

Secure Fragile Watermarking Algorithm with Side Information

Ying Zhang, Jun Xiao, Ying Wang, and Yan.d

College of Computing & Communication Engineering, Graduate University of Chinese Academy of Sciences
Beijing, 100049, China

Email: zhangying207@mails.gucas.ac.cn, xiaojun@gucas.ac.cn, ywang@gucas.ac.cn, yanddenator@gmail.com

Abstract—Security is an important performance of watermarking system. In this paper, the idea of side information is introduced into the security domain of watermarking system, and a secure fragile digital watermarking algorithm with side information is proposed associating with the idea of cryptography. In the proposed algorithm, the original image is segmented into blocks and the watermark is segmented into subsections, and then the current subsection of watermark is preprocessed by using the former subsection of watermark as side information. The embedding position of each subsection of watermark is also chosen by using the position of the former subsection of watermark as side information. Each part of watermark and embedding position is good associated, so good security of the proposed watermarking system can be obtained. Experimental results show that the proposed algorithm can improve the security of watermarking system effectually.

Index Terms—fragile watermark; security; side information; cryptology;

I. INTRODUCTION

With the development of computer and network, digital watermark is becoming widely used, and as an important factor, watermarking security worth more research [1, 2].

There have been great achievements for watermarking security [3-9], most of which applying cryptography and can be attributed to two categories: one is encrypting the embedding place [3, 4], and the other is encrypting the watermark [5-9]. In the year 2002, Weiwei and others brought up a typical method based on chaos theory [3], the method can resist the exhaustive attack by encrypting the embedding place. But the embedding positions are selected randomly in this method, when the selected positions are the high significant bits, the image will be affected highly.

Encrypting the watermark can also be classified to two categories, one is using image scrambling [5, 6], and the other is using cryptography [7-9]. The initial watermark is encrypted and embedded by using the classical numeration of the image scrambling, e.g. Arnold, Hilbert, Fibonacci and Fibonacci-Q. So, the initial watermark still can not be seen by the attacker when the carrier is attacked. But the image scrambling still has hidden trouble, when attacked, the encrypted watermark is extracted and may lead to the initial watermark be resumed finally. The cryptography is mostly used in text watermark. The text watermark is encrypted by using

cryptographic algorithm and embedded. The method has the same defect as the image scrambling.

Today, side information is seldom used in the researches of watermarking security. In 1999, Cox and others considered watermark as communications with side information [10]. Now, the advantages of watermarking system with side information are accepted by more and more people. But there is still no any report on enhancing the watermarking security by using side information.

Side information will be used for enhancing the watermarking security in this paper, and a new algorithm is proposed, the relationship between watermark and the carrier will be made full use of when the watermark is preprocessed or the embedding position is selected.

The realization of the algorithm will be explained in the second part of this paper, including the embedding and extracting procedure. The algorithm will be tested and the conclusion will be given in the third part of this paper.

II. SECURITY WATERMARKING ALGORITHM BASED ON SIDE INFORMATION

To make full use of the idea of side information, the relationship between the watermark and its carrier is considered as side information. The watermarking security is improved in two ways, i.e. the embedding position and the watermark. The embedding place is selected by using Hill Cipher's idea. And the watermark is preprocessed by using XOR algorithm. The two ways are connected to improve the watermarking security. The Fig.1 shows the embedding and extracting procedure.

A. Embedding procedure

As shown in the Fig.1, the embedding procedure can be divided into four steps.

Step 1: Segment the original image into blocks. Suppose the cover image C_0 is a gray image with size of $M \times N$ pixels and is segmented into blocks with $M_0 \times N_0$ pixels. In order to unify the modular arithmetic of coordinate, we need to make sure that $\left\lceil \frac{M}{M_0} \right\rceil = \left\lceil \frac{N}{N_0} \right\rceil$, $\lceil \cdot \rceil$ stands for floor. And we use $C_0(k, i, j)$ stands for the pixel of (i, j) in block k. Let

$$P = \begin{bmatrix} M \\ M_0 \end{bmatrix} = \begin{bmatrix} N \\ N_0 \end{bmatrix}, \text{ and the position of block is}$$

expressed in the form of two-dimensional (x, y) , such as $(1,1)$ stands for $C_0(1,::)$, $(1,2)$ stands for $C_0(2,::)$, \dots , $C_0(1+P,::)$, (P, P) stands for $C_0(P \times P, ::)$.

Step 2: Watermarking preprocess with side information. Watermark m is segmented into subsections $a_1 \dots a_L$, and the size of each subsection is $M_0 \times N_0$. The previous watermarking subsection is considered as side information, and the current watermarking subsection is treated according to XOR algorithm by using the side information, then the watermark subsections $b_1 \dots b_L$ are got, as in (1).

$$\begin{cases} b_1 = a_1 \\ b_2 = a_2 \oplus a_1 \\ \vdots \\ b_L = a_L \oplus a_{L-1} \end{cases} \quad (1)$$

Step 3: Calculate the embedding position of watermark with side information. Before embedded, the image is considered as side information and the embedding position is calculated according to the mathematical thought of Hill Cipher algorithm by using the side information.

Particular way is: The next embedding position is calculated by multiplying key matrix by the current embedding position, as the function $F(x, y)$ shown in (2).

$$F(x, y) : (x', y')^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (x, y)^T \text{ mod } P \quad (2)$$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ stands for key matrix, P is got from step 1,

$(x', y')^T$ and $(x, y)^T$ stands for the position got in step 1. In counting, the initial position (x, y) stands for current position, (x', y') stands for the next position got from the current position according to (2). Then the position calculation is continued by considering (x', y') as current position.

It is worth noting that to avoid the position collision, the initial position should be changed after being calculated for a set number of times, and then the position calculation is continued with the new initial position until all the embedding positions are got. Moreover, suppose the (x', y') is the calculated position, then we use $(x'+1, y'+1)$ as the embedding position, because the Equation (2) is modular arithmetic and the initial position of block is $(1,1)$

Step 4: Watermark Embedding. In the algorithm, one bit of the watermark subsection is embedded in one pixel of image block by using the least significant bit algorithm. After finishing the watermark embedding, we need also embed the encrypted key matrix and last position into the specified block, and the storage format is shown in Fig.2 and Fig.3. k_i stands for the digit of the binary representation of i , n_0 stands for the number of last position. The encrypted key matrix and last position can also be used to realize the user authentication.

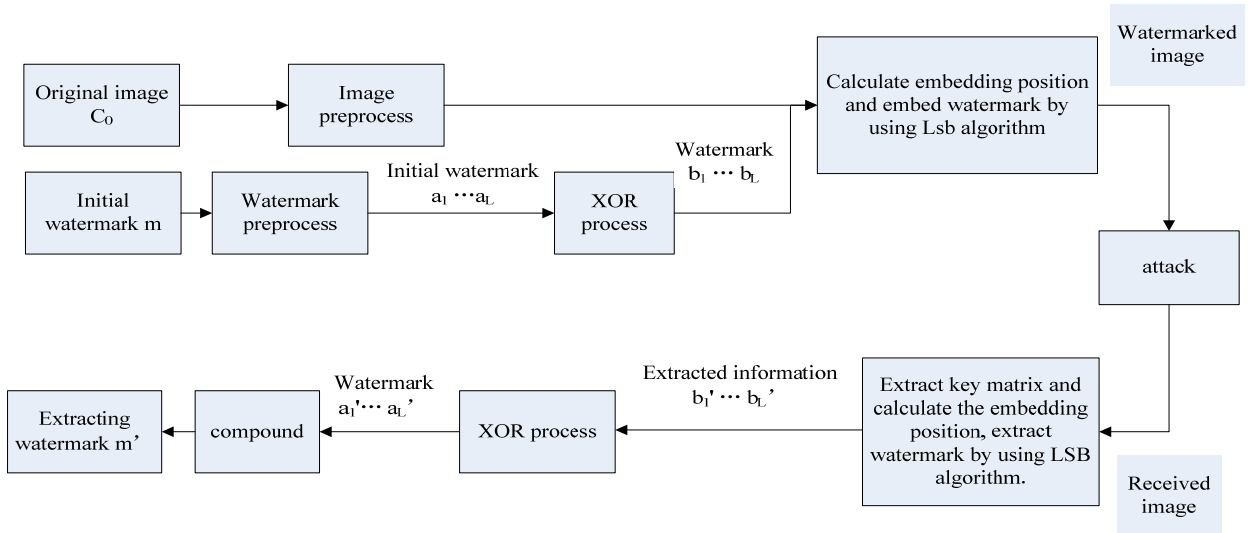


Figure 1. Algorithm diagram

From the embedding procedure, we can see that the idea of cryptograph is blended into the watermark algorithm, and the side information is also used to ensure the watermarking security.

k_a	a	\dots	k_d	d
-------	-----	---------	-------	-----

Figure 2. The storage format of the key matrix

n_0	k_{x_1}	x_1	k_{y_1}	y_1	\dots
-------	-----------	-------	-----------	-------	---------

Figure 3. The storage format of the last position

B. Extracting procedure

According to the Fig.1, the extracting procedure of the new algorithm is the inverse of the embedding procedure. The extracting procedure can be described as the following three steps.

Step 1: Extract the key matrix and the last position. We segment the received image into blocks like the step 1 of embedding procedure, and extract the key matrix and last position from the specified block first. Then we calculate

the modular inverse matrix $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ according to (3).

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (3)$$

Step 2: Calculate the embedding position. We calculate the preceding position according to the function $F'(x, y)$ in (4) by using the modular inverse matrix of the key matrix and the last position, and extract the embedding information $b_1' \dots b_L'$ by using LSB algorithm.

$$\begin{aligned} F'(x, y) &: \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} (x', y')^T \bmod P \\ &= \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} (x, y)^T \bmod P \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (x, y)^T \bmod P \\ &= (x, y)^T \end{aligned} \quad (4)$$

Step 3: Resume the watermark. The initial watermark subsections $a_1' \dots a_L'$ is resumed from $b_1' \dots b_L'$ extracted in the step 2 according to (5).

$$\begin{aligned} G'(x, y) &: b_1' = a_1' \\ a_1' \oplus b_2' &= a_1' \oplus a_1' \oplus a_2' = a_2' \\ a_2' \oplus b_3' &= a_2' \oplus a_2' \oplus a_3' = a_3' \\ &\vdots \\ a_{L-1}' \oplus b_L' &= a_L' \end{aligned} \quad (5)$$

From the embedding and extracting procedure, we can see that the watermarking security is improved by using side information, even though attackers can obtain some watermark subsections, they can't get any useful information. And after attacked, some watermark subsections will be destroyed, as a result, watermark will be destroyed because of the XOR process.

III. EXPERIMENTAL RESULTS

To verify the security of the new algorithm, we use the new algorithm and the traditional LSB algorithm to test many images and obtain the same result. Due to space constraints, here we only use the lena image with size of 256*256 shown in Fig.4 and the watermark image with size of 64*64 shown in Fig.5, and segment the lena image into blocks with size of 8*8 as example to show the experimental result, as shown in TABLE I.

We can see from the test result given in TABLE I, when the image is attacked by shearing, most of the watermark is intact by using LSB algorithm. Yet by using the new algorithm, the watermark will be destroyed seriously because of the XOR process. And when the image is attacked by scaling, average of four fields and window median filter, the watermark extracted by using LSB algorithm can be recognized. By contrast, the watermark extracted by using the new algorithm can't be made out because of the XOR process. When the image is attacked by exhaustive attack, the watermark will be extracted integrality by using LSB algorithm, but the watermark won't be extracted integrality because of the embedding position calculation by using the new algorithm.

Moreover, when the image is attacked by JPEG compression and Gaussian noise, due to the fragility of the new algorithm, the digit information shown in Fig.2 and Fig.3 will be destroyed, and then the algorithm will exit and the watermark can't be extracted.

We can see that the new algorithm is more fragile than the traditional LSB algorithm. When the watermark embedded by using the new algorithm is attacked, because of the side information is fully used in the new algorithm, the watermark extracted can't be recognized. And if the key matrix or the last position in the specified block is destroyed, the new algorithm will exit. So the new algorithm has high security.











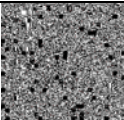
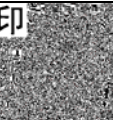


Figure 4. Original image



Figure 5. watermark

TABLE I. COMPARISON BETWEEN THE NEW ALGORITHM AND THE LSB

Attack type	New algorithm	LSB algorithm
Shearing		
Double the size of image		
Reduce the size of image by a quarter		
Average of four fields		
Window median filter		
Exhaustive attack		

IV. CONCLUSION

A new algorithm with the idea of cryptograph is proposed in this paper. In the new algorithm, the image is segmented into blocks, and watermark is segmented into subsections, then the subsection has been embedded is considered as side information. The embedding position and the watermark are encrypted by using different methods, and side information is used to improve the watermarking security.

It is shown in the experiment that the new algorithm has good fragility and high security. The side information is fully used in the new algorithm to interconnect each part of watermark, so that if you want to get right watermark you must obtain all right parts of watermark.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China (No.60772155), Beijing Natural Science Foundation (No.4082029) and China Postdoctoral Science Foundation.

REFERENCES

- [1] Ying Wang, Jun Xiao, and Yun-hong Wang, Digital Watermarking Principles and Techniques. Science Press, Beijing, 2007(in Chinese).
- [2] Cayre, Francois, Fontaine, Caroline, and Furon, Teddy, Watermarking security: Theory and practice, IEEE Transactions on Signal Processing, v 53, n 10 II, p 3976-3987, October 2005.
- [3] Weiwei Xiao, Zhen Ji, Xhong Zhang, and Weiyong Wu, A watermarking algorithm based on chaotic encryption, TENCON apos' 02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, Volume 1, Issue , Page(s): 545 – 548, 28-31 Oct. 2002.
- [4] Liu, Pei-Pei, Zhu, Zhong-Liang, Wang, Hong-Xia, and Yan, Tian-Yun, A novel image fragile watermarking algorithm based on chaotic map, Proceedings-1st International Congress on Image and Signal Processing, CISP 2008, v 5, p631-634, 2008.
- [5] Zhao, Rui-Mei, Lian, Hua, Pang, Hua-Wei, and Hu, Bo-Ning, Digital image watermarking algorithm with double encryption by Arnold transform and logistic, Proceedings-4th International Conference on Networked Computing and Advanced Information Management, NCM 2008, v 1, p 329-334, 2008.
- [6] Ye, Ruisong, and Li, Huiliang, A novel image scrambling and watermarking scheme based on cellular automata, Proceedings of the International Symposium on Electronic Commerce and Security, ISECS 2008, p 938-941, 2008.
- [7] Craver, Scott, and Katzenbeisser, Stefan, Security analysis of public-key watermarking schemes, Proceedings of SPIE-The International Society for Optical Engineering, v 4475, p 172-182, 2001.
- [8] Xie, Rongsheng, Wu, Keshou, Du, Jiangbo, and Li, Chunguang, Survey of public key digital watermarking systems, Proceedings-SNPD 2007:Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, v 2, p 439-443, 2007.
- [9] Picard, J, and Robert, A, On the public key watermarking issue, Proceedings-2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IHH-MSP 2008, p 1344-1347, 2008.
- [10] Cox I J, Miller M L, and Mckellips A L, Watermarking as Communications with Side Information, Proceedings of the IEEE, 87(7): 1127~1141, 1999