International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol. 10, No. 5 (2017), pp.143-156
http://dx.doi.org/10.14257/ijsip.2017.10.5.12

Research on Improved Digital Watermark Algorithm Based on QR Code

Yuanmei Wang[1] and Tao Li[2]*

School of Electronics and Information, Yangtze University, Jingzhou, China
[1]yuanyzq@163.com, [2]taohust2008@163.com

Abstract

Aiming at the problem that the digital watermark is vulnerable to be attacked, a digital watermark algorithm based on QR code is proposed in this paper. Firstly, encoding the text information to QR code as digital watermark, then host image is decomposed by discrete wavelet transform, and then the low-frequency sub-band have singular value decomposition, and the watermark information is embedded into the image. The experimental results show that the proposed method can resist the common attacks such as rotation, shearing, noise and so on, and it also has a good robustness to the change of histogram equalization and contrast ratio. QR code watermark is scrambled, which not only increases the anti-attack of digital watermark, but also make the watermark image to carry more information and has confidentiality, so digital watermark technology can be widely applied in the copyright protection for digital products.

Keywords*: digital watermark; discrete wavelet transform; chaotic scramble; QR code; singular value decomposition; robustness*

1. Introduction

In recent years, with the vigorous development of the Internet and digital storage technology, digital information technology is increasingly applied in all fields in our daily life, images in daily communication and dissemination of information becomes more and more convenient and quick. How to effectively protect the copyright of digital content has become a research hotspot. Digital watermark technology [1-4] make use of the data inherent redundancy of digital signal and unknown sense of identity of human sense organs, through a certain algorithm identified information is hided in digital images, video, audio and other digital products, and it does not affect the use of the original image, which is a new information security technology with the information not easily be discovered and modified. This technology can realize the protection of property right and tamper identification of digital products. Two- dimensional bar code technology is a standard of information storage and automatic identification technology based on computer image processing technique and coding theory, which is widely applied for the characteristic of the large information capacity, a wide coding range, strong error correcting ability, certain anti-fake ability. QR code is a matrix two-dimensional code, it not only has the advantages of a one-dimensional bar code and other two-dimensional bar code, also has super high speed full range reading and effectively express the Chinese word. On this basis, the author puts forward “rapid response matrix, QR codes” as digital watermark, applying the idea of digital watermark technology to improve the application of two-dimensional bar code in the field of anti-counterfeiting to improve the application of two-dimensional bar code in the field of anti-counterfeiting depth and breadth, which enhances the robustness of watermark technology. The algorithm is simple with small

*Corresponding author. Tel.: +86-716-8060625
E-mail address: yuanyzq@163.com (T. Li).

ISSN: 2005-4254 IJSIP

amount of calculation and less impact on image quality, which has very strong practicability.

2 Analysis of Algorithm

2.1. QR Code Watermark

QR code [5-8] is matrix two-dimensional bar code symbols which was developed by Japan Denso Company in September 1994, which has the advantages of large information, high reliability, high speed full range reading, effectively express Chinese characters etc. Compared with the common watermark image, QR code has the performance of selectable error correction, belonging to the error correction coding [9-10]. Though the QR code has a certain degree local damage, as long as the scope of the loss within its error correction ability, it can still be correctly decoded. For example, in the process of recognition, although 50% image is defaced, it can still recover the original image. Combined with the characteristics of QR code, it can be used in the field of digital watermark, which can enhance the robustness of the watermark. Figure 1 is the original QR code image generated by the text information "Yangtze University".

Figure 1. The Original QR Code

2.2. Logistic Chaos Mapping

As Chaos is a kind of deterministic stochastic process phenomena appearing in the nonlinear dynamic system, which is sensitive to the initial value with no-cycle or no-convergence. Logistic mapping [11-13] is very simple so it is widely used in classical chaotic mapping, which is defined as follows as Eq.1:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

$0 \le \mu \le 4, \mu$ as the branch parameter, $x_n \in (0,1)$, $when\, 3.5699456 \le \mu \le 4$, Logistic mapping works in the state of chaos.

The advantages of using mapping for image processing are as follows:

1. The form is simple: only needing a given branch parameters and initial value k, $k \in [0,1]$, then you can get a pseudo-random sequence.

2 Sensitive to initial value: even if the initial value has a small change, the result sequence is completely different.

3. It has statistical properties of white noise.

4. Certainty: only the branch parameter and the initial value are all same, then can get the same system.

So the setting parameters and initial value can be used as the key to encrypt the image, which makes the image more confidential.

2.3. Discrete Wavelet Transform

The basic idea of 2-D wavelet transform is multi-resolution of discrete wavelet transform (DWT). After DWT [14-16], the image will be decomposed into a series of different frequency sub-band images, then processing the sub image. The image has wavelet decomposition as Figure 2.

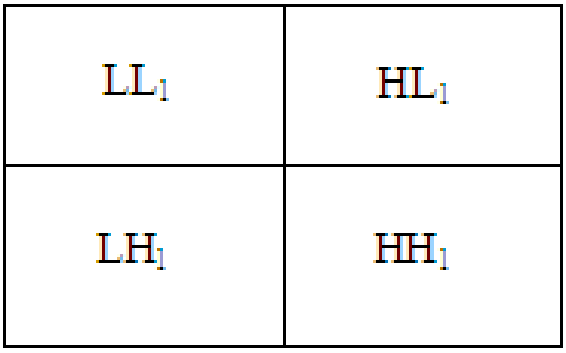

Figure 2. Image Decomposition by DWT

After one level discrete wavelet decomposition, the image is decomposed into four frequency bands: LL_1 (low frequency), LH_1 (intermediate frequency), HL_1 (intermediate frequency), HH_1 (high frequency). Image energy is mainly concentrated in the low frequency after discrete wavelet decomposition which is the most important part for human vision; the energy of the high frequency part is very little which mainly included the edge and texture of image. The basic idea of the digital watermark algorithm based on discrete wavelet transform is to embed the watermark into the frequency band coefficients of the image after discrete wavelet transform. If watermark is embedded in the low frequency sub-band, although watermark has better robustness, as the low frequency sub-band image contains most of the information, the low frequency sub-band image changes a little then it easily lead to larger image distortion. If watermark is embedded in the high frequency sub-band, although it can avoid image distortion, the robustness of watermark is relatively poor, watermark is easy to be attacked such as image loss compression. Therefore, a good digital watermark algorithm in discrete wavelet transform field must balance the robustness of the watermark image and the distortion of the image.

2.4. Singular Value Decomposition

Singular value decomposition (SVD) [17-19] is an important tool of linear algebra, it is the earliest applied in orthogonal matrix by Beltrami and Jordan. It was as a kind of complex calculation numerical tool later. SVD is applied in image compression, watermark technology and other signal processing fields. From the perspective of linear algebra, a digital image may be regarded as many matrixes made up nonnegative scalar. Therefore, all the matrix processing technology can be applied in image processing to achieve the rapid processing of image data.

Setting matrix $A \in R^{m \times n}$,for the matrix is positive semi-definite, negative square root of the characteristic value is called singular value of matrix A, which is denoted as $\sigma_1 \geq \sigma_2 \geq \mathrm{L} \geq \sigma_n \geq 0$,,setting $\sigma(A)$ express all singular value of matrix A as Eq.2

$$\sigma(A)=\left\{\sigma\geq 0: A\times Ax=\sigma^2 x, x\in R^{m\times n}, x\neq 0\right\} \tag{2}$$

Singular value decomposition is a kind of orthogonal transformation. It can be diagonalization of matrix. Setting matrix $A\in R^{m\times n}$ having orthogonal matrix, $U=[u_1,u_2,\text{L},u_m]\in R^{m\times n}$, $V=[v_1,v_2,\text{L},v_n]\in R^{m\times n}$, then $U^TAV=diag(s_1,s_2,\text{L}\ s_p)=S$,because U and V are orthogonal, then $A=USV^T$. Among them $p=\min\{m,n\}$, s_i as the singular value of matrix A, $\sigma_1\geq\sigma_2\geq\text{L}\geq\sigma_p\geq 0; u_i, v_i$ are called the left and right singular vectors respectively, satisfied with $Av_i=\sigma_i u_i, Au_i=\sigma_i v_i, i=1,2,\text{L},p;$ U and V are the characteristic vector of AA^T and A^TA, so the $A=USV^T$ as the SVD of A.

Due to the singular value reflects not only the visual characteristics but intrinsic characteristics of the image, which is the relationship among matrix elements. Based on some properties of singular value decomposition, though the image is subject to minor disturbances, singular value does not produce obvious change, so watermark algorithm based on singular value decomposition (SVD) has good the robustness.

3 Watermark Embedding and Extraction

3.1 Generate QR Code Watermark and Watermark Scrambling Processing

According to the relevant regulations of GB /T1824-2000, the text information "Yangtze University" as identification information rights is encoded to QR code as shown in Figure 1. Assuming the size of the water image is N*N, according to Eq.1, Setting the initial value as 0.2345, branch parameters u as 3.99999, then generate a one-dimensional chaotic sequence m, its size is N*N. According to Eq.3, adding the operation of mold 2 to the sequence m, then get a new sequence m.

$$m=\text{mod}(1000*m,256) \tag{3}$$

The sequence m and the watermark image sequence have bit XOR operation, then scrambled watermark image can be got as shown in Figure 3.

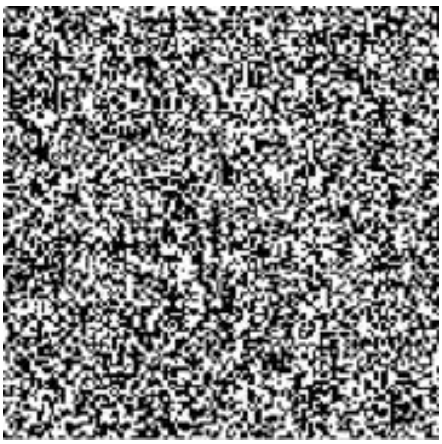

Figure 3. Encrypted QR Code Image

3.2. Watermark Embedding

The process of watermark embedded is shown as following.

Step 1: the original host image I has two level discrete wavelet transform with "Harr" wavelet, then getting seven sub-bands: LL_2, LH_i, HL_i, HH_i (i=1, 2);

Step 2: the LL_2 sub-band is decomposed by SVD, $LL_2 = US_I V^T$,then get the singular value matrix S_I by Eq.4;

$$S_I = diag(\lambda_{M1}, \lambda_{M2}, \cdots, \lambda_{MP}) \tag{4}$$

Step 3: the text information "Yangtze University" as identification information rights are encoded to QR code, then using Logistic chaotic scrambling method to scramble QR code (setting the initial value as 0.2345and branch parameter $u = 3.99999$ as the key), then get encrypted watermark image W ;

Step 4: determining α as the intensity factor of embedding watermark, adding the watermark image matrix to S_I (the singular value matrix of the LL_2, then get the singular value matrix of embedded watermark LL_2image by Eq.5;

$$S^* = S_I + \alpha W \tag{5}$$

Step 5: then the singular value matrix S^* has SVD decomposition, then get a new singular value matrix S_1 by Eq.6.

$$U_1 S_1 V_1^T = S^* \tag{6}$$

Step 6: Having inverse SVD with S_1 to get the embedded watermark sub-band image LL_2^* by Eq.7;

$$LL_2^* = U\ S_1 V^T \tag{7}$$

Step7: Combining LL_2^* embedded watermark sub-band image with others sub-bands image LH_1, HL_1, HH_1,then have inverse discrete wavelet transform, lastly get the host image embedded with watermark.

3.2 Watermark Extraction

The process of watermark extracted is shown as following:

Step 1: the watermarked image is decomposed by DWT, then get sub-band image LL_{w2}, if needing to test the robustness of watermark, adding all different types and strength attacks to the watermarked image, then have discrete wavelet transform, then can obtain the LL_2 sub-band image;

Step 2: the sub-band image LL_{w2} is decomposed by SVD, get the singular value matrix of the sub- band LL_{w2} by Eq.8 and Eq.9.

$$LL_{w2} = U_2 S_2 V_2^T \tag{8}$$

$$S_3 = U_1 S_2 V_1^T \tag{9}$$

Step 3: according to intensity factor of embedded watermark, after inverse SVD transform, can get extracted watermark W^* by Eq.10;

$$W^* = (S_3 - S_I) / \alpha \tag{10}$$

Step 4: decrypting the watermark image W^* with the key, then get the original QR code image.

4. Experimental Results and Analysis

In experiment, the host image is the Lena image with the size of 512x512 pixels, as shown in Figure 4, QR codes binary image as watermark image with the size of 128x128 pixels, which includes the text copyright information "Yangtze university" as shown in Figure 5; common binary watermark image as shown in Figure 6. To process Figure.4 with the watermark image in Figure 5, get the watermarked image in Figure 7; processing the Figure 4 with the watermark image in Figure 6, then get the watermarked image in Figure 8.

Figure 4. Host Image

Figure 5. QR Code Image

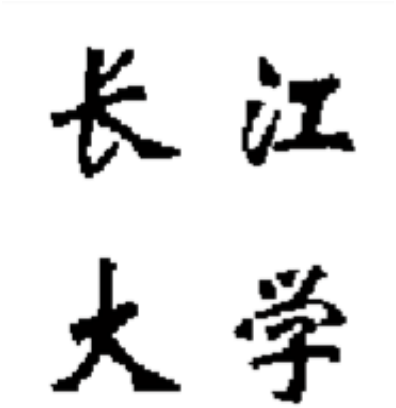

Figure 6. Common Watermark Image

Figure 7. Watermarked Host image

Figure 8. Watermarked Host Image

4.1. Algorithm Evaluation

In order to have an objective assessment for watermark algorithm, using the peak signal to noise ratio ($PSNR$) and similarity (NC) [20-21] is as a criteria to test the algorithm. PSNR measures the difference between the watermarked image and the host image. Supposing host image as $f(i,j)$ and watermarked image as $f^{'}(i,j)$, M,N are the width and height of the host image and watermarked host image. PSNR is as following Eq.11:

$$PSNR = 10\lg \frac{M*N*255^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[f(i,j)-f^{'}(i,j)]^2} \tag{11}$$

The robustness of the watermark is the ability of watermark detection and recovery, when the watermarked host image has some attacks or damage such as cropping, filtering, image smoothing, contrast variation, noise and geometric distortion etc. Often using the normalized correlation coefficient NC of the extracted watermark image and the original watermark, NC measures the similarity of extracted watermark and original watermark ($0 < NC \le 1$). Supposing original watermark image as W, the extracted watermark image as W*, m, n are width and height of the watermark image and exacted watermark image, then the correlation coefficient NC is expressed as Eq.12:

$$NC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}W(i,j)W^{*}(i,j)}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}W(i,j)^2} \tag{12}$$

4.2 Experimental Results and Analysis

Experimental results show that the PSNR of the original host image and the embedded watermark image with no previously attacks is 40.1687, which indicates the naked eye can't recognize the change between the original host image and watermarked image, which meets the human visual requirements. Meanwhile, the NC of the extracted watermark and the original QR code watermark is 0.9915, decrypted QR code image can be translated into the original text information, so the extracted watermark has high correlation with the original watermark.

To further test the robustness of the watermark algorithm, adding such attack tests as noise, rotation, shear, histogram equalization, changing contrast ratio, brightness change and other common attacks to the watermarked image in this paper, then calculating the value of PSNR and NC. The simulation results are shown in Figure.9. The data of correlation coefficient of the extracted watermark and the original watermark is shown in Table 1. The data in Table1 shows that the quality of watermark based on proposed algorithm has improved significantly, the watermark has good invisibility. Meanwhile, in the case of QR code watermark with some attacks, the watermark still can be extracted and accurately decrypted the original information carried by the QR code. So the digital watermark algorithm proposed in this paper has better security and robustness.

(a) Watermark Extracted and Decrypted when No Attack

(b) Watermark Extracted and Decrypted when “salt & pepper” Attack

(c) Watermark Extracted and Decrypted when “Gaussian” Attack

(d) Watermark Extracted and Decrypted when Rotate 90^0 Attack

(e) Watermark Extracted and Decrypted when Rotate 45^0 Attack

(f) Watermark Extracted and Decrypted when Left Cutting Attack

(g) Watermark Extracted and Decrypted when Right Cutting Attack

(h) Watermark Extracted and Decrypted when Middle Cutting Attack

(i) Watermark Extracted and Decrypted when Histeq Attack

(j) Watermark Extracted and Decrypted when Adding Contrast Ratio Attack

(k) Watermark Extracted and Decrypted when Decreasing Contrast Ratio Attack

(l) watermark extracted and decrypted when image brighter attack

(m) Watermark Extracted and Decrypted when Image Dimming Attack

Figure 9. (a-m) Simulation Results When Adding Different Attacks

Table 1. the Data of NC and PSNR When Different Attacks

attack form	algorithm in other papers	algorithm in this paper（QR code）	
	NC	PSNR	NC
no attack	0.9816	40.1687	0.9915
salt & pepper 5%	0.9641	18.4646	0.9869
salt & pepper 10%	0.9569	15.5058	0.9853
gaussian（0,0.01）	0.9637	28.7527	0.9887
gaussian（0,0.03）	0.9683	27.9860	0.9889
rotate 90^0	0.9608	27.7688	0.9915
rotate 45^0	0.9816	27.2889	0.9878
cut left	0.9637	23.7688	0.9860
cut middle	0.9658	22.2889	0.9866
cut right	0.9644	23.9860	0.9869
histeq	0.9660	27.7328	0.9888
adding contrast ratio	0.9644	31.1348	0.9866
decreasing contrast ratio	0.9793	29.7645	0.9905
image brighter	0.9784	28.5643	0.9901
image dimming	0.9812	24.4696	0.9913

In order to test the robustness of the algorithm for different host images, selecting the Airplane and Peppers images as test images, The experimental data are shown in Table 2.

Table 2. Test NC for Different Host Images

attack form	Peppers image (NC)	cameraman image (NC)
no attack	0.9915	0.9915
salt & pepper 5%	0.9846	0.9888
salt & pepper 10%	0.9781	0.9883
gaussian（0,0.01）	0.9910	0.9902
gaussian（0,0.03）	0.9803	0.9882
rotate 90^0	0.9895	0.9884
rotate 45^0	0.9862	0. 9915
cut left	0.9877	0.8571
cut middle	0.9871	0.9731
cut right	0.9900	0.9050
Histeq	0.9883	0.9898
adding contrast ratio	0.9897	0.9771
decreasing contrast ratio	0.9888	0.9877
image brighter	0.9888	0.9873
image dimming	0.9914	0.9910

Above the above experimental results as shown in Figure.9 and experimental data in Table 1 and Table 2 show that digital watermark based on based on QR code in this paper has good invisibility and robustness.

5. Conclusion

A digital watermark algorithm based on QR code is proposed in this paper, QR code as digital watermark, QR code is encrypted by Logistic chaotic mapping, combining with discrete wavelet transform and singular value decomposition, digital watermark is embedded in low frequency sub-band image of host image. Taking into account the invisibility of watermark, more strong robustness of the watermark can be got by increasing the security of the watermark and the amount of watermark information to obtain. The result is verified in MATLAB by adding such attack tests as noise, rotation, shear, histogram equalization, changes in contrast, brightness change to the watermarked image. The experimental results show that the robustness of the watermark is improved by such attacks as crop, rotate, noise, for QR code has the inner performance of error detection and correction.

Acknowledgments

This work is supported by the Teaching Research Project of Hubei Province under Grant 2014260 and the National Natural Science Foundation of China under Grants 61672112.

References

[1] Y. Yixian and N. Xin-xin, “Digital Watermarking Theory and Technology”, Higher Education Publishers, Beijing, **(2006)**, pp. 144-149.
[2] W. Rui-ling, “A Study on the Technology of Digital Water-marking in Two-Dimension Barcode, Journal of Hangzhou Electronic and Technology University, **(2010)**, pp. 1-65.
[3] S. Bing and G. Meifeng, “Research on Digital Watermarking Algorithm Based on QR Barcode”, Journal of Computer and Morden, vol. 11, **(2011)**, pp.74-77.
[4] S. Vongpradhip and S. Rungraungsilp, “QR code using invisible watermarking in frequency domain”, Journal of ICT and Knowledge Engineering (ICT & Knowledge Engineering), **(2012)**, pp. 47-52.

[5] W. Zi-yu and S. Liu-jie. "Improved QR Code Based on Digital Holographic Watermark", Journal of Packaging Engineering, vol. 33, no. 77, **(2014)**, pp. 144-148.
[6] L. Li, Z. Ya-jian and Z. Bin, "Digital Watermarking Method for QR Code Images Based on DCT and SVD", Journal of Infrared and Laser Engineering, vol. 26(S2), **(2013)**, pp. 304-311.
[7] B. Tao-tao, L. Zhen and L. Peng, "Geometrical Attack Resistant Digital Watermark Based on QR Code", Journal of Packaging Engineering, vol. 33, no. 13, **(2013)**, pp. 104-107.
[8] Z. Xiong and L. Guo-dong, "Filtering for QR Code Image Pre-processing", Journal of Applied Optics, vol. 31, no. 3, **(2010)**, pp. 413-417.
[9] F. Han-lu, H. Ying-wei and N. Xiao-jiao, "Principle and Implementation of Error Correcting Coding of QR Code", Journal of Computer Applications, vol. 31, no. 1, **(2011)**, pp. 40-42.
[10] Z. Cheng-hai, Z. Duo and Z. Shou-xiang, "Bar Code Technology and Application", Tsinghua University Publishers, Beijing, **(2009)**.
[11] S. Wu and Z. Tan, "Multi-resolution Watermarking Scheme Based on Chaotic Sequence", Journal of Xi'an Jiaotong University, vol. 3, no. 6, **(2000)**, pp. 35-39.
[12] P. Makisha, S. Maier and P. Enrique, "Switching Induced Oscillations in the Logistic Map", Journal of Physics Letters A, vol. 374, no. 8, **(2010)**, pp. 1028-1032.
[13] N. Singh and A. Sinha, "Chaos-based Secure Communication System Using Logistic Map", Journal of Optics and Lasers in Engineering, vol. 48, no. 3, **(2010)**, pp. 398-404.
[14] W. Sweldens, "The lifting scheme: A Construction of Second Generation Wavelets", Journal of Mathematical Analysis, vol. 29, no. 2, **(1997)**, pp. 511-546.
[15] S. Qiang and Z. Hong-bin, "Color Image Self- embedding and Watermarking Based on DWT, International Conference on Measuring Technology and Mechatronics Auto-Mation, Beijing, **(2010)**.
[16] L. Xiao-jing, X. Hong-xia and M. Hai-ying, "Robust Digital Watermarking Algorithm Based on Two Dimensional Hyper-chaotic Mapping", Journal of TV Technology, vol. 39, no. 19, **(2015)**, pp. 30-33.
[17] W. Shu-mei, Z. Wei-dong and W. Zhi-cheng, "Research on Image Digital Watermarking Methods Based on SVD", Journal of Computer Engineering and Design, vol. 29, no. 11, **(2008)**, pp. 2834-2836.
[18] G. Bhatnagar and B. Raman, "A New Robust Relerence Watermarking Scheme Based on DWT- SVD", Journal of Computer Standards & Interlac, vol. 31, no. 5, **(2009)**, pp. 1002-1013.
[19] L. Min and Y. Yu, "An audio blind watermarking scheme based on DWT-DCT-SVD", Journal of Beijing University of Posts and Telecommunications, vol. 34 (S), **(2011)**, pp. 51-54.
[20] H. Deng, D. Zhang and T. Wang, "Objective Image Quality Assessment for High-Resolution Photospheric Images by Median Filter-Gradient Similarity", Journal of Solar Physics, vol. 290, no. 5, **(2015)**, pp. 1479-489.
[21] Z. Y. Li, K. Z. Tang and J. M. Hu, "Directional Weighted Mean Filter for Image with Salt & pepper Noise", Journal of Image and Graphic,201, vol. 18, no. 11, **(2014)**, pp. 1407-1415.

