Secret Key Watermarking for Image Authentication

Chan-Il Woo, In-Chul Shin.

Dept. of Electronics and Computer Engineering, Dankook University, Seoul, Korea

Tel : +82-2-709-2592, Fax : +82-2-796-6395

E-mail : ciwoo@dankook.ac.kr, char@dankook.ac.kr

Abstract

As the growth of internet and the diffusion of wide multimedia applications are increased, the ownership verification and authentication in communication channel for a digital image become more important. For these purpose there are many watermarking scheme available for image, video stream and audio data.

In this paper we studied on techniques for integrity and authentication of digital images and proposed new watermarking algorithm. The proposed algorithm is implemented in C language on IBM-PC and the test results are shown.

1. Introduction

The increasing availability of digital information and the development of new multimedia broadcasting services has recently motivated research on copyright protection and authentication schemes for these services. Digital media offers several distinct advantages over analog media; easier edition and content modification, faster and more reliable transmission over networked information systems. In spite of these advantages many problems associated with copyright protection and authentication are increased. [1,2,3,4,5]

Watermarking methods are classified robust watermarking and fragile watermarking. Robust watermarks are designed to be detected even after attempts are made to remove watermark while fragile watermarks are capable of detecting minute changes of the watermarked content.[5,6,7,8]

In this paper we proposed a new technique for integrity and authentication of digital images. In this proposed algorithm we used by MD5 hash function and symmetric key encryption algorithm and the secret key is used as an input of the MD5 hash function for generating hash output code. Then we decided the position of embedding watermark and the bit position in that pixel by using the information of the hash output code.

The proposed algorithm has the advantage of difficulty to find positions of inserted watermarks, and keep the similar watermarked image quality with Wong's research.

2. Hash function

Traditionally authentication of digital information is performed using the digital signature principle. Digital signatures make use of one-way functions. In order to assure integrity a hash function is applied to the information bit-stream and the result of the hash function is ciphered. A hash function accept a variable-size message M as an input and produces a fixed-size hash code H(M), sometimes called a message digest as output and even a single bit in the original message produces a quite different hash output. So authentication based on hash functions is a powerful tool.

A hash function H must have the following properties.[8,9]

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.

3. H(M) is relatively easy to compute for any given M.
4. For any given code H, it is computationally infeasible to find M such that H(M) = H.
5. It is computationally infeasible to find any pair (M1, M2) such that H(M1) = H(M2)

The MD5 hash function is very popular in ciphering. This algorithm takes a message of arbitrary length as an input and produces a 128-bit message digest as an output.

The encryption process consists of an algorithm and a key. The algorithm produces a different output depending on the specific key being used at the time. In the symmetric encrypt system the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. Fig. 1 illustrates the encryption process. [9,10,11]

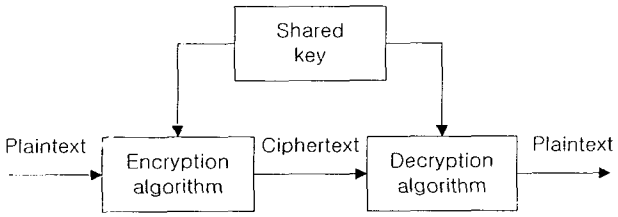

Fig. 1. Model of symmetric encryption

3. Proposed algorithm.

In this paper we proposed a new technique for improving the Wong's algorithm. [7] Wong insert watermark image into LSBs of all original image pixels. This method has two drawbacks, image distortion and known positions of watermarked image by a third party. So we conceal the embedded positions in watermarked image. The procedure of the proposed algorithm is shown in the following sections.

3.1 Embedding process.

1. The generation of hash output code

   Secret key is used as an input of the MD5 hash function. And the result of hash function is a 128-bit hash output code(H2), which will be used in calculation of embedding position of watermark.

   Fig. 2 shows the procedure of the message digest generation.

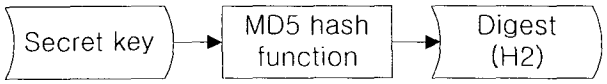

Fig. 2. The generation of hash output code.

2. Decision of embedding positions.

   A 128-bit hash output code is divided into N-bits blocks and M-bits blocks respectively. Pixels for inserting watermarks in original image are decided by multiplying M by N. (M is 4 bit in this paper.) In the selected pixel of the original image, we select a bit position to insert of watermark.

3. Decision of bit position.

   The bit position in the selected pixels for inserting watermark is decided by a value of a N-bit(2 bits in this paper).

   And selected bit positions in the original image are initialized to "0". The initialized image is used as the input of MD5 hash function to generate H1.

4. Generation of watermark

   The XOR operation between H1 and secret key generates H3. H3 is used to generate watermark(H4) using encryption algorithm. Fig. 3 shows the watermark generation process.

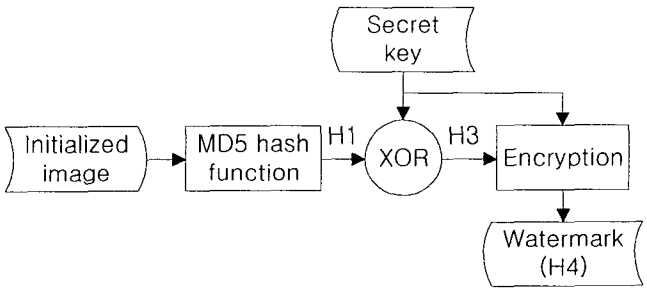

Fig. 3. Watermark generation process

Fig. 4 shows whole process for embedding the watermarks.

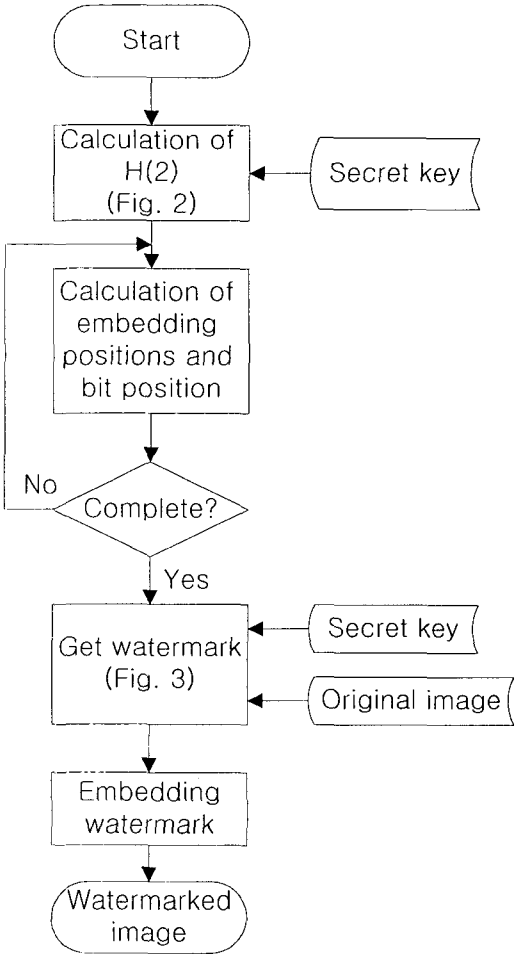

Fig. 4. Watermark embedding process.

3.2 Retrieval process.

The retrieval is processed in reverse order of embedding process.

1. Secret key is used as an input of the MD5 hash function. And the result of hash function is a 128-bit hash output code(H2).
2. A 128-bit hash output code is divided into N-bits blocks and M-bits blocks respectively. Pixels of inserted watermarks are decided by multiplying M by N and the bit position in that pixel is retrieved by a N-bit value of H2. The retrieved positions in the watermarked image are initialized to "0".
3. We extract watermark(H4). And the initialized image is used as the input of MD5 hash function to generate H1.
4. Extracted watermark is decrypted by secret key. The result of decryption is H3. The result of the XOR operation between H1 and H3 should be secret key.
5. The secret key and the detected secret key are compared. If they are equal, then authentication is a success. Fig. 5 shows this process.

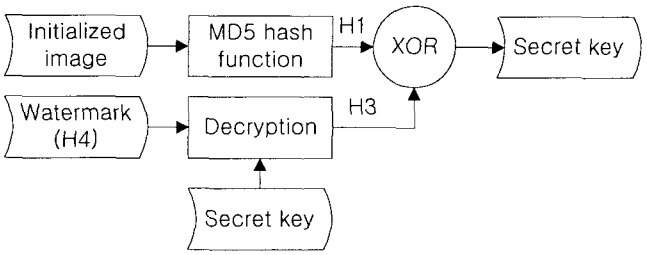

Fig. 5. Detection of secret key.

4. Experimental results

In this paper we use 256×256 Lena image of fig. 8 as an original image. Followings are the parameters and results we took :

- secret key ;

  1a d d3 28 56 79 f3 ee dd 38 7a ad de 29 18 80

- Hash value of the secret key ;

  92 3e fd c4 d8 1 e9 da 52 8e 25 75 f4 df 6e 41

- Values of M and N ;

  M = 4

  N = 2

- Embedding positions ;

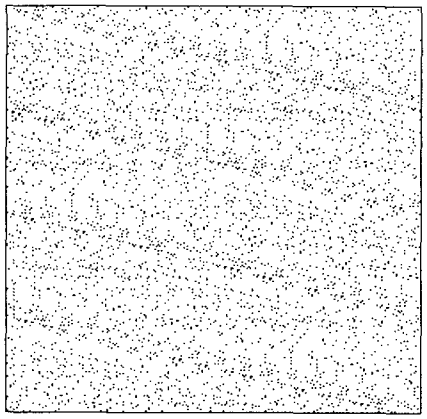

Fig. 6. Embedding positions

- Watermark ;

  1e 4 1f 59 3e 42 8d 57 22 66 95 96 8d 3b 32 cf

- Watermarked image ;

Fig. 7. Watermarked image.

- PSNR of watermarked image : 49.95dB

Fig. 8. 256×256 Lena.(original)

The PSNR of watermarked image using proposed algorithm is 49.95dB and Wong's algorithm is 51.13dB. Image distortion of the proposed algorithm is similar to Wong's algorithm. Wong insert watermark into LSBs of all original image pixels, so embedding positions are revealed but in this proposed algorithm, embedding positions can not be found without secret key.

5. Conclusion

In this paper we described new technique of spatial domain watermarking using MD5 hash function and secret key encryption algorithm for integrity and authentication. The proposed algorithm has the advantage to hide embedded positions of the watermark image from illegal third party. For the further research, we consider that our method can be used together with other robust methods for copyright protection. Thus it will be improve the effectiveness and robustness of our proposed method.

References

[1] M.P.Queluz, "Content-based integrity protection of digital images," Proc. of SPIE, Vol. 3657, Jan., pp. 85 ~ 93, 1999.

[2] K.S.NG and L.M.CHENG "Selective block assignment approach for robust digital image watermarking," Proc. of SPIE, Vol. 3657, Jan., pp. 14 ~ 20, 1999.

[3] M. D. Swanson, Bin Zhu, A. H. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE ICIP, Vol. 3, Sep., pp. 211~214, 1996.

[4] Keith T. Knox, "Reversible Digital Image," Proc. of SPIE, Jan., pp. 397~401. 1999.

[5] Q.SUN, J.WU, R.DENG, "Recovering modified watermarked image with reference to original image," Proc. Of SPIE, Vol. 3657, Jan., pp. 415~424, 1999.

[6] E.T.Lin, C.I.Podilchuk, E.J.Delp, "Detection of image alterations using semi-fragile watermarks," http://dynamo.ecn.purdue/~ace/delp-pub.html.

[7] P. W. Wong, "A Public Key Watermark for Image Verification and Authentication," In Proc. of ICIP, Oct., 1998.

[8] R. B. Wolfgang, J. D. Edward, "Fragile Watermarking Using VW2D Watermark," Proc. of SPIE, Vol. 3657, Jan., pp. 204 ~ 213, 1999.

[9] William Stallings, Network and Internetwork Security, Prentice Hall, 1995.

[10] 박창섭, 암호이론과 보안, 대영사, 1999.

[11] 이민섭, 현대암호학, 교우사, 1999.