pre-processing stage and the embedding stage, and the side information is also used in both stages, which can be obtained from the cover, the attacker and the detector. So we can say that this model makes full use of the idea of side-informed communication, where side information may be the correlation between the cover work and the watermark, and also the side information may be extracted from the attack or the detector.

In this model, we divide all the processes into three layers:

(1) the first layer is the information layer, and all the data and operations before embedding are in this layer;

(2) the second layer is the operation layer, in which the watermark information after pre-processing is embedded into the cover work;

(3) the third layer is the transmission layer, in which the watermarked cover work is transmitted to the receiver, and in this layer the watermark may be attacked maliciously.

According to the proposed model and the defined layers above, we can describe all the transfer

process of the watermark information with the following steps.

Step one, the original watermark information is preprocessed in the information layer (the first layer), which includes coding, encrypting and other operations, such as error correction encoding which can be used to reduce and correct the possible errors in the follow up transmission processes, the encrypting or the scrambling which can be used to further improve the security of the watermarking system. It is worth noting that the side information from the cover, the attack and the detector will be made full use to associate all the information, and thus improve the security.

Step two, the preprocessed watermark information is embedded into the cover work in the operation layer. In this step, also the side information from the cover, the attack and the detector will be made full use to get good performances such as the capacity, robustness, fidelity and security. For example, encryption technology can be used to encrypt the embedding positions with the side information from the cover work, the algorithm will be more robust when the side information from the cover work and the attack is fully used to choose the embedding positions, and the fidelity of the watermarked work will be better if the side information from the cover work is fully used.

Step three, the watermark after preprocessing and embedding will be transmitted to the receiver in the transmission layer (the third layer), and the attacks usually happen in this layer, such as filtering, compression, copy attack and other operations which include both the regular operations and hostile attacks.

When the receiver receives the watermarked and attacked cover, the watermark information will be detected, decrypted and decoded, which is the reverse process of the steps described above.

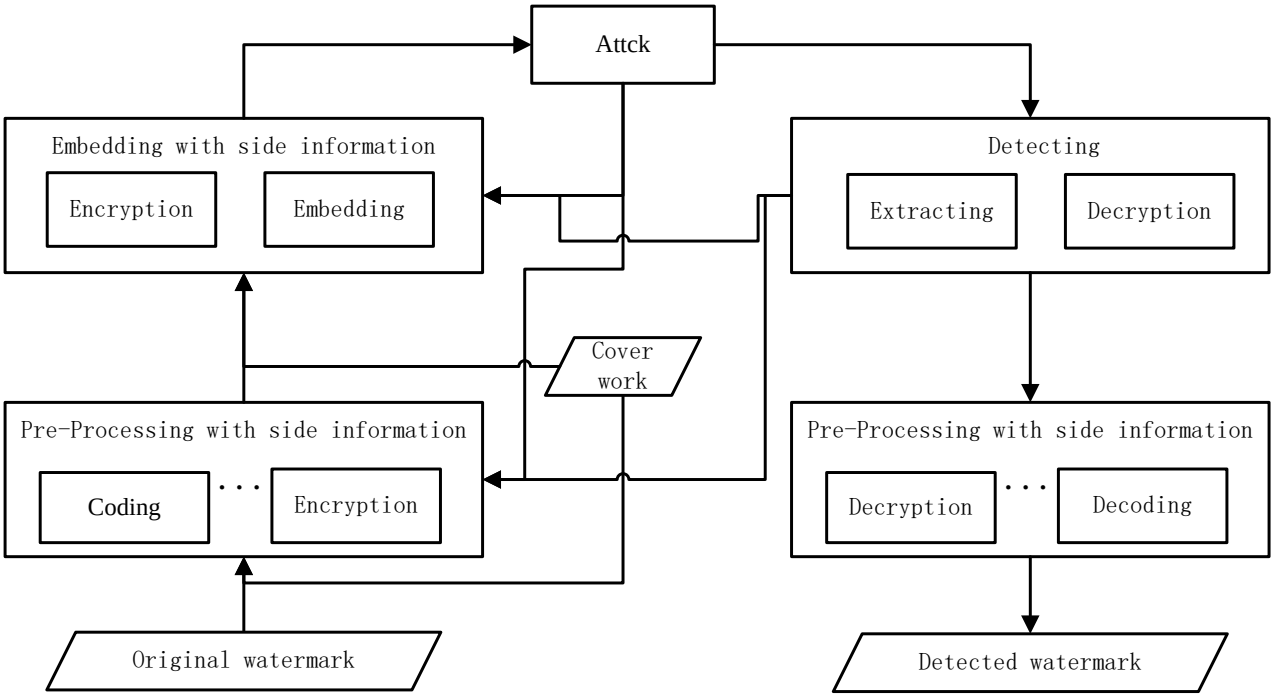

Fig.2. Preliminary secure watermarking model

Security mechanisms can be used in the secure watermarking model

There are many secure attacks, most of them can be divided into three classes, they are unauthorized removal, unauthorized detection and unauthorized embedding, but many attack methods can be used to realize the above attack effect. In this paper, we will give some mechanisms which can be used in the secure watermarking model resisting the typical secure attacks.

(1) security mechanisms against collusion attack

Collusion attack is a typical realizing manner of unauthorized removal. When collusion attack occurs, if the attacker can obtain many copies of the same cover, but with different watermark information, the attacker can get the average value of all the copies by adding all the copies together, and then the watermark is removed from the cover, while the attacker obtains the approximate version of the cover work. For the collusion attack, a study shows that when the copy is more than

ten, the obtained cover is almost the same as the original cover.

We found that, double watermark can be used to resist this collusion attack, that is to say, and if two watermarks (public watermarking and private watermarking) are embedded, the public watermark is used to identify the information of the cover work itself, while the private watermark is used to identify the owner or the resource of the cover work. For example, we can extracted the features of the cover work as the public watermark, and this is also can be called the side information, then we divide the cover into different sub-block, and at last the public watermark is embedded into some fixed sub-blocks, while the private watermark is embedded into the other blocks .

The public watermark is used to tell us that the cover work contains watermark, it can be distinguished from the cover work without watermark, and so the embedding algorithm should be very robust, while the private watermark can be embedded by robust algorithm or fragile algorithm.

For the same cover work, the public watermark is the same, as well as the embedding positions, so the watermark can be detected even after collusion attack, and only the private watermark is removed, and then the detector can give a warning message that “unauthorized removal happened”.

(2) security mechanisms against homology detection and copy attack

Copy attack can be used to realize unauthorized embedding, but encryption mechanism can solve this problem. In order to resisting copy attack, another key must be introduced into the cipher algorithm except the basic private key, and it is called the public key which is extracted from the cover, so this also can be called side information. When encryption, both the private key and the public key are used to encrypt the watermark information in the information layer, and thus the encrypted watermark information is related to the cover work. When copy attack happens, the watermark can’t be decrypted correctly.

It is noteworthy that only two methods can be used when encryption: the private key is used after the public key, or a new key is used which is obtained by some computing operations using both the private key and the public key.

In particular, this security mechanism also can be to resist the homology detection attack which belongs to the unauthorized detection.

(3) encryption in the operation layer

The above mechanisms can be used to resist some typical secure attacks described above, but in practical use, many attacks may be used at the same time, so if the encryption can be also used in the operation layer, the security will be further improved. For example, the embedding positions and the embedding strength can be encrypted according to the feature of the cover work.

If the optional positions can be used to embed the watermark is n, the length of the watermark to be embedded is $m(m \le n)$, when brute force occurs, the total probability P can be described as

$$P = C_n^m \times m! \tag{1}$$

According to formula (1), if m is big enough, it will be very difficult to break it, and the watermarking system will be more secure.

Conclusion

In this paper, a novel but preliminary secure watermarking model with side information and cryptography is proposed based on Shanoon information theory and encryption technology. The proposed model makes full use of the idea of side-informed communication, and all the possible side information from the cover, the attack and the detector are included. Based on the proposed model, some security mechanisms resisting secure attacks such as unauthorized removal, unauthorized detection and unauthorized embedding are also presented to explain the application of the model and demonstrate the proposed model. With this model, many watermarking algorithms with higher security can be designed, and this will be the future work.

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]Ying Wang, Jun Xiao, and Yun-hong Wang, Digital Watermarking Principles and Techniques [M]. Science Press, Beijing, 2007.

[2] Cayre, Francois, Fontaine, Caroline, and Furon, Teddy, Watermarking security: Theory and practice [J]. IEEE Transcations on Signal Processing, 2005, 53(10):3976-3987.

[3]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.

[4] 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.

[5] Liu Peipei, Zhu Zhongliang, Wang Hongxia, Yan Tianyun. A novel image fragile watermarking algorithm based on chaotic map[C]. Proceedings of 2008 International Congress on Image and Signal Processing, 2008, 5:631-634.

[6] Zhao Ruimei, Lian Hua, Pang Huawei, Hu Boning. Digital image watermarking algorithm with double encryption by Arnold transform and logistic[C]. Proceedings-4th International Conference on Networked Computing and Advanced Information Management, 2008,1: 329-334.

[7] Ye Ruisong, Li Huiliang. A novel image scrambling and watermarking scheme based on cellular automata[C], Proceedings of the International Symposium on Electronic Commerce and Security, 2008: 938-941.

[8] SA Craver, S Katzenbeisser. Security analysis of public-key watermarking schemes[C]. Mathematics of Data/Image Coding, Compression, and Encryption IV, with Applications, July 2001, San Diego, Calif, USA, Proceedings of SPIE 4475, 172–182.

[9] Xie Rongsheng, Wu Keshou, Du Jiangbo, Li Chunguang. Survey of public key digital watermarking systems [C]. Proceedings-SNPD 2007:Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007, 2:439-443.

[10] Picard J., Robert A., On the public key watermarking issue[C]. Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008: 1344-1347.

[11] T. Mittelholze. An information-theoretic approach to steganography and watermarking [C]. Lecture Notes in Computer Science. 1999, 1768: 1-17.

[12]Pedro Comesaña, Luis Pérez-Freire, Fernando Pérez-González. Fundamentals of data hiding security and their application to spread-spectrum analysis [C]. Lecture Notes in Computer Science. 2005, 3727: 146-160.

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

[14]Niu Shaozhang. Survey of digital watermarking security [J]. Journal of southeast university

(Natural Science Edition).2007, vol37, sup(1):220-224.

[15]Costa, M.. Writing on Dirty Paper [J]. IEEE Transactions on Information Theory.1983, 29(3), 439-441.

[16]Cox I J, Miller M L, and Mckellips A L, Watermarking as Communications with Side Information [J], Proceedings of the IEEE, 1999,87(7): 1127-1141.

[17]Feng Guori, Jiang Lingge, He Chen. An Effectively Preprocessing Method to Enhance the Security of I mage Watermarking System [J]. Journal of shanghai jiaotong university. 2004, 38(9):1505-1508

[18]Xiao Jing, Li Jianhua. A Secure Watermarking Protocol Based on Digital Signature[J]. Computer Engineering and Applications. 2006, 39(16):160-162.

[19]He Hongjie, Chen Fan. On the Security of the Self-Embedding Watermarking Scheme[J]. Acta electronica sinica. 2007,35(3):557-562.

[20]Ying Zhang, Jun Xiao, Ying Wang. Side informed image watermarking algorithm with high security [C]. Proceedings of 2009 IEEE Youth Conference on Information, Computing and Telecommunication，2009: 395-398.

[21]Ying Zhang, Jun Xiao, Ying Wang and Yan Yan.dd. Secure Fragile Watermarking Algorithm with Side Information [C]. Proceedings of 2nd International Symposium on Information Processing. 2009:41-44.

[22]Dengyu Li, Jun Xiao, Ying Wang, Li Zhu. A Secure Watermarking Algorithm Resisting Copy Attack based on Information Layer Encryption [C]. The 2015 5th International Conference on Information Engineering for Mechanics and Materials. Huhhot, Inner Mongolia, July 25-26, 2015，950-955.