Digital Watermarking Algorithm Based on Chaotic and Wavelet Transform

Wenhao Wang\textsuperscript{1,*}, and Zhenyang Yu\textsuperscript{1}

\textsuperscript{1}HuaiYin Institute of Technology, Huai'an city, Jiangsu 223003, China

Abstract. To protect the copyright of multimedia data effectively, the adaptive digital watermarking algorithm is presented in this paper, which based on chaotic sequence and two-dimensional wavelet transform. Firstly, a chaotic sequence generated by Logistic chaotic map is utilized to encrypt watermark image. Then the strength and position of watermark embedding are obtained by discrete wavelet transform of host image. Finally the encrypted watermark is embedded in the host image. The experimental results show this method has better effect: the watermark is invisibility and robust against common image. It can protect multimedia data effectively.

1 Introduction

With the rapid development and wide application of the multimedia technology and network technology, digital media has provided a fast, efficient and convenient way to access information. However, digital media can be easily copied illegally or suffered deliberate tampering during the transmission by the third party. Therefore, the security of the digital media has become increasingly prominent, which has become a very important and urgent issue during the dissemination of digital information [1].

The traditional security technology based on theory of cryptography has some limitations to the protection of multimedia content [2]. As the information of digital media is larger, the amount of encryption and decryption calculation will be very large; In addition, multimedia content is easy to copy and spread, thus restricting the application of digital multimedia. Digital watermarking technology opens up a whole new way for the safely stored and transferred of the multimedia data. At present, digital image watermarking algorithms are basically divided into two categories: one is the spatial domain method of adding watermark by directly changing the gray value of some pixels of the image, such as LSB, extended spectrum etc. [3]; the other is the transform domain method of adding watermark after making some transformation of the image, such as DCT (discrete cosine transform), DWT (discrete wavelet Transform) etc. [4]. In this paper, a digital watermark based on chaotic sequence in wavelet domain is proposed. The experimental results show that this method can effectively resist all kinds of attacks on image and has good robustness.
2 Correlation theories

2.1 Chaotic encryption

Chaos is a deterministic and random process in nonlinear dynamical system. This process is neither periodic nor convergent, and has a very sensitive dependence on the initial value [5]. In the time domain, the sequence obtained by chaotic mapping is similar to random sequence, with weak correlation and good white like noise characteristics, so they can be used to generate pseudo-random signals or pseudo-random codes. The simplest mapping is Logistic map, and it can be written as follows:

\[ x_{k+1} = u x_k (1 - x_k) \]  

The remarkable feature of logistic function is its simplicity and dynamic complexity. when \( 3.5699456\ldots<u<4 \) , Logistic function will work in the chaotic state, the generated sequence \( \{ x_k : k=0,1,2,3\ldots \} \) is non-periodic and non-convergent.

Suppose the image size is \( M \times M \), \( Image(i, j) \) represents the gray value of the pixel \( p(i, j) \), where \( 1 \leq i \leq M, 1 \leq j \leq N \), \( EncImage(i, j) \) is the encrypted image. An encryption algorithm is to design a mapping function \( f \), which make \( f: Image(i, j) \rightarrow EncImage(i, j) \). The encryption scheme proposed in this paper as shown in Fig. 1.

\[ Figure 1. Flow diagram of encryption. \]

2.2 Discrete wavelet transform

The wavelet transform of function \( f(t) \) is defined as:

\[ W_{\psi}f(a, b) = \frac{1}{2} \int_{-\infty}^{\infty} f(t) \psi\left(\frac{t-a}{b}\right) dt \quad a, b \in R, a \neq 0 \]

An original image is transformed into four sub images by one-level wavelet transform: low-frequency component LL, intermediate-frequency component HL and LH and high-frequency component HH. Where low-frequency LL contains the most energy and basic characteristics of the original image. The intermediate and high frequency have less energy, which mainly contains the detail characteristics of the original image. If the low-frequency image LL is decomposed by wavelet, four sub-band images with lower resolution can be obtained. The second-level wavelet decompose of the image is shown as Fig.2.
The low-frequency area contains the basic features of the image. If embedding watermark in low-frequency can well resist the noise attacks, compression attacks and so on, but poor invisibility. The high-frequency area mainly represents on the detain portion of the image. If the watermark is embedded in the high frequency band, the invisibility of the algorithm is better, but the robustness of the algorithm is poor. So the watermark is embedded in the intermediate-frequency area band in this paper.

The stronger the image texture is, the stronger the watermark can be embedded. As the high frequency coefficients of wavelet transform reflect the texture and edge information of the image, the larger the high frequency coefficients are, the stronger the texture is. So, the strength of texture can be measured by whether the absolute value of high frequency coefficient in the sub-image is greater than a certain threshold $T$. Assume that $I_{HH,L}$ represents its high-frequency coefficient of L-level wavelet decomposition of image, then the threshold $T$ is determined by the following formula:

$$T = \frac{\max(\text{abs}(I_{HH,L}(i,j)))}{2}$$  \hspace{1cm} (3)

If $|I_{HH,L}| \geq T$, the coefficients of this positions are important coefficients. Otherwise, the coefficient of the position is not important.

### 3 Digital watermarking algorithms

The digital watermarking algorithm in this paper is shown in Fig.3. Firstly, The watermark image is scrambled by chaos algorithm to get one-dimensional watermark sequence. Then the host image is decomposed by L-level wavelet, and the embedding strength is determined according to the high-frequency component of wavelet, and the watermark is embedded in the bigger intermediate-frequency coefficients. Finally, the image with watermark can be obtained by inverse wavelet transform.
Assume that the original image \( I \) is grayscale, which size is \( M \times M \), watermark image is \( W \), which size is \( N \times N \). Watermarking algorithm is described as follows:

1. The original image \( I \) was decomposed by \( L \)-level wavelet, which \( L = M / N \), \( I_k(i,j) \) represents the \( k \)-th sub-image, \( k \in \{ LL, LH, HL, HH \} \).

2. The watermark image \( W \) is encrypted by chaotic sequence, and the encrypted watermark image is represented by \( W' \).

3. Select the bigger intermediate-frequencies from \( I_{HL}(i,j) \) and \( I_{HL}(i,j) \). Without losing generality, assuming that \( I_{HL}(i,j) \) is the bigger one. The threshold \( T \) is calculated according to equation (3), \( I_{HL}(i,j) \) is classified as important coefficient and unimportant coefficient according to threshold \( T \). An auxiliary matrix \( norm(i,j) \) is defined, \( norm(i,j) = 1 \) for important coefficient, and \( norm(i,j) = 0 \) for unimportant coefficient.

4. The watermark is embedded according to the following equation

\[ I'_{HL}(i,j) = I_{HL}(i,j) + a \ast W'(i,j) \]  

where \( a \) represents the embedding strength, \( a \) value is adaptively selected according to high-frequency coefficient. For the important coefficient \( a = 40 \); other \( a = 20 \).

5. The embedded image \( W \) is obtained by \( L \)-level wavelet inverse transform. Before embedding the watermark, chaotic sequence is used to encrypt the watermark image, which can enhance the security of watermark image.

The process of watermark extraction is the reverse of watermark embedding.

4 Experimental results and analysis

4.1 Experiment of chaotic encryption

The chaotic encryption was tested on a plenty of images, Fig.4 (a) is a Lena original image to be encrypted. The parameters of the algorithm are set as follows \( u1 = 3.7 \), \( x1 = 0.4 \), \( u2 = 3.88 \), \( x2 = 0.8 \). Fig.4 (b) is the result of encrypting the original image, From Fig.4 (b), we can’t see any information of the original image at all, which achieve the effect of visual encryption. Fig.4 (c) is the result of decryption, almost the same as the original image. Fig.4 (d) is the decryption image when \( u1 = 3.7000001 \), \( x1 = 0.4 \), \( u2 = 3.88 \), \( x2 = 0.8 \). By the experiment, it is clear that the key is slightly different, it cannot be decrypted.

(a) Original image (b) Chaotic Encrypted (c) Correctly decrypted (d) Error decrypted

Figure 4. Encryption and decryption test results.

4.2 Experiment of watermarking algorithms

In this experiment, the host image is Lena image which size is \( 512 \times 512 \), the watermark image is a binary image which size is \( 64 \times 64 \). The watermark is embedded and extracted as shown in Fig.5. Because the algorithm in this paper fully considers the characteristics of human vision, it is difficult to distinguish the difference between the host image and the embedded image, and the extracted watermark has a good visual effect.
In order to detect the anti-attack effect of the algorithm, the attack experiment of embedded watermark image is carried out. The experimental results are as follows:

| No. | Attack type          | Watermark ed image | Watermark |
|-----|----------------------|--------------------|-----------|
| 1   | High pass filter     | HYJS               | HYJS      |
| 2   | Mean filtering       | HYJS               | HYJS      |
| 3   | salt and pepper noise(0.01) | HYJS   | HYJS      |
| 4   | Gauss noise          | HYJS               | HYJS      |
| 5   | reduce size          | HYJS               | HYJS      |

From the series of attacks of above experimental results, the digital watermark algorithm proposed in this paper has strong robustness. The extracted watermark image and the original watermark image are also good similarity.

This paper was supported by the Jiangsu province industry-university-research cooperation project under Grant DH20190167. The authors would like to thank the anonymous reviewers and the editors for their many helpful suggestions.

References

1. Zhang, H., Wang, C., & Zhou, X. A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain. Future Internet, 9(3) (2017).
2. Wenhao Wang. Adaptive Watermarking Algorithm in DCT Domain Based on Chaos. Sensors & Transducers, 21(5): 153-158(2013).

3. Zhou, R., Hu, W., & Fan, P. Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Information Processing, 16(9) (2017).

4. Mehto, A., & Mehra, N. Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT. Procedia Computer Science, 78, 88-94 (2016).

5. Bahi, J. M., & Guyeux, C. A new chaos-based watermarking algorithm. arXiv: Multimedia, (2015).