The text image watermarking using arnold scrambling and DFT

Fan Wu, Jingbing Li*

College of Information Science and Technology Hainan University, Haikou, China

Received 1 October 2014, www.cmnt.lv

Abstract

With the popularization of Internet and the development at full speed of the multi-media technology, the copyright protection of digital works has already become the hot issue at present. Generally speaking, image, audio and video watermarking is comparatively similar in algorithm realization, with their redundancy, in which we can embed watermark. But other than the aforementioned, there is no redundancy to transfer secret info in text document. Nowadays, to embed watermark in text documents are limited to methods such as shifting the line and word, amending the characters' traits and disposing in the level of semantics. All these algorithms are not robust or lack of concealment, generally not serving the turn of Chinese text documents riffles. Based on the studies of the document digital watermarking methods and techniques, this dissertation presents that the problems of existed documents watermarking algorithms can be solved by Arnold Scrambling and DFT technique. The experimental results show that the scheme has strong robustness against common attacks and geometric attacks.

Keywords: Arnold scrambling, digital watermarking, DFT, zero-watermarking, text image

1 Introduction

With the rapid development of computer science and technology, and multimedia communication technology, digital media is becoming more and more universal. Digital watermarking is an important method for protecting digital media copyright. Most work focuses on audio, video, grayscale, and color images. However, binary images are very useful for security records, insurance information, financial document, fax images, case history, contract, e-business, e-Government, etc. Therefore, it may be very useful to embed and extract watermarking in binary images. For binary images, pixels take only two different values. Hence, embedding watermarking without causing visible perceivable changes in binary images is more difficult than in grayscale images. Brassial et al. proposed to change line spacing to embed the watermarking. Huang et al. presented a way to change word spacing to embed the watermarking. By changing a particular feature of an individual character can be embed with the watermarking. However there are some disadvantages to these watermarking approaches. The amount of data that can be hidden is few. The Process of embedding and extracting the watermarking is very complicated. Furthermore, these algorithms are vulnerable to many attacks, especially to geometric attacks.

This paper proposes an algorithm which combines DFT and Arnold scrambling. The algorithm combines both the first generation watermarking techniques and the second generation watermarking techniques. In the watermarking embedding process, firstly, the watermarking is encrypted by scrambling transformation technology, then the encrypted watermark information is embedded in the text of DFT transform image, to obtain a feature vector of the text image, then use the eigenvectors and watermarking information by HASH function to generate a binary logic series, as the sequence of keys. The result of experiment indicates that the algorithm can achieve a true embedded zero-watermarking. Meanwhile, it has a strong robustness against common attack and geometric attack.

2 The fundamental theory

2.1 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:

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

where 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

* ***Corresponding author*** e-mail: Jingbingli2008@hotmail.com

transform formula can be obtained:

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

$$x', y' = \{0,1,2...,N-1\}.$$

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.

2.2 A METHOD TO OBTAIN THE FEATURE VECTOR OF TEXT 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 1. 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 1. 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 1. 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 text image. Furthermore, it proves that the sequence of the DFT coefficient signs can reflect the main visual characteristics of text images.

TABLE 1 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		1.259	–0.006 + 0.005i	–0.022 + 0.017i	–0.034 + 0.010i	–0.045 + 0.009i	101010101	1.00
Gaussian interference (10%)	13.04	1.152	–0.005 + 0.002i	–0.017 + 0.010i	–0.026 + 0.006i	–0.035 + 0.007i	101010101	1.00
JPEG compression (10%)	17.71	1.219	0.002 + 0.006i	–0.016 + 0.019i	–0.030 + 0.012i	–0.044 + 0.012i	111010101	0.9
Median filter [3×3]	8.279	1.395	–0.035 – 0.001i	–0.046 + 0.006i	–0.047 – 0.001i	–0.048 + 0.001i	100010001	0.7
Rotation（clockwise, 5°）	6.319	1.250	–0.020 + 0.004i	–0.035 + 0.014i	–0.044 + 0.008i	–0.047 + 0.008i	101010101	1.00
Scaling(×0.5)		3.126	–0.011 + 0.014i	–0.054 + 0.042i	–0.085 + 0.023i	–0.113 + 0.020i	101010101	1.00
Translation (2% down)	7.389	1.259	–0.006 + 0.005i	–0.022 + 0.017i	–0.034 + 0.010i	–0.045 + 0.009i	101010101	1.00
Cropping (2%) (from Y direction)		1.259	–0.006 + 0.005i	–0.022 + 0.017i	–0.034 + 0.010i	–0.045 + 0.009i	101010101	1.00

DFT transform coefficient unit 1.0e+007

3 Robust watermarking algorithm based on digital text image

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

3.1 THE ALGORITHM OF THE EMBEDDED WATERMARKING

Step 1 Acquire the the encrypted watermarking image. The binary watermarking image is scrambled by Arnold scrambling transform, $BW(i, j)$.

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

Step 2 Acquire the feature vector of the original text 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 $V=\{v(j)|v(j) = 0 \text{ or } 1;\ 1 \le j \le L\}$, 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).

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

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

Step 3 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 text image, so as to achieve the purpose of the protection of text images.

3.2 THE ALGORITHM OF THE EXTRACTED WATERMARKING

Step 1 Acquire the feature vector of the tested image. This process of acquiring the feature vector $T\_V'(j)$ is same tostep1 of the watermarking embedding process. The obtained feature vector, $T\_V'(j) = \{t\_v(j)|t\_v(j) = 0 \text{ or } 1; 1 \le j \le L\}$, also consists of the signs sequence of the DFT coefficients, where L has the same meaning as previously.

$$FF'(i,j) = DFT2(F'(i,j)), \tag{7}$$

$$T\_V'(j) = -Sign(Y'(j)). \tag{8}$$

Step 2 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.

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

Step 3 Using the Arnold scrambling inverse transform to restore the extracted watermarking $BW'(i, j)$, get the watermarking of the being tested image, $W'(i, j)$.

$$W'(i,j) = IAT(BW'(i,j)). \tag{10}$$

3.3 DETECTION ALGORITHM OF THE WATERMARKING

Step 1 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:

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

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

Step 2 Evaluation of the quality of the text 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:

$$PSNR = 10 \lg \frac{MN \max_{i,j} (I(i,j))^2}{\sum_i \sum_j (I(i,j) - I'(i,j))^2}, \tag{12}$$

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.

4 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 a paragraph in an article as the original text image. The original watermarking $W = \{w(i, j)|w(i, j) = 0 \text{ or } 1; 1 \le i \le 32, 1 \le j \le 32\}$. The original text image $F = \{f(i, j), 1 \le i \le 128, 1 \le j \le 128\}$.

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.

Figure 1 represents the results when a binary watermarking is scrambled by Arnold scrambling transform. Figure 1a is the original watermarking. Figure 1b is the scrambled watermarking when n equaled to eight. Figure 1c shows the restored watermarking.

a) b) c)

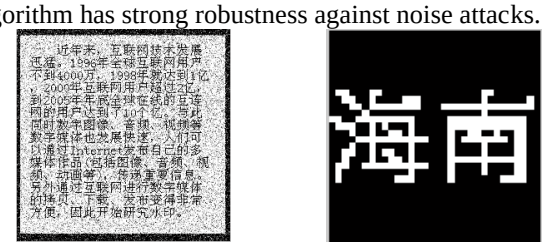
FIGURE 1 The watermarking is scrambled by Arnold scrambling transform: a) the original watermarking, b) the scrambled watermarking, c) the restored watermarking

In order to investigate this approach of embedding watermarking robust performance, the verification described below is chosen.

4.1 COMMON ATTACKS

4.1.1 Adding Gaussian noise.

In the watermarked text image, Gaussian noise is added by the noise function with different noise level. The text image under the attack of Gaussian noise (10%) with PSNR=12.96dB. At this time, the watermarked text image has been very vague, as shown in Figure 2a. The watermarking can obviously be extracted with NC=1.0. As shown in Figure 2b. The results prove that our proposed algorithm has strong robustness against noise attacks.



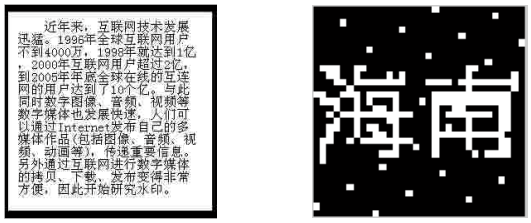
a) b)

FIGURE 2 The watermarked text image under Gaussian noise attacks (10%): a) the watermarked text image under noise attack, b) the extracted watermarking

4.1.2 JPEG attacks

JPEG compression process is done by using the percentage of image quality as a parameter to measure. The

watermarked text image with *PSNR* = 17.71dB under JPEG attacks (10%) is shown in Figure 3a. the watermarking can obviously be extracted with *NC* = 0.93 as shown in Figure 3b. The results show that the watermarking algorithm has strong robustness against JPEG attacks.



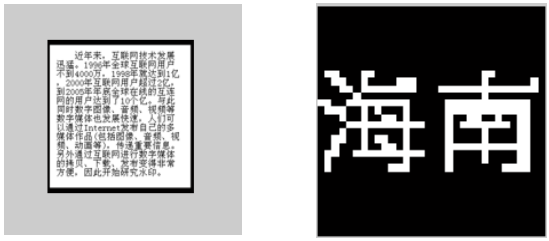
a) b)

FIGURE 3 The watermarked text image under JPEG attacks (10%): a) the watermarked text image under JPEG attacks, b) the extracted watermarking

4.2. GEOMETRICAL ATTACKS

4.2.1 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 0.5 times, its pixel point has become the double of the original. Figure 4a shows that the watermarked image shrunk with a scale factor of 0.5. Moreover, Figure 4b shows that the watermarking can be extracted with *NC* = 1.00. It proves that our proposed algorithm has strong robustness against scaling attacks.

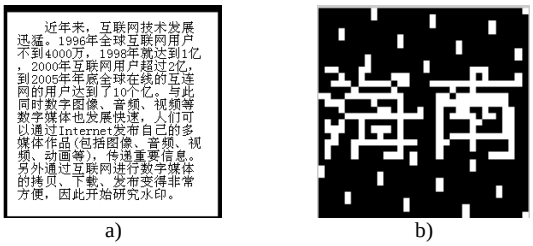


a) b)

FIGURE 4 The watermarked text image under scaling attacks: (0.5 times), a) the watermarked text image under scaling attacks, b) the extracted watermarking

4.2.2 Cropping attacks

The cropping attacks are added to the watermarked image for validating the effectiveness of our proposed algorithm. Figure 5a shows that the medical image cropping from *Y* axis with the ratio of 2%. Moreover, Figure 5b shows that the watermarking image can be extracted with *NC* = 0.87. The results show that the watermarking algorithm has strong robustness against cropping attacks.



a) b)

FIGURE 5 Under cropping attacks (from the *Y* axis, 2%): a) an image with cropping attack, b) the extracted watermarking image

5 Conclusion

This paper presents a watermarking encryption algorithm based on Arnold scrambling and DFT for text 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 cannot recover the images even after extracting the watermarking from the watermarked image. Such additional encryption provides double protection for text 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 text 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 (No: 60894).

References

[1] Pan J, Hiang H, Wang F 2002 A VQ-based multi-watermarking algorithm *Proceedings of 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering TENCON '02* **1** 117-20
[2] Solachidis V,Pitas I 2001 *IEEE Transactions on Image Processing* **10**(11) 1741-53
[3] Zhou Y, Jin W 2009 A novel image zero-watermarking scheme based on DWT-SVD *2011 International Conference on Multimedia Technology (IMCT)* 2873-6
[4] Niu X M, Lu Z M, Sun S H 200 Digital image watermarking based on multiresolution decomposition *Electronics Letters* **36** 1108-10
[5] Unoki M, Miyauchi R 2011 Reversible Watermarking for Digital Audio Based on Cochlear Delay Characteristics *Proceedings of the 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing* 314-7
[6] Kutter M, Bhattacharjee S K, Ebrahimi T 1999 Towards second generation watermarking schemes *ICIP'99* Kobe Japan **3** 320-3
[7] Kaur S, Farooq O, Singhal R, Ahuja B S 2010 Digital watermarking of ECG data for secure wireless communication *Proceedings of the 2010 IEEE International Conference on Recent Trends in Information, Telecommunication and Computing* 140-4
[8] Li X, He G 2012 Efficient Audio Zero-Watermarking Algorithm for Copyright Protection Based on BIC and DWCM Matrix *IJACT: International Journal of Advancements in Computing Technology* **4**(6) 109-17
[9] Zhang Y, Bi H, Zhu B, Dong B 2012 An Improved ICA-based Digital Watermarking *AISS: Advances in Information Sciences and Service Sciences* **4**(2) 167-74

Authors

Fan Wu, born in March, 1989, Haikou, China

University studies: Master's degree at Information Science & Technology College of Hainan University.
Scientific interests: digital watermarking technology.
Publications: 1 paper.

Jingbing Li, born in July, 1966, Haikou, China

Current position, grades: professor and doctoral supervisor at Hainan University.
University studies: PhD in control theory and control engineering at Chongqing University of China in 2007.
Scientific interests: medical image processing, artificial intelligence, digital watermarking, volume data.
Publications: 4 patents, 37 papers, 4 books.