

# The Medical Image Watermarking Using Arnold Scrambling and DFT

Jingbing Li \*

College of Information Science and Technology  
Hainan University  
Haikou, China  
Jingbingli2008@hotmail.com

SuiMiao

College of Information Science and Technology  
Hainan University  
Haikou, China  
miao630808@163.com

**Abstract**—During network transmission, when an exception occurs (such as forgery, tampering, information confusion), digital medical image, as a diagnostic basis, can not serve as the evidence of medical accident case. And the ROI of medical image is unable to tolerate significant changes. In order to dealing these problems, we have proposed an algorithm that uses Arnold scrambling to preprocess on the original watermarking, improve the security of watermarking, and combing the visual feature vector of image, the encryption technology and the concept of third-party. Moreover, without the sophisticated process to finding the Region of Interest (ROI) of medical images, so, compared with the existing medical watermarking techniques, it can embed much more data, less complexity. The experimental results show that the scheme has strong robustness against common attacks and geometric attacks.

**Keywords**—Arnold scrambling; DFT; Zero-watermarking; Medical image.

## INTRODUCTION

With the rapid development of computer science and technology, and multimedia communication technology, telemedicine is becoming more and more universal [1]. When medical image transmission on the Internet, the personal information of the patient is likely to leak [2][3]. Using the invisibility and robustness of digital watermarking can better solve this problem. The patient's personal information, as a digital watermarking, embedded in medical image.

Currently the field of digital watermarking for medical research focused on the spatial domain and transform domain (DCT, DFT and DWT) [4], which can be implemented by changing some pixel gray-scale values in the space domain or by changing the values of coefficients in the transform domain to embed watermark.

Although current traditional watermarking techniques were primarily developed for applications such as multimedia copyright protection, they may not be quite suitable for the medical image's information security. The protection of medical information has strict ethics and legislative rules. Due to the lesions (we also called ROI) exists in the medical image, and this content is unable to tolerate significant changes [5]. So some people put the watermarking into the outside of lesion areas (we also called RONI) [6]. But it must be waste lots of time and energy to select the outside of lesion areas.

This paper proposes a watermarking algorithm which employs the Arnold scrambling to preprocess on original

watermarking, improve the security of watermarking information. And avoiding the tedious process for selecting ROI. The result of experiment indicates that the algorithm can achieve a true embedded zero-watermarking. The feature of blind extraction incorporated increases the strength of the watermarking system as it does not need the original unmarked image for watermarking extraction. Meanwhile, it has a strong robustness against common attacks and geometric attacks.

## THE FUNDAMENTAL THEORY

### A. Arnold scrambling Transform (AT)

Scrambling transformation as a means of encrypted technology is applied in the pretreatment stage of the watermarking, after scrambling transformation, one meaningful watermarking will become a meaningless, chaotic image. If you do not know the scrambling algorithm and keys, the attacker can not recover it even if he gets the watermarking from the embedded watermarking. And thus plays a role of secondary encryption. Additionally, after scrambling transformation, it will upset the relationship between the space locations of pixels and make it evenly distributed in all space of the carrier image. This will improve the robustness of the algorithm. Two-dimensional Arnold scrambling transformation is defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad x, y \in \{0, 1, 2, \dots, N-1\} \quad (1)$$

Wherein,  $x, y$  is the pixel coordinates of the original space;  $x', y'$  is the pixel coordinates after iterative computation scrambling,  $N$  is the size of the rectangular image, also referred to as a step number.

By the above formula the corresponding inverse transform formula can be obtained:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} + \begin{bmatrix} N \\ N \end{bmatrix} \bmod N \quad x', y' \in \{0, 1, 2, \dots, N-1\} \quad (2)$$

It is easy to restore the original initial state according to the corresponding iterations. Arnold transformation is cyclical, when iterate to a step, will regain original image. So if you do not know cycle and iterations, you will not be able to restore the image. Therefore, cycle and iterations can exist

as a private key. Meanwhile, different image, because the desired effect is different, iterations should also be changed according to your need.

#### B. A method to obtain the feature vector of medical image

First, the original image is computed using DFT. Then, we choose 5 low-frequency coefficients ( $F(1,1)$ ,  $F(1,2)$ , ...,  $F(1,5)$ ) for formation of the feature vector, shown in Table I. We find that the value of the low-frequent coefficients may change after the image has undergone an attack, particularly geometric attacks. However, the signs of the coefficients remain unchanged even with strong geometric attacks, as also shown in Table I. Let “1”

represents a positive or zero coefficient, and “0” represents a negative coefficient, and then we can obtain the sign sequence of low-frequency coefficients, as shown in the column “Sequence of coefficient signs” in Table I. After attacks, the sign sequence is unchanged, and the Normalized Cross-correlation (NC) is equal to 1.0.

This means that the signs of the sequence can be regarded as the feature vector of the medical image. Furthermore, it proves that the sequence of the DFT coefficient signs can reflect the main visual characteristics of medical images.

TABLE I. CHANGE OF DFT LOW-FREQUENCY COEFFICIENTS WITH RESPECT TO DIFFERENT ATTACKS.

Image processing	PSNR	F(1,1)	F(1,2)	F(1,3)	F(1,4)	F(1,5)	Sequence of coefficient signs	NC
Original image		405.1	-238.1-13.6i	-1.7-0.07i	34.6+4.6i	9.5+5.3i	1100001111	1.00
Gaussian interference (2%)	9.61	557.4	-185.8-12.4i	-2.6-2.1i	29.8+9.1i	5.2+4.3i	1100001111	1.00
JPEGcompression(4%)	17.61	418.9	-211.4-17.0i	-13.1-0.08i	35.5+6.8i	12.7+9.8i	1100001111	1.00
Median filter [3x3]	24.52	407.9	-241.4-13.3i	-0.1-0.2i	35.6+4.7i	9.9+5.4i	1100001111	1.00
Rotation (clockwise, 20°)	12.38	405.0	-220.6-39.6i	-12.6-11.7i	22.8+11.1i	10.6+14.0i	1100001111	1.00
Scaling(×2)		101.5	-59.4-4.8i	-0.57-0.05i	8.5+1.8i	2.2+1.6i	1100001111	1.00
Scaling(×0.5)		1623.1	-953.9-42.7i	-7.9-0.2i	138.6+13.3i	39.7+19.8i	1100001111	1.00
Translation(7%, down)	11.69	393.3	-227.6-12.8i	-9.1-1.1i	38.1+5.5i	9.3+5.1i	1100001111	1.00
Cropping(10%) (fromY direction)		381.0	-218.6-12.7i	-11.1-0.9i	35.4+5.1i	11.4+5.1i	1100001111	1.00

### III. ROBUST WATERMARKING ALGORITHM BASED ON DIGITAL MEDICAL IMAGE

Use a meaningful binary image as the watermarking, Represented by  $W$ ,  $F$  represents the original medical image, The  $W=\{w(i,j) | w(i,j)=0,1; 1 \leq i \leq M1, 1 \leq j \leq M2\}$  as digital watermarking. At the same time, we select the tenth slice of one medical volume data as the original medical image. It is describe as:  $F=\{f(i,j) | f(i,j) \in R; 1 \leq i \leq N1, 1 \leq j \leq N2\}$ , where  $w((i,j))$  and  $f(i,j)$  denote the pixel gray values of the watermarking and the original medical image, Let  $M1 = M2 = M$ ,  $N1 = N2 = N$ .

#### A. The algorithm of the embedded watermarking .

##### Step1 Acquire the the encrypted watermarking image.

The binary watermarking image is scrambled by Arnold scrambling transform,  $BW(i,j)$ .

$$BW(i,j) = AT(W(i,j)) \quad (3)$$

##### Step2 Acquire the feature vector of the original medical image.

First, DFT of the whole  $F(i,j)$  is computed as the DFT coefficient matrix,  $FF(i,j)$ . Then, after arranging the DFT

coefficients from low to high frequency, the low-frequency sequence  $Y(j)$  can be obtained. Finally, the feature vector  $V=\{v(j) | v(j)=0 \text{ or } 1; 1 \leq j \leq L\}$ , can be achieved as a signs sequence of the top  $L$  values in the low-frequency  $Y(j)$  by symbolic computation. Where the value of  $L$  can tune the robustness and capability of the embedded watermarking (in this paper we set  $L=32=4 \times 8$  bits).

$$FF(i,j) = DFT2(F(i,j)) \quad (4)$$

$$V(j) = -Sign(Y(j)) \quad (5)$$

##### Step3 Generate the public key sequence

Utilizing the encrypted watermarking  $BW(i,j)$  and the feature vector  $V(j)$ , we can generate the public key sequence,  $Key(i,j)$ .

$$Key(i,j) = V(j) \oplus BW(i,j) \quad (6)$$

The public key sequence,  $Key(i,j)$ , can be computed by the HASH function of cryptography. The  $Key(i,j)$  should be stored for extracting the embedded watermarking later. Furthermore,  $Key(i,j)$  can also be regarded as a public key and registered to the third part to preserve the ownership of

the original image registered to the third part to preserve the ownership of the original medical image, so as to achieve the purpose of the protection of medical images.

#### B. The algorithm of the extracted watermarking.

##### Step1 Acquire the feature vector of the tested image.

This process of acquiring the feature vector  $T\_V'(j)$  is same to step1 of the watermarking embedding process. The obtained feature vector,  $T\_V'(j) = \{t\_v(j) \mid t\_v(j) = 0 \text{ or } 1; 1 \leq j \leq L\}$ , also consists of the signs sequence of the DFT coefficients, where  $L$  has the same meaning as previously.

$$FF'(i, j) = DFT2(F'(i, j)) \quad (7)$$

$$T\_V'(j) = -\text{Sign}(Y'(j)) \quad (8)$$

##### Step2 Extracting the watermarking $BW'(i, j)$ .

According to the key which generated in the embedded watermarking and the visual feature vector  $T\_V'(j)$  of the being tested image, use HASH function properties to extract the watermarking  $BW'(i, j)$ . Extracting watermarking doesn't need original image, so it can protect the original image better.

$$BW'(i, j) = \text{Key}(i, j) \oplus T\_V'(j) \quad (9)$$

Step3 Using the Arnold scrambling inverse transform to restore the extracted watermarking  $BW'(i, j)$ , get the watermarking of the being tested image,  $W'(i, j)$ .

$$W'(i, j) = \text{IAT}(BW'(i, j)) \quad (10)$$

#### C. Detection algorithm of the watermarking.

Step1 By calculating NC (Normalized Cross-Correlation) to determine whether there is the existence of the watermarking. The larger the value of NC is, the more approximation between  $W'(i, j)$  and  $W(i, j)$ . Defined as:

$$NC = \frac{\sum_i \sum_j W_{(i,j)} W'_{(i,j)}}{\sum_i \sum_j W_{(i,j)}^2} \quad (11)$$

Where,  $W(i, j)$  is the original watermarking,  $W'(i, j)$  is the extracted watermarking.

Step2 Evaluation of the quality of the medical image after Embed watermarking by calculating the peak signal-to-noise ratio PSNR (dB), we often use peak value signal-to-noise ratio PSNR (dB) to reflect the quality of signal, defined as:

$$PSNR = 10 \lg \left[ \frac{MN \max_{i,j} (I_{(i,j)})^2}{\sum_i \sum_j (I_{(i,j)} - I'_{(i,j)})^2} \right] \quad (12)$$

where  $I(i, j)$ ,  $I'(i, j)$  denote the pixel gray values of the coordinates  $(i, j)$  in the original image and the watermarking, respectively;  $M$ ,  $N$  represent the image row and column numbers of pixels, respectively.

## IV. EXPERIMENTS

To verify the effectiveness of our proposed algorithm, we carried out the simulation in Matlab2010a platform. We choose a significant binary image as the original watermarking and select the tenth slice of one medical volume data as the original medical image. the original watermarking  $W = \{w(i, j) \mid w(i, j) = 0 \text{ or } 1; 1 \leq i \leq 32, 1 \leq j \leq 32\}$ . the original medical image  $F = \{f(i, j), 1 \leq i \leq 128, 1 \leq j \leq 128\}$ .

In the experiment, the parameter values: Arnold scrambling period is 24, and the number of transform times are 10, i.e.  $T=24, n=10$ .

Fig. 1 represents the results when a binary watermarking is scrambled by Arnold scrambling transform. Fig1 (a) was the original watermarking. Fig1 (b) was the scrambled watermarking when  $n$  equaled to eight. Fig1 (c) showed the restored watermarking.

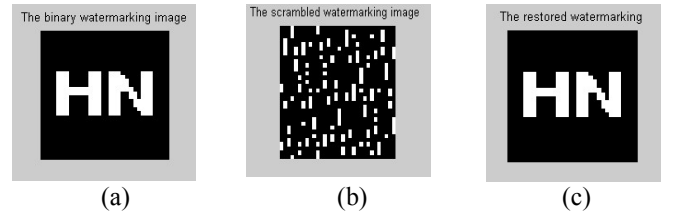


Figure 1. The watermarking is scrambled by Arnold scrambling transform. (a) the original watermarking. (b) the scrambled watermarking. (c) the restored watermarking.

In order to investigate this approach of embedding watermarking robust performance, I chose the following verification:

#### A. Common attacks.

##### 1) Adding Gaussian noise.

In the watermarked medical image, Gaussian noise is added by the `imnoise()` function with different noise level. The medical image under the attack of Gaussian noise (5%) with PSNR=5.92dB. At this time, the watermarked medical image has been very vague, as shown in Fig.2(a). The watermarking can obviously be extracted with NC=0.94. As shown in Fig. 2(b). The results prove that our proposed algorithm has strong robustness against noise attacks.

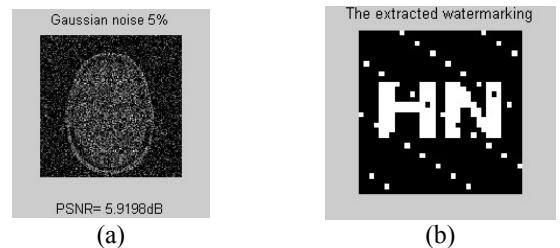


Figure 2. The watermarked medical image under Gaussian noise attacks(5%). (a) the watermarked medical image under noise attack. (b) the extracted watermarking

## 2) JPEG attacks.

JPEG compression process is done by using the percentage of image quality as a parameter to measure. The watermarked medical image with PSNR=17.61dB under JPEG attacks (4%) is shown in Fig. 3(a). the watermarking can obviously be extracted with NC=0.88. As shown in Fig. 3(b). The results show that the watermarking algorithm has strong robustness against JPEG attacks.

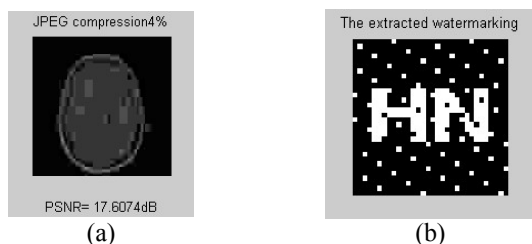


Figure 3. The watermarked medical image under JPEG attacks (4%). (a) the watermarked medical image under JPEG attacks. (b) the extracted watermarking..

## B. Geometrical attacks.

### 1) Scaling attacks.

We use the scaling factor as parameter to validate the effectiveness of our proposed algorithm on different scaling attacks. When the watermarked image is scaled 4 times, its pixel point has become a quarter of the original. The resolution has sent a lot of. Fig. 4(a) shows that the watermarked image shrunk with a scale factor of 4.0. Moreover, Fig. 4(b) shows that the watermarking can be extracted with NC=1.00. It proves that our proposed algorithm has strong robustness against scaling attacks.

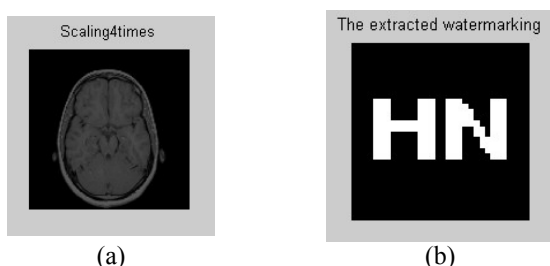


Figure 4. The watermarked medical image under scaling attacks. (4.0 times). (a) the watermarked medical image under scaling attacks. (b) the extracted watermarking.

### 4) Cropping attacks

The cropping attacks are added to the watermarked image for validating the effectiveness of our proposed algorithm. Fig. 5(a) shows that the medical image cropping from Y axis with the ratio of 6%. Moreover, Fig. 5(b) shows that the watermarking image can be extracted with NC=0.88. The results show that the watermarking algorithm has strong robustness against cropping attacks.

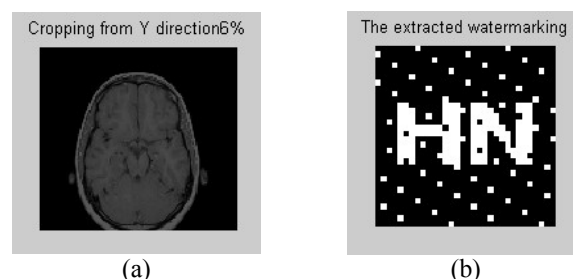


Figure 5. Under cropping attacks (From the Y axis, 6%). (a) an image with cropping attack. (b) the extracted watermarking image

## V. CONCLUSION

This paper presents a watermarking encryption algorithm based on Arnold scrambling and DFT for medical images, combing the visual feature vector of image, the encryption technology and the concept of third-party, and integrating Arnold scrambling. In watermarking embedding process, Arnold scrambling is employed to preprocess on the original watermarking. Without knowing the scrambling algorithm and key, the attackers can not recover the images even after extracting the watermarking from the watermarked image. Such additional encryption provides double protection for medical images. Our experiments show the proposed embedding watermarking scheme has robustness for common attacks and geometrical attacks while still keeping the quality of the original medical image. Moreover, the proposed watermarking algorithm can be applied to protecting the other area's images.

## ACKNOWLEDGEMENT

This work is supported by the National Natural Science Foundation of China (No:61263033) and the NSF of Hainan Province of China(60894).

## REFERENCES

- [1] X. Kong and R. Feng, "Watermarking medical signals for telemedicine , "IEEE Transactions on Information Technology in Biomedicine, v01. 5, no. 3, PP. 195—201, 2001.
- [2] S. Kaur, O. Farooq, R. Singhal, B. S. Ahuja, "Digital watermarking of ECG data for secure wireless communication," In Proceedings of the 2010 IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 140-144, March 2010.
- [3] K. A Navas and M. Sasikumar, "Survey of Medical Image Watermarking Algorithms," In Proceedings of the 4th Sciences of Electronic, Technologies of Information and Telecommunications International Conference, Tunisia, pp. 25-29, March 2007.
- [4] Y. X. Zhou, W. Jin, "A novel image zero-watermarking scheme based on DWT-SVD," In Proceedings of the 2010 IEEE International Conference on Multimedia Technology, pp. 2873-2876, Dec. 2009..
- [5] M. Unoki, R. Miyauchi, "Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics," In Proceedings of the 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 314-317, Oct. 2011.
- [6] E. F. Badran, M. A. Sharkas, O. A. Attallah, "Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images," In Proceedings of the 26th National Radio Science Conference ( NRSC 2009), pp. 1-8, March 2009.