Authentication algorithm of secure digital halftone watermark based on SM4 algorithm

IOP Conf. Series: Materials Science and Engineering **563** (2019) 052013 doi:10.1088/1757-899X/563/5/052013

Authentication algorithm of secure digital halftone watermark based on SM4 algorithm

L Guo[1], A L Wang[1, 2], S K Li, J P Pang, K Xin, S X Fan and F P Liu

[1] Beijing Institute Of Graphic Communication

[2] Corresponding author, e-mail address is zuoanyizhen@163.com.

Abstract: With the development of information technology, the problem of piracy is getting worse. In order to increase the security of watermark information, this paper has proposed a security watermark authentication algorithm based on SM4 encryption algorithms, which is embedded in the frame of the vehicle image when the watermark information is encrypted. SM4 is the block cipher standard adopted in WAPI of wlan standard in China, and then adopted by commercial cipher standard in China. It is characterized by adding nonlinear changes in the calculation process, which greatly improves the security of the algorithm. Because the watermark information is embedded in the feature points of the structure, which is relatively stable and not easy to change, so the robustness of the watermark is enhanced to a certain extent. Through the test, the algorithm can encrypt and authenticate the watermark information.

1. Introduction

The increasing demand for material culture promotes the rapid development of science and technology. From traditional paper media to today's digital products, people's life has been greatly enriched. With the rapid development of the Internet, a lot of information has been provided for us. We can get all kinds of digital products from the Internet, but more and more problems followed[1]. There are a large number of pirated digital products on the Internet, or products that are used without authorization. Such infringement seriously affects the security order of the network and damages the interests of producers. Modern cryptographic technology plays a crucial role in ensuring information security. In order to ensure the security of digital products, this paper uses SM4 encryption algorithm for watermark encryption. SM4 encryption algorithm is a symmetric block cipher algorithm, but contains a non-linear part, compared with the international symmetric block cipher algorithm DES, it in the calculation round number, block length, key length and other aspects of performance due to DES[2]. In addition, nonlinear transformation is added in the calculation process, which greatly improves the security of the algorithm. SM4 encryption algorithm because of its convenience and feasibility, fast decryption speed and high security, have good results in e-commerce and e-government applications, provides a new solution for effectively protection of digital information and property security.

Halftone digital watermarking technology is a technology to hide information in the process of printing and output, and it is an effective measure to solve the problems of copyright protection, source authentication and certificate, bill and currency security of printed matter and output[3]. However, because only two pixels are "0" and "1"in halftone digital image, it is always a difficult problem to embed the watermark and keep the carrier image with good quality and the concealment of the watermark. The watermark embedding algorithm based on structural feature points can solve this problem well. Firstly, the image feature points do not have great continuity, which can disperse the watermark information and enhance the concealment of the watermark. Secondly, the structural

feature points of the carrier are selected instead of the direct feature points of the image, so that the feature of the carrier image will not change too much so as to maintain a good quality.

2. Halftone watermark information generation and SM4 encryption

2.1 Halftone watermarking information generation

Digital halftone technology refers to the quantization of a continuous tone image (such as grayscale image and color image) with a small amount of color into a binary image or an image with only a few concentrated colors, and the visual effect of the quantized image is similar to the original image. This quantization of the image we call the halftone image. The main halftone techniques include threshold jitter, error dispersion, point dispersion and noise halftone. In this paper, the error dispersion method is mainly used for halftone processing of carrier image[4]. In order to make the halftone image good and easy to realize, this algorithm will use the error dispersion method to obtain the halftone carrier information. The error dispersion method is a commonly used digital halftone method, which can disperse the noise generated by quantization to the intermediate frequency and high frequency which are not sensitive to human eyes, making the picture more exquisite. The basic idea of the error dispersion method is to spread the error which product by halftone to the pixels in the adjacent area. In this way the error caused by halftone is not obvious in the overall effect of the output image.
The process is shown in figure 1.

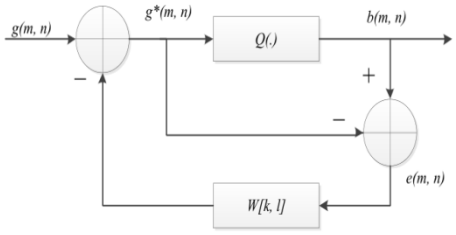

Figure1. Error dispersion method

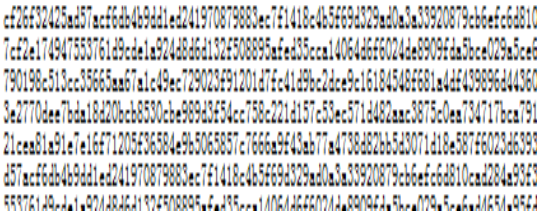

Figure5. Encrypted watermark information

Input $g[m, n] \in [0,1]$ represents the original continuous - tone image, output $b[m, n] \in \{0,1\}$ represents a halftone image, $g^*[m, n]$ is the quantization input, $w[k, l]$ is the weight coefficient of the error dispersion kernel, $e[m, n]$ is the quantization error, $Q(.)$ is the threshold quantization function. The carrier image and the carrier image after halftone are shown in figure 2 and 3.

Figure2. Carrier image

Figure3. Halftone image

Figure.4 Watermark image

2.2 SM4 encryption algorithm encryption watermark information

SM4 is a packet symmetric key algorithm, the plaintext, key, ciphertext are 16 bytes, encryption and decryption keys are the same. Encryption and decryption are realized through the nonlinear iterative round function of 32 cycles. These include the nonlinear transformation s-box, and the linear transformation composed of shift xor[5]. Plaintext X becomes ciphertext Y after 32 rounds of iterative function F, X and Y are both 128 bits, plaintext X is denoted as $(X_0,X_1,X_2,X_3) \in (Z_2^{32})^4$, Z_2^{32}represents a vector set of 32 bits, ciphertext Y is denoted as $(Y_0,Y_1,Y_2,Y_3) \in (Z_2^{32})^4$, The wheel key is $rk_i \in (Z_2^{32})^4$, i is the number of rounds , value range [1,32]. The iteration function F mainly consists of xor operation and synthetic substitution T, the synthetic substitution T is composed of the nonlinear transform and

the linear transform L. The specific operation expression of the round iteration function F is shown in formula (1).

$$X_{i+4}=Xi \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \quad (1)$$

The nonlinear transform consists of four parallel S boxes. Each s-box is a nonlinear transformation with an input and output of 8bit. The input to the linear transformation is $B \in (Z_2^{32})^4$,output is $C \in (Z_2^{32})^4$, the calculation expression of linear L is shown in formula (2) .

$$C=B \oplus (B<<<2) \oplus (B<<<10) \oplus (B<<<18) \oplus (B<<<24) \quad (2)$$

The encrypted watermark information of SM4 is shown in figure 5.

3. Secure digital halftone watermark authentication system based on SM4 algorithm

With the development of the Internet, the use of digital products has become more and more frequent. In order to protect the copyright of digital products, various corresponding algorithms have been proposed. This algorithm will use SM4 encryption algorithm to encrypt important information, protect the security of digital watermark and realize the authentication of digital halftone watermark. SM4 is the block cipher standard adopted in WAPI of wlan standard in China, and then adopted by commercial cipher standard in China. It is characterized by adding nonlinear changes in the calculation process, which greatly improves the security of the algorithm. SM4 algorithm is a grouping algorithm, the decryption algorithm and encryption algorithm structure is the same, but the use of round key order is opposite, the decryption round key is the reverse of the encryption round key order. As the block cipher standard of China's commercial passwords, it is expected that SM4 will gradually replace 3DES, AES and other foreign block cipher standards in sensitive but unclassified application fields in China, and be used for communication encryption, data encryption and other application occasions. The process is shown in figure 6.

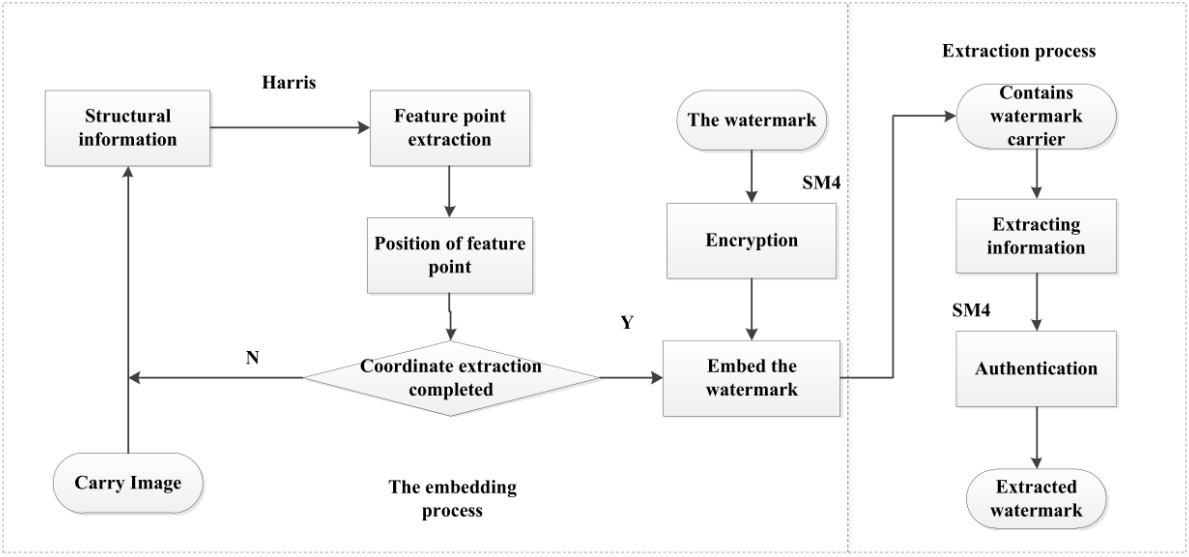

Figure6. System flow chart

3.1 Feature point extraction based on image structure

The encryption of watermark image has been realized and the processing of watermark embedding has been completed. This algorithm is embedded based on the structural feature points of the carrier image, so it is necessary to identify and locate the feature points of the carrier image. The steps are as follows:

(1). Carrier image halftone processing. The carrier image is shown in figure 3.

(2). Extracting the structure information of halftone image.

Matlab was used to extract the edge operator to extract the structural information. Because the

extracted structural information was incomplete and the edge was discontinuous, the image was smoothed and the edge was enhanced. The resulting image is shown in figure 8.

Figure7. Structural feature

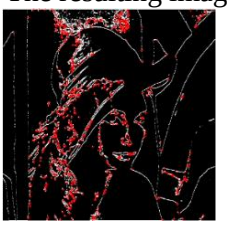

Figure8. Characteristic points

Figure9. Carrier characteristic points

(3). Harris corner point extraction algorithm is applied to identify feature points of halftone carrier image [6], and the location of feature points is recorded. As shown in figure 9.

(4). The location of the feature points corresponding to the half-tone image is shown in figure 10, and the system interface is shown in figure 11.

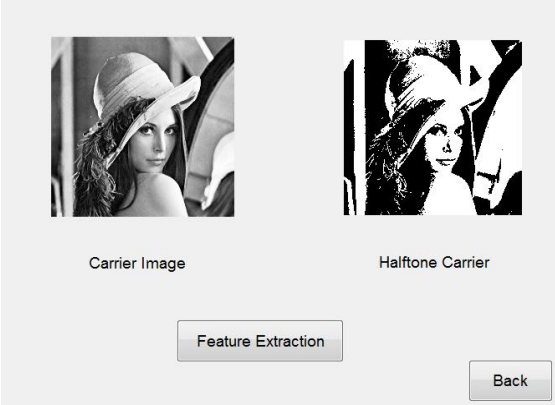

Figure10. Feature extraction

Figure11. Watermark embedding

3.2 Watermark embedding

Embedding the encrypted watermark information into the position of the feature points (directly embed in the alternative mode). The embedded carrier diagram is shown in figure 12, and the system interface is shown in figure 13.

Figure12. Embedded watermark carrier

Figure13. Extract the watermark

3.3 Watermark extraction and authentication

The first is to obtain the position of the structural feature points, the second is to extract the information at the position of the structural feature points, the third is to conduct SM4 decryption authentication of the extracted information, and the last is to re-synthesize the decrypted information into the watermark image, as shown in figure 13.

Figure14. Authentication interface

Figure15. Authentication successful

4. Summarize

Through the test, the algorithm can encrypt and authenticate the watermark information well. As SM4 algorithm is a grouping algorithm, the grouping length of this algorithm is 128 bits, and the key length is 128 bits. Both encryption algorithm and key expansion algorithm adopt 32 rounds of non-linear iterative structure, so they have good security and are difficult to crack, which can play the role of copyright protection. Half-tone carriers can be well applied in the field of printing and publishing, and further research will be carried out in the field of half-tone to strengthen the copyright protection in the field of printing and publishing. This algorithm uses structural feature points to embed watermark and applies it to halftone image, which greatly improves the quality of carrier image.

Acknowledgments

The authors thank all the Editor and the anonymous referees for their constructive comments and valuable suggestions, which are helpful to improve the quality of this paper. This paper is supported by the Beijing Municipal Natural Science Foundation Project B (KZ201510015015), Beijing Higher Education Improvement Program (PXM2017_014223_000063), BIGC Project (Ec201803 Ed201802 Ea201806).

References:

[1] Fan J Research on digital watermarking and fingerprint recognition algorithm in copyright protection and identity authentication 2012 D. Nanjing university of aeronautics and astronautics
[2] Yang R D and Li Z C. Research and implementation of a new E-mail encryption system based on the state secret algorithm 2018 J Information security research 4(11):1046-1051
[3] Xie K Research on digital watermarking technology based on halftone technology 2015 D Xi 'an university of electronic science and technology
[4] Liu W T, Yan Q, Song Z Y, Xu X, Chen Y H and Zou B Research on anti-printing watermarking algorithm based on half-tone digital image 2017 J Journal of qilu university of technology3 1(06):69-73.
[5] Zhang J, Wu W L Authentication encryption algorithm based on SM4 function design 2008 J Electronic news 46(06):1294-1299
[6] Liu K X, Improvement of Harris algorithm2018 J China new communications, 20(16):121