A Secure Watermarking Algorithm Resisting Copy Attack based on Information Layer Encryption

Dengyu LI, Jun XIAO , Ying WANG, Li Zhu

College of Engineering & Information Technology, University of Chinese Academy of Sciences, BeiJing, 100049 ,China

email: xiaojun@ucas.ac.cn

Keywords: Digital Watermark; Copy Attack; DES Encryption; Image Feature

Abstract. Among various attacks against watermarking security, copy attack can embezzle other people's copyright information, which brings challenge to copyright protection of digital works. In this paper, a new watermarking algorithm based on information layer encryption is proposed. This algorithm uses two keys to encrypt the original watermark. One key called public-key is generated by image feature, and the other called private-key is offered by user. This strategy ensures that if the watermark is copy to other carriers, the watermark detector will not decrypt it correctly. The experimental result shows that this algorithm can not only protect the watermark information from leakage, but also resist copy attack.

Introduction

With the rapid development of internet, digital works' copyright protection is facing more and more serious problem, and digital watermarking technology is born to solve digital copyright protection and authentication [1-3]. But adversary can use watermark copy attack [4] [5] to embezzle other people's copyright information by insert other's watermark into his own works. The validity of watermarking algorithm when facing with copy attack has become the bottleneck of its usage.

At present, the main idea of solving copy attack is using digital signature. In Ref [6], the digital signature is obtained based on independent component analysis, and is embedded to the host image as watermark. In Ref [7], the feature describing the original image uniquely is attained from the chroma component of the original color image, and is embedded into the luminance components of the host color image. Although these two methods can resist copy attack, the watermark embedded doesn't have copyright information. In Ref [8], both the image signature and the watermark are embedded into the original image synchronously, so the fidelity isn't high. In Ref [9], the scheme mainly relies on the deployment of content-dependent watermarks, where each is a combination of an informative watermark and a robust hash. In general, the security of the algorithms already exist is not high, and the payload of the watermark embedded is low.

In this paper, a new secure watermark scheme is proposed. The main idea is use two keys to encrypt the original watermark. One key called public-key is generated by image feature, and the other called private-key is offered by user. This operation constructs a correlation between the watermark embedded and the carrier, which means the watermark is only valid in this carrier.

The Watermark Algorithm based on Information Layer Encryption

In order to prevent unauthorized user embezzle other people's watermark information, this algorithm encrypt the original watermark before it is embedded into the carrier. Traditional encryption algorithm use private-key to encrypt information, so it can be used to protect watermark from leakage, but cannot prevent the adversary copy it to other carriers. To solve this problem, a new key called public-key is added, which is extracted from the carrier. The final-key used to encrypt the watermark is computed from the public-key and the private-key. After encryption, a correlation between the watermark embedded and the carrier is constructed, which means if the watermark is copy to other carriers, the watermark detector will not decrypt it correctly, so it is invalid. This strategy solves the copy attack problem.

For ease of experimental tests and comparison, the watermark is embedded into the spatial domain. The flow chart of watermark embedding is show in Figure1. The embedding procedure can be divided into five steps: 1. Public-key extraction; 2. Key pre-process; 3. Watermark encryption with DES cryptographic algorithm; 4. Encode watermark with error correction coding and scrambling; 5. Watermark embedding based on LSB. Each step is discussed in detail below.

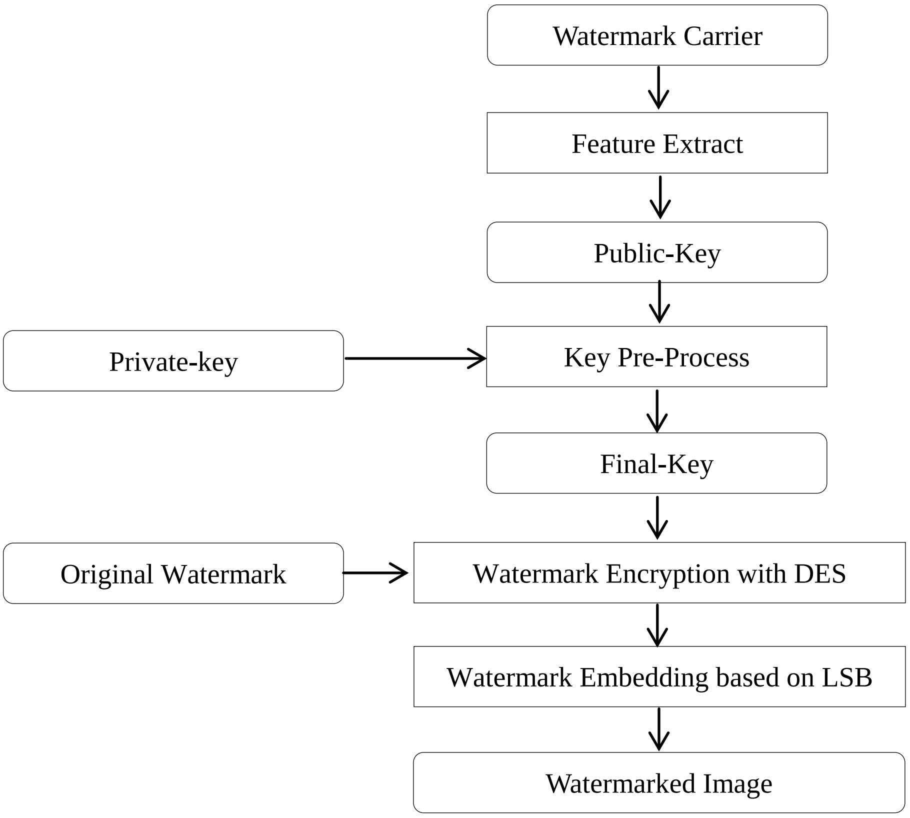


Fig.1. The flow chart of watermark embedding

Public-Key Extraction

Public-key is extracted from the carrier, and is used in watermark encryption and decryption. So the construction of public-key must select the stable feature of the carrier, and must make sure it will not change after the watermark embedding. Image gradient reflect the change speed of the pixels value. Some image processing methods may affect the image gradient, but the overall trend changes slightly. So we select image gradient to construct public-key, Figure 2 shows the flow chart of public-key extraction. The detailed procedure is as follows:

1. Compute the gradient of each pixel by gray value.

2. Project the gradient vector to four major directions, whose direction angles are $0^{\circ}, 90^{\circ}, 180^{\circ}$ and 270°.

3. Accumulate the gradient value of each major direction.

4. Sort the gradient value of each major direction, and convert the order index into binary, then combine them together to gain the final 8 bits feature sequence.

In this paper, we divide the carrier image into four parts, and compute the feature sequence respectively, and then combine them together to obtain the final 32 bits public-key.

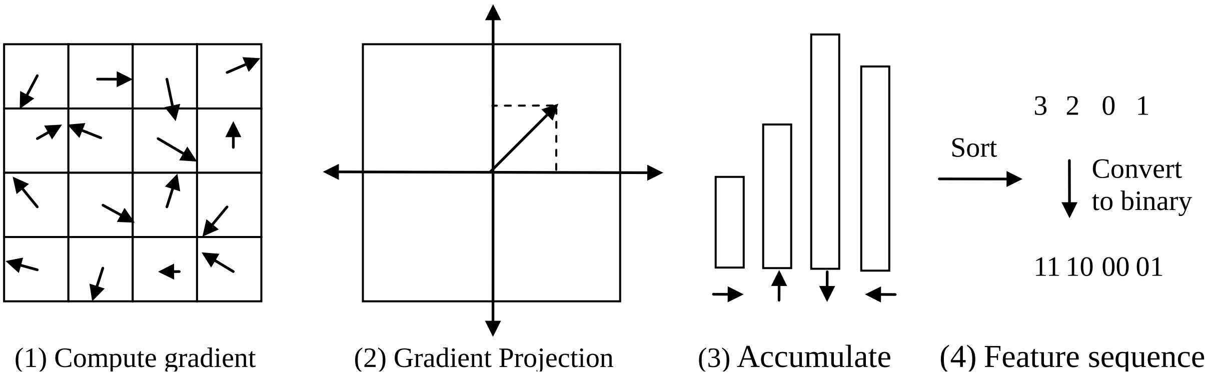


Fig.2. The flow chart of public-key extraction

Key Pre-Process

This paper choose DES encryption algorithm to encrypt the watermark. The key length is fixed 64 bits, 8 of them are parity bits, so only 56 bits are useful. Users can input 7 hexadecimal numbers called user-key. The watermark system computes the parity bits by user-key, and combines them together to form the private-key.

The idea of key pre-process is doing Bitwise XOR operation between public-key and private-key, the result is denoted by final-key.

Watermark Encryption with DES

The watermark information is encrypted by DES symmetric encryption algorithm. Because the length of the plaintext being encrypted by DES is fixed to 64 bits, so long message is divided into several groups, and each group is encrypted separately. This means the avalanche effect of DES only exists in each group, so parts of information may be cracked and leaked when it is transferred. To solve this problem, avalanche effect of DES should be extended between all groups, and form a global avalanche effect.

The algorithm to extend avalanche effect proposed in this paper is shown in figure 3. As can be seen from the figure 3, 8 bits are overlapped between two adjacent groups. In the first round of encryption process, each group is encrypted sequentially from left to right, so backward avalanche effect is produced; in the second round, each group is encrypted sequentially from right to left and forward avalanche effect is produced. In this way, avalanche effect of DES is extended to global field.

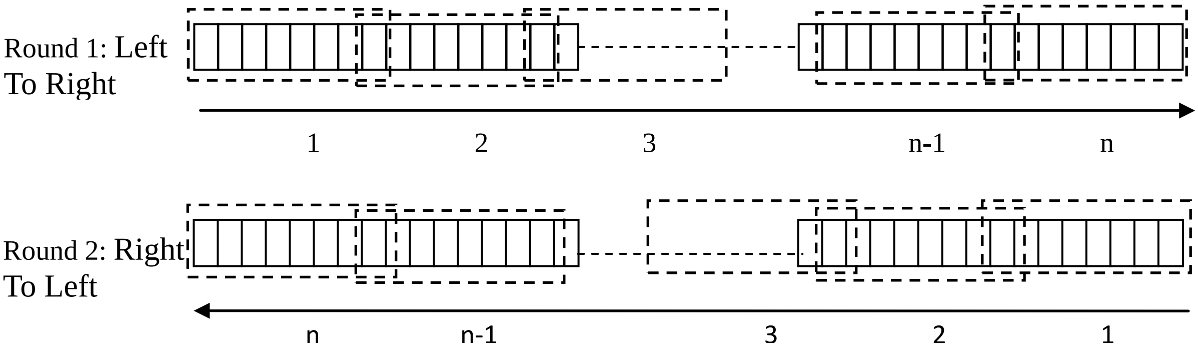


Fig.3. Extend avalanche effect of DES

Encode Watermark with Error Correction Coding and Scrambling

In the transfer process, random noise interference may be added to the watermark, in order to recover the watermark completely, error correcting code is adopted to encode the watermark in the information layer. The cipher text obtained in the previous step is encoded by hamming$(7,4)$code. After this, the watermark is scrambled by Arnold transform, which can disperse the centralized errors in the transport layer.

Watermark Embedding based on LSB

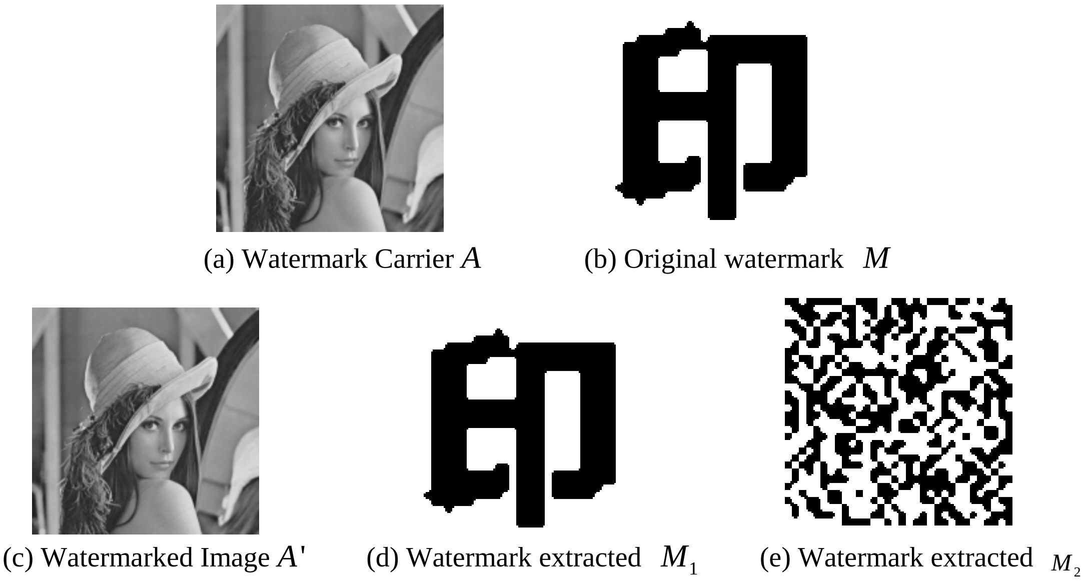
For ease of experimental tests and comparison, the classical LSB algorithm is adopted to embed the watermark. Limited by the space of paper, the embedding process of LSB is not given here.

The watermark extracting procedure is the inverse process of embedding procedure, it is also unnecessary to go into details.

Experimental results

The algorithm proposed in this paper is implemented on Matlab 2010. Lots of experiments are conducted, and the results are similar. Take one of them for example, the carrier is a 512×512 pixel Lena image (Figure 4(a)), watermark is a 32×32 pixel image (Figure 4(b)), the result is presented as follows.

Figure 4 shows the validation test result. The key used to encrypt the original watermark is ’3af234dc8e9b73’. Image A' (Figure 4(c)) is the watermarked image. The PSNR value is 41.89dB, which means the algorithm has high fidelity. M_1 (Figure 4(d)) is the watermark extracted from A' with correct decryption key. M_2 (Figure 4(e)) show the extracted watermark with the incorrect decryption key, which is ’3af234dc8e9b74’. The bit error rate of M_2 is 51.56% and the correlation is 0.0392. This indicates although only the last digit of the decryption key changes from 3 to 4, the extracted watermark is totally different. This verifies that this new watermark algorithm is very secure.



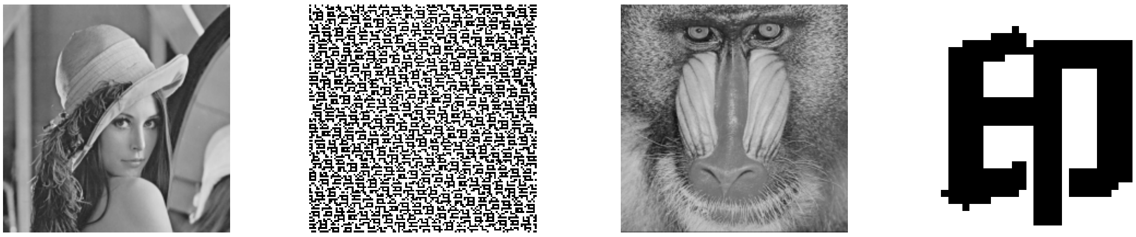
(a) Watermark Carrier A (b) Original watermark M

(c) Watermarked Image A' (d) Watermark extracted M_1 (e) Watermark extracted M_2

Fig.4. Copy Attack on Classical LSB Algorithm

The classical LSB algorithm has been chosen in the comparison tests of copy attack due to the watermark algorithm proposed in this paper is based on LSB. The attack strategy is copying the least significant bit-plane of the carrier with watermark to a new carrier, and then extracting the watermark in the new carrier by the detector.

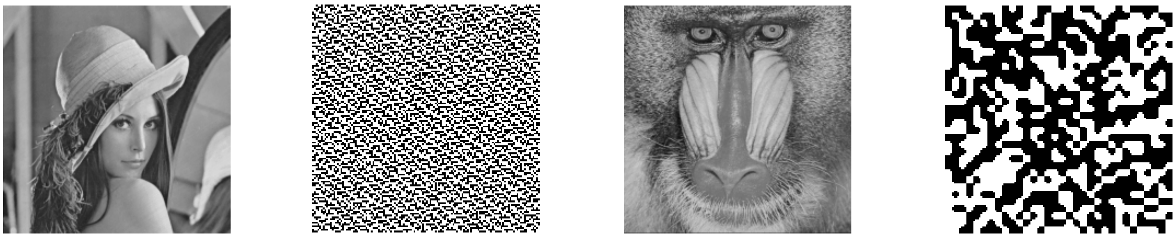
Figure 5 shows the attack result of classical LSB. Image B' (Figure 5(c)) is the new carrier embedded with the watermark M' (Figure 5(b)), which is copied from image A' (Figure 5(a)). Figure 5(d) is the watermark extracted from figure 5(c), the bit error rate is 0 and the correlation is 1. It is obvious that copy attack has implemented successfully to LSB watermark algorithm.



(a) Watermarked Image A' (b) Copied watermark (c) Copy Attacked Image B' (d) Watermark extracted

Fig.5. Copy Attack on Classical LSB Algorithm

Figure 6 shows the attack result of the watermark algorithm proposed in this paper. The key used to encrypt the watermark is ’3af234dc8e9b73’. Image B' (Figure 6(c)) is the new carrier embedded with watermark M' (Figure 6(b)), which is copied from image A' (Figure 6 (a)). Figure 6(d) is the watermark extracted from figure 6(c), the error rate is 49.41% and the correlation is 0.0220. The reason is that the public-key extract from B' cannot decrypt the encrypted watermark information correctly. Thus, the extracted water information is incorrect.



(a) Watermarked Image A' (b) Copied watermark (c) Copy Attacked Image B' (d) Watermark extracted

Fig.6. Copy Attack on Algorithm Proposed in this Paper

The experimental results verify that the encryption in information layer based on carrier features proposed in this paper can not only prevent watermark information from leakage, but also resist the copy attack.

Conclusion

This paper proposed an anti-copy attack watermarking algorithm based on information layer Encryption. The main idea is that in the procedure of pre-process, the feature of the carrier is used to encrypt the watermark information, which means the watermark embedded into the carrier is related to the carrier itself. This strategy ensures that if the watermark is copy to other carriers, the public-key extract by watermark detector will not decrypt the watermark correctly, so this new algorithm can resist copy attack. The experimental results also verify the conclusion above, and show that the watermark algorithm proposed in this paper is quite secure.

Acknowledgement

This work is supported by the state password development fund (No.MMJJ201401010).

References

[1] Pradhan C, Saha B J, Kabi K K. Comparative analysis of digital watermarking scheme using enhanced playfair cipher in DCT & DWT[C] Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on. IEEE, 2014: 1-6.

[2] Petrovic R, Atti V. Watermark based access control to copyrighted content[C] Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th

International Conference on. IEEE, 2013, 1: 315-322.

[3] Kavipriya R, Maheswari S. Statistical quantity based reversible watermarking for copyright protection of digital images[C] Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on. IEEE, 2014: 1-6.

[4] Kutter M, Voloshynovskiy S V, Herrigel A. Watermark copy attack[C]. Electronic Imaging. International Society for Optics and Photonics, 2000: 371-380.

[5] Zheng P, Wang W, Wang J. A Hybrid Watermarking Technique to Resist Tampering and Copy Attacks[C] Intelligence Information Processing and Trusted Computing (IPTC), 2011 2nd International Symposium on. IEEE, 2011: 111-114.

[6] NIU Xiao-li, LIU Ju, SUN Jian-de. A novel watermarking method resistant to copy attack [J]. Journal of ShanDong University, 2006, 41(4): 121-123.

[7] Zhang J, Zhang Q, Geng S, et al. A feature-based watermarking algorithm resistant to copy attack[C] Information and Automation (ICIA), 2011 IEEE International Conference on. IEEE, 2011: 838-842.

[8] Hu Hui-bo, Liu Ju, Sun Jian-de. An ICA-Based Watermarking Scheme Resistant to Copy Attack[J]. Journal of Electronics & Information Technology, 2005, 27(7): 1035-1038.

[9] Lu C S, Hsu C Y. Content-dependent multipurpose watermarking resistant against generalized copy attack[C] Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on. IEEE, 2004, 3: 2039-2042.