A Blind Watermarking Algorithm for Intangible Cultural Heritage Protection Based On DWT-DCT

Yanfang Hu[1]
[1] College of Information Science and Technology,
Hainan University, China,
763941952@qq.com

Jingbing Li*[2]
[2] College of Information Science and Technology,
Hainan University, China,
Jingbingli2008@hotmail.com

Mengxing Huang[3]
[3] College of Information Science and Technology,
Hainan University, China,
huangmx09@163.com

Abstract—Intangible cultural heritage is an important symbol to recognition different ethnics. In order to enhance the copyright protection and authentication of intangible cultural heritage, this paper presents a novel way to process the carried image that Li brocade. Firstly, Li brocade image was decomposed into a new image that has four different components of low frequency, horizontal, vertical and diagonal image features though DWT transformation, then the low frequency component was processed by the whole DCT transform to eliminate coefficient correlation for obtaining an image, which was well suitable for the human visual system. Secondly, employing the bit operation of Hash function (OR), between the encrypted watermarking and visual feature vector, to realize the watermarking embedding and protect some information. Finally, the watermarking image is extracted by blind watermarking algorithm. The simulation results show this method not only has ultra-robustness and imperceptivity, but also can resist greater geometrical attack than others, thus, it has better application value in protecting the copyright of Intangible Cultural Heritage.

Keywords-intangible cultural heritage; Li brocade; blind watermarking; DWT-DCT; ultra-robustness

I. INTRODUCTION

Intangible cultural heritage is a form to express the national culture, and an important symbol to recognition different ethnics [1]. Currently, its styles are declining, and the skills are facing dangerous, thus it is difficult to inheritance the ethnic culture.

Hainan Li brocade culture is a part of intangible cultural heritage, it is very precious for Li people, because the people don't have text, and textile activity has become the main way to record their lives, therefore, the Li brocade has become intangible cultural heritage for them [2].

Digital watermarking is one of the key methods in protecting information security. It can embed private information into the media data without affecting the original data in order to achieve the copyright certification and to meet robustness and invisibility [3] [4]. In addition, it also has high security that a person who is an unauthorized client can't detect the presence of the watermarking. Therefore digital watermarking is needed.

This paper takes the Li brocade image as an example to study intangible cultural heritage protection adopting blind watermarking algorithm. The experiments show that the algorithm has strong ability in resisting common attacks and geometric attacks.

II. THE FUNDAMENTAL THEORY

A. The Discrete Wavelet Transform

The wavelet transform, is a new signal analysis theory and a "time-frequency" method. The basic idea is to decompose the sign $f(t)$ based on wavelet function, $\psi_{a,b}(t)$.

$$W_{f(a,b)} = \int_R f(t)\overline{\psi}_{a,b}(t)dt \tag{1}$$

Where, wavelet function$\psi_{a,b}(t)$is a set of functions, which are obtained by translating and stretching of the same base function$\psi_{a,b}(t)$.

$$\psi_{a,b}(t) = |a|^{-1/2}\psi((t-b)/a) \quad a,b\in R, a\neq 0 \tag{2}$$

Where, the basic wavelet is ψ , a and b are the dilation factor and the translation factor, respectively. The decomposing equation of Mallat algorithm is defined as follows:

$$c_{j+1,k} = \sum_{n\in z} c_{j,n}\overline{h}_{n-2k} \qquad k\in R \tag{3}$$

$$d_{j+1,k} = \sum_{n\in z} c_{j,n}\overline{g}_{n-2k} \qquad k\in z \tag{4}$$

The reconstruction equation of the Mallat algorithm is given by:

$$c_{j,k}=\sum_{n\in z} c_{j+1,n}h_{k-2n}+\sum_{n\in z} d_{j+1,n}g_{k-2n} \quad k\in z \tag{5}$$

The original Li brocade image can be decomposed into four sub-bands called three high frequency detail sub-bands, including LH1、HL1、HH1、and a low frequency sub-band LL1. The marginal information of original image exists in high frequency detail sub-bands. However, the external interference can affect it. In addition, the low frequency sub-band not only includes the image's basic information, but also it can against some attacks [5][6]. Therefore, the watermarking, which is embedded in low frequency sub-band, can provide better robustness than others.

B. The Discrete Cosine Transform

DCT transform is compatible with international data compression standard and is used by over the world. It is well known for the best balance between operation speed and high precision of extracting the feature vector [7] [8]. The M×N Li brocade image's DCT transform is defined by:

$$F(u,v)=c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{6}$$

$$u=0,1...,M-1; v=0,1,...,N-1$$

$$c(u)=\begin{cases}\sqrt{1/M} & u=0\\ \sqrt{2/M} & u=1,2,...,M-1\end{cases} \qquad c(v)=\begin{cases}\sqrt{1/N} & v=0\\ \sqrt{2/N} & v=1,2,...,N-1\end{cases}$$

Where *x*, *y* is sampled value in the spatial domain sampling and *u*, *v* is the one in frequency domain. Usually digital image is expressed by pixels square, namely M=N.

III. THE ALGORITHM

The significant binary image is described as $W=\{w(i,j)\,|\,w(i,j)=0 or 1;1\le i\le M1,1\le j\le M2\}$. At the same time, we select a gray image as the original Li brocade image. It is described as $F=\{f(i,j)\,|\,f(i,j)\in R,1\le i\le N1,1\le j\le N2\}$. To facilitate the operation, we assume M1=M2=M, N1=N2= N.

A. A algorithm to obtain the feature vector of Li brocade image

Firstly, DWT is applied to the original Li brocade image to obtain the approximated sub-band LL1. Then, DCT of the whole LL1 is computed and the DCT coefficient matrix is acquired. We choose 10 low-frequency DWT-DCT coefficients (F (1, 1), F (1, 2), F (1, 10)) to constitute the feature vector, which is shown in the following Table 1. Where "1" represents a positive or zero coefficients, and "0" represents a negative coefficient, then to obtain the sign sequence of low-frequency coefficients. It can be seen that the sign sequence is unchanged after attacking, and the normalized cross-correlation (NC) is equal to 1.00, as shown in the column "NC".

TABLE Ⅰ. CHANCE OF LOW-FREQUENCY COEFFICIENTS WITH RESPECT TO DIFFERENT ATTACK STYLES

Image processing	F(1,1)	F(1,2)	F(1,3)	F(1,4)	F(1,5)	F(1,6)	F(1,7)	F(1,8)	F(1,9)	F(1,10)	Sequence of signs	NC
Original image	1.95	-0.18	-0.40	0.05	-0.29	0.03	-0.30	-0.01	-0.31	0.05	1001010001	1.00
Gaussian noise (4%)	2.13	-0.17	-0.32	0.06	-0.23	0.03	-0.23	-0.01	-0.26	0.05	1001010001	1.00
JPEG compression (5%)	1.20	-0.18	-0.37	0.06	-0.26	0.04	-0.27	-0.01	-0.28	0.04	1001010001	1.00
Median filter [3×3]	1.93	-0.18	-0.40	0.05	-0.29	0.03	-0.29	-0.01	-0.31	0.05	1001010001	1.00
Rotation (1.5 °)	1.95	-0.18	-0.40	0.06	-0.29	0.03	-0.28	-0.01	-0.30	0.06	1001010001	1.00
Scaling (×4)	7.79	-0.73	-1.59	0.22	-1.14	0.13	-1.18	-0.03	-1.22	0.20	1001010001	1.00
Translation (3%)	1.95	-0.22	-0.39	0.02	-0.28	0.01	-0.29	-0.02	-0.29	0.07	1001010001	1.00
Cropping (3% from X)	1.98	-0.29	-0.29	0.04	-0.20	0.06	-0.22	-0.09	-0.24	0.04	1001010001	1.00

The unit of transform coefficients is 1.0e+004 *

B. Watermarking encryption algorithm

In this experiment, we take 64×64 binary image W as watermark image, and 289×289 gray image of Li brocade as carrier. The method to embed watermarking is showed as the following:

- Step1: Generate the chaotic sequences.
  The chaotic sequences X (j) were generated by the initial values x0. But it is one-dimension sequence. In order to match the two-dimension watermarking image, we need get two-dimensional matrix through liter-dimension operation. Finally, the binary encrypted matrix $C(i,j)=\{c(i,j)=0 or 1;1\le i\le M1,1\le j\le M2\}$, can be achieved as the chaotic sequences $X(j)$ by symbolic computation. Where the value of $X(j)$ is more than 0.5, we noted as "1"; or we noted as "0".
- Step2: Acquire the encrypted watermarking image.
  We can generate the encrypted watermarking image as follows:

$$BW(i,j)=W(i,j)\oplus C(i,j)$$

Where, $BW(i, j)$ denotes the encryption watermarking image, $W(i, j)$ denotes the binary watermarking image, $C(i, j)$ denotes the binary encrypted matrix.

The initial value, x0, is regard as the private key. Even if the algorithm is public, the original watermarking image cannot be recovered without the private key [9]-[11].

C. Watermarking embedding algorithm

- Step1: Acquire a robust feature vector of the original Li brocade image using DWT-DCT.

  Firstly, DWT is used to decompose the original Li brocade image $F(i, j)$, to get approximated sub-band coefficient matrix $FA(i, j)$. Then, DCT of the whole approximated sub-band, we can get the DWT-DCT coefficients matrix $FD(i, j)$. Then, after arranging the DWT-DCT coefficients from low to high frequency, the low-frequency sequence $Y(j)$ can be acquired. Finally, the feature vector $V(j)$ can be obtained as a sign sequence of the top L values in the low-frequency sequence by symbolic computation. In this paper, we set L=32bits.

  The process can be described as follows:

$$FA(i, j) = DWT2(F(i, j))$$

$$FD(i, j) = DCT2(FA(i, j))$$

$$Y(j) = Zig - Zag(FD(i, j))$$

$$V(j) = Sign(Y(j))$$

- Step2: Acquire the key sequence.

  By utilizing the encrypted watermarking and the feature vector, we can generate the public key sequence as follows:

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

Where $V(j)$ denotes the feature vector of the original Li brocade image, $BW(i, j)$ denotes the encrypted watermarking image. 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 as a key and registered to the third part to preserve the ownership of the original image[12] [13].

D. Watermarking extracting algorithm.

- Step1: Acquire the feature vector of the tested image.

  This process of acquiring the feature vector of the tested image is same to step1 of the watermarking embedding process.

$$FA'(i, j) = DWT2(F'(i, j))$$

$$FD'(i, j) = DCT2(FA'(i, j))$$

$$Y'(j) = Zig - Zag(FD'(i, j))$$

$$V'(j) = Sign(Y'(j))$$

Where $F'(i, j)$ denotes the tested image, $FD'(i, j)$ denotes the DWT-DCT coefficient matrix. $V'(i, j)$, denotes the feature vector of the tested image.

- Step2: Extract watermarking.

  The watermarking image $BW'(i, j)$ can be extracted as follows:

$$BW'(i, j) = key(i, j) \oplus V'(j)$$

E. Watermarking detection algorithm.

The Normalized Cross-correlation (NC) is used for measuring the quantitative similarity between the extracted and embedded watermarking, which is defined as:

$$NC = \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_i \sum_j W^2(i,j)} \quad (7)$$

Where W denotes the embedded original watermarking and W' denotes the extracted original watermarking [14].

The higher the NC value, the more similarity there is between the embedded and extracted original watermarking.

The Peak Signal to Noise Ratio (PSNR) is used for measuring the distortion of the watermarked image, which is defined as:

$$PSNR = 10\lg \left[\frac{MN \max_{i,j} \left(\mathrm{I}(i,j) \right)^2}{\sum_i \sum_j \left(\mathrm{I}(i,j) - \mathrm{I}'(i,j) \right)^2} \right] \quad (8)$$

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

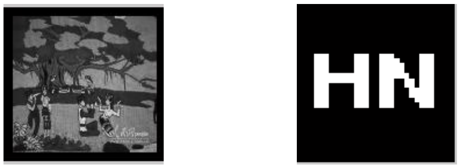
IV. EXPERIMENTS

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 image and select a gray image regard as the original Li brocade image. Fig .1(b) shows the original binary watermarking $W = \{w(i, j) = 0 or 1; 1 \le i \le 64, 1 \le j \le 64\}$. Fig .1(a) shows the original Li brocade image $F = \{f(i, j); 1 \le i \le 289, 1 \le j \le 289\}$.

In the experiment, the parameter values: The initial value is 0.2, another parameter of Logistic map is 4, and the number of chaotic system is 64, X0=0.2, u=4, k=64.

It can be seen visually from Fig .1 that the quality of the Li brocade image embedded has hardly any change.

The quality of extracted watermarking is of high-quality with no difference with the original in normal case (no attacking on watermarking).



(a) (b)

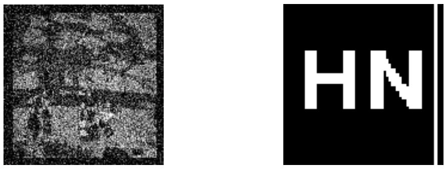
Figure 1. The watermarked Li brocade image without attacks: (a) the original Li brocade image; (b) the original binary watermarking.

The followings are several types of common and geometrical attacks to test the robustness of the algorithm.

A. Common attacks

1) Gaussian noise

In the watermarked image, Gaussian noise is added by the impose function with different noise intensity. The Li brocade image under the attack of Gaussian noise (4%) with PSNR=14.99dB is shown in Fig .2(a). As shown in Fig .2(b), the watermarking image can be extracted with NC=0.98. The results prove that our proposed algorithm has strong robustness against noise attacks.

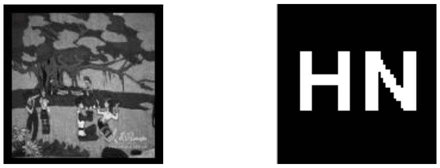


(a) (b)

Figure 2. Watermarked image attacked by Gaussian noise (4%): (a) the image with Gaussian noise; (b) the extracted watermarking image.

2) Median filter

After using [3x3] median filer and repeating the process twice, the edge of encrypted Li brocade image is a little fuzzy, and the PSNR value is equal to 31.88dB which is shown in Fig .3(a). As shown in Fig .3(b), the watermarking image can be extracted and NC=1. The results show that the watermarking algorithm has strong robustness against median filter.



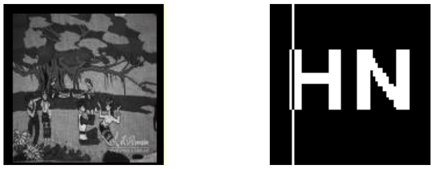
(a) (b)

Figure 3. Median filter ([3x3], repeating time=2): (a) image after median filter; (b) the extracted watermarking image.

B. Geometrical attacks

1) Scaling attacks

Fig .4(a) shows the Li brocade image is down by scaling and the scaling factor is 4, the PSNR after attacking Li brocade image is 18.92dB. Fig .4(b) shows that the watermarking can be extracted and NC=0.95. The results show that the watermarking algorithm has strong robustness against scaling attacks.

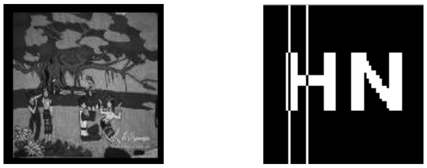


(a) (b)

Figure 4. Scaling down test (scaling factor is 4): (a) watermarked image scaled down; (b) the extracted watermarking image.

2) Translation attacks

In this experiment, we make the watermarked image horizontal translation and the distance is 30pixeis. Fig .5(a) and 5(b) show that the PSNR=20.36 and NC=0.93 respectively. The results show that the watermarking algorithm has strong robustness against translation attacks.



(a) (b)

Figure 5. Horizontal translation (distance is 30 pixels): (a) an image with translation attack; (b) the extracted watermarking image.

V. CONCLUSION

The paper uses digital watermarking technology to enhance copyright protection of Hainan Li brocade image for promoting the inheritance for intangible cultural heritage, Experiments show that its robustness resulted from digital watermarking technology is better than DWT or DCT algorithm alone after applying the same attacks, it is more fast and simple than others. In addition, it can be used to improve the PSNR and is enable to blind extraction.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (No: 61263033) 、 the NSF of Hainan Province of China (No: 60894)、the Institutions of Higher Learning Scientific Research Special Project of Hainan Province(Hnkyzx2014-2) and the International Science and Technology Cooperation Project of Hainan (KJHZ2014-16).

REFERENCES

[1] LI Jun."Digital-protection of Tujia minority brocade heritage,"Journal of Jinan University(Natural Science), Vol.32 No.5Oct. 2011.

[2] Liang, H. Y., Cheng, C. H., Yang, C. Y. & Zhang, K. F. “ A Blind Data Hiding Technique with Error Correction Abilities and a High

Embedding Payload". Journal of Applied Research and Technology, 11, 259-271.2013.

[3] 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.

[4] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications, Vol. 5 No. 1, January, 2011

[5] M. J. Sahraee, S. Ghofrani. "A robust blind watermarking method using quantization of distance between wavelet coefficients". Signal, Image and Video Processing, 2013, 7(4).

[6] Yu-Guang Yang, Xin Jia."Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform". Quantum Information Processing, 2013, 12(8).

[7] B. Y., Soon, I. Y., & Li, Z. "Blind and robust audio watermarking scheme based on SVD–DCT. Signal Processing", 91(8), 1973–1984.2011.

[8] Tai-yue Wang , Hong-wei Li. "A Novel Robust Color Image Digital Watermarking Algorithm Based on Discrete Cosine Transfor ".Journal of Computers, 2013, Vol.8 (10), pp.2507-2511Academy.

[9] Yuling Liu, Ting Jiang. "A robust text zero-watermarking algorithm based on dependency parsing". Advances in Information Sciences and Service Sciences, 2013, 5(1): 78-81.

[10] Xueming Li, Guangjun He, "Efficient Audio Zero-Watermarking Algorithm for Copyright Protection Based on BIC and DWCM Matrix", IJACT, Vol. 4, No. 6, pp. 109 ~ 117, 2012.

[11] M.Sabery.K, M.Yaghoobi, "A New Approach for Image Encryption using Chaotic Logistic Map," In Proceeding of 2008 International Conference of the IEEE on Advanced Computer Theory and Engineering, pp. 585-590, 2008.

[12] Zhang, Q., Li, Y., & Wei, X.. "An Improved Robust and Adaptive Watermarking Algorithm Based on DCT ", Journal Of Applied Research And Technology, 10(3), 405-415.2012

[13] K. Okagaki, K. Takahashi, H. Ueda. "Robustness Evaluation of Digital Watermarking Based on Discrete Wavelet Transform ". In Proceedings of 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010, pp. 114-117.

[14] G. T. Oh, Y. B. Lee, M. S. Jung, S. J. Yeom. "Design of a Robust Watermarking Algorithm against the Geometric Distortion for Medical Image Security ". In Proceedings of Second International Conference on Future Generation Communication and Networking Symposiac, 2009, 3: 167-170.