Research on Anti-counterfeiting Technology Based on QR Code image Watermarking Algorithm

De Li[1], XueLi Gao[1], YuChao Sun[1] and LiHua Cui[2*]

[1]*Department of Computer Science, Yanbian University, Yanji, China*
[2]*College of Economics and Management, Yanbian University, Yanji, China*
*leader1223@ybu.edu.cn, 942969567@qq.com, 1185828046@qq.com,
2732677@163.com

Abstract

In this paper, a new anti-counterfeiting scheme and a high robustness digital watermarking algorithm based on DWT and SVD were proposed. We took a QR code as the carrier image, which is generated by the relevant information of the copyright owner, and then embedded the copyright owner's information into the QR code as a watermark. Afterwards we obtained the watermark information contained in the QR code by using watermark detection and two dimensional bar code scanning tools. In order to achieve the purpose of anti-counterfeiting, we could verify its authenticity by checking watermark information and scanning information. The experiment proved that this method can resist compressive attack, rotation attack, noise attack and so on. The new scheme and algorithm provide a strong guarantee for the bill anti-counterfeiting technology.

Keywords: Digital watermarking, SVD, DWT, QR code, bill anti-counterfeiting

1. Introduction

Nowdays, QR codes are widely used because of its advantages, such as large information capacity, wide range of encoding, strong fault tolerance and low cost, *etc.* And QR codes also can encode photos, fingerprints and text, and can read documents automatically. What's more, it has anti-counterfeiting function to some extent. But the encoding method of QR code is open which is easily copied and forged. So, it is not a strict anti-counterfeiting technology [1-2].

Digital watermarking technology is an important technology and effective method for the protection of digital copyright and security authentication [3]. So it is a hot research spot in recent years, especially in combining the digital watermarking technology with the two dimensional code technology to realize anti-counterfeiting function [4-6]. At present, the QR code is the most potential of the two dimensional code technology. In this paper, the two dimensional code technology based on digital watermarking is mentioned. It solves the problem of anti-counterfeiting by embedding digital watermark into QR code, which provide effective protection for bill anti-counterfeiting.

2. Anti-counterfeiting Scheme and Watermarking Algorithm

From the current research situation, because the two dimensional code is binary image, most of the existing methods embed watermark in spatial domain, so the watermark capacity is very limited [7]. And the method of embedding watermark in transform domain is still not very extensive [8,9]. With reference to taking QR code as a carrier image and identifying it by the barcode scanner at the same time, there are little relevant references. According to the reference [10], the effect of extracting watermark is very good without attacking when embedding watermark into QR code, but the robustness is

---

* Corresponding Author

very poor. The author proposed a QR code watermarking algorithm which based on SVD and DCT, it can effectively resist noise attack, but the capability of resisting other attacks were relatively weak[11]. In this paper, a new watermarking algorithm based on SVD and DWT is proposed. It can effectively resist noise, cropping, rotation, compression and other attacks, so the robustness is further enhanced.

2.1. Basical Frame of Anti-counterfeiting Scheme

By applying QR code to bill to expand its application scope, since it provides effective anti-fake. In the Anti-counterfeit scheme, we took QR code as the carrier image, which is generated by the relevant information of the copyright owner, and then embedded the copyright owner's information into QR code as a watermark. Afterwards we obtained watermark information through watermark detection tools, and got the information contained in QR code by two-dimensional bar code scanning tools. In order to achieve the purpose of anti-counterfeiting, to check watermark information and to scan information are identical to verify its authenticity. The followings are the carrier image and the watermark image, the one on the left is the carrier and the other is the watermark:

Figure 1. Carrier Image and Watermark Image

The process of QR code in bill security scheme is as shown below:
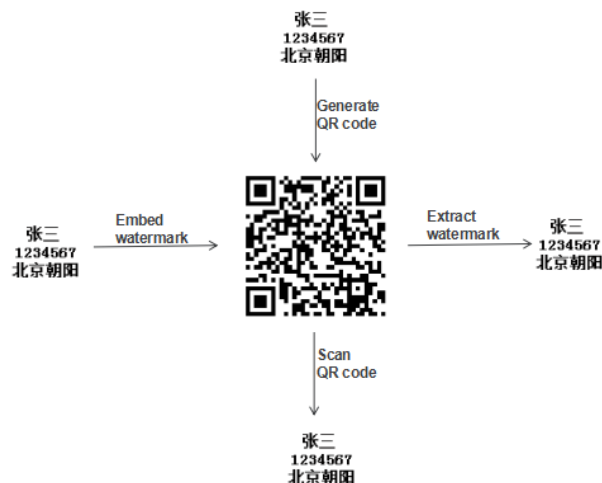
Figure 2. The Process of QR Code in Bill Security Scheme

2.2. QR image Preprocessing and Normalization

The QR code is a matrix two-dimensional bar code, which consists of an encoding area and a functional graphics, including the position detection patterns, the separator for detection patterns, the positioning of the graphics and the correction graphics. functional graphics cannot be used for data encoding, the symbol is surrounded by a blank area, as shown in Figure 3:
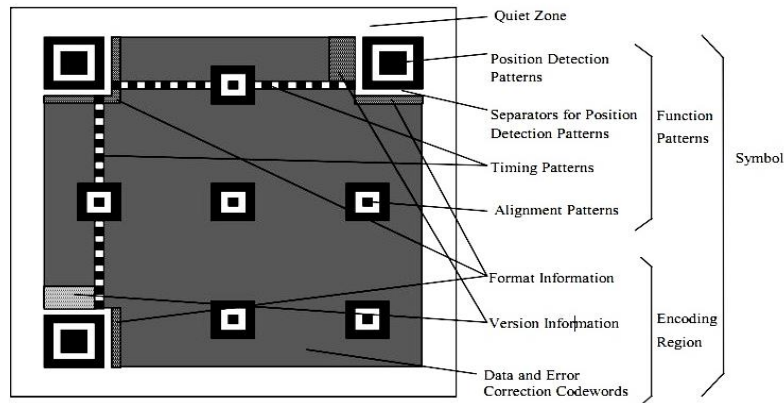
Figure 3. Symbol Structure of QR Code

The three position detection patterns ensure a quick scan in different directions. In order not to affect the fast scan of QR code and avoid obvious visual anomaly, in this paper, the position detection patterns and separator for the position detection patterns of QR code are extracted and replaced by a blank space.

According to the characteristics of QR code, the operation of adding noise does not affect correct identification of QR code. first, we extract position detection patterns and separator for position detection patterns of QR code, and then the image is processed through gauss ambiguity. In the experiment, we use 256×256 QR code image whose correction rate was 30% to deal with the Gaussian noise fuzzy processing which the mean is 0 and the Variance is 0.000001. Specific steps are as follows:

(1) To replace the position detection patterns and the separator for position detection patterns of QR code with the blank area, changed image are obtained by removing the position detection patterns and the separator for position detection patterns. The original image and the changed image showed in Figure 4.

Figure 4. The Original QR Image and the Changed QR Image

The automatic extraction algorithm of the position detection patterns and the separator for position detection patterns is as follows:

1) According to the characteristics of QR code image, the position detection patterns are square of the same size, so the separation of the QR code has some rules.

2) To take the upper left corner of position detection patterns as an example, we scan QR code from left to right. The first scan of separator for position detection patterns is the left boundary of position detection patterns, and the last scan is the right boundary of the position detection. Then the size of the position detection and coordinate position can be determined.

3) In the same way, the specific coordinates of the other two position detection patterns can be determined.

4) Use the blank area instead of the three the position detection patterns.

(2) We add Gaussian noise to obscure the changed image which had the position detection patterns and the separator for position detection patterns removed. The preprocessed image is obtained by adding the position detection patterns and separator for position detection patterns to its original position, and it can be correctly identified.

In addition, Moment-based image normalization refers to the moment of the image itself to find a set of appropriate parameters, then a series of standard transformation operation is applied to the image, which makes the transformation process of the original image to a fixed standard form. The standard image after transformation is called normalized image. Moment in physics is an important parameter for recognizing the shape of an object, and moment is also one of the methods described in the region.

In region $f(x, y)$, the moment $(p+q)$ is defined as:

$$m_{pc} = \sum_x \sum_y x^p y^q f(x, y), p, q = 0, 1, 2...$$ (1)

The corresponding central moment could be defined as:

$$\mu_{pq} = \sum_x \sum_y (x - \bar{x})^p (y - \bar{y})^q f(x, y), p, q = 0, 1, 2...$$ (2)

among：$\bar{x} = \dfrac{m_{10}}{m_{00}}; \bar{y} = \dfrac{m_{01}}{m_{00}}$

In the process of normalization, in order to perform affine transformation, homogeneous coordinates need to be used, and then use $(x, y, 1)$ to indicate two vector, $x' = x + tx; y' = y + ty$ equal to:

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$ (3)

By adding a row and a column in the matrix, the element value of the lower right corner is set to 1, and the others are set to 0, the method can convert all linear transformation to affine transformation.

For images, the affine transformation is a linear transformation from two dimensional coordinate to two dimensional coordinates. The relative position of the image is kept unchanged before and after transformation. Affine transformation has good resistance to geometric attacks such as translation, rotation, scaling, turning, *etc*. Moment itself has the characteristics of invariance, and image normalization method based on moment and affine transformation is still a good method to resist geometric attacks.
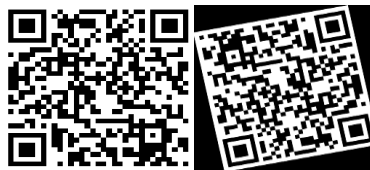
Figure 5. Original QR Images, Normalized QR Images and Standard QR Images

2.3. Watermark Embedding Algorithm

In this paper, the QR code image, whose error correction rate is 30%, is adopted as the carrier image. At first image is pretreated, and then normalized and standardized. The LL region is extracted after DWT transformation, and D-matrix is obtained by the SVD decomposition in the LL region. Then we embed the arnold transformation watermark into D-matrix. The final carrier image is obtained by embedding watermark after SVD inverse transformation and IDWT transformation.

The specific steps of the watermark embedding algorithm are as follows:

(1) Pretreatment for the QR code image Q (256×256) to get image I.

(2) Standardized image I_{norm}(256×256) is obtained by using the transformation matrix to carry on reverse mapping transformation based on normalized processing of image I.

(3) Process Processing Arnold transformation to watermark image W_{mark}, and then get the watermark image W, at the same time, save the transformation times N. we set N = 10 in this step.

(4) Process I_{norm} (256×256) for twice DWT transformation, that is to take the left corner coefficient matrix 1/4 region (LL region) after DWT transformation and again like this, and then take the left corner to call matrix A (64×64).

(5) Conduct SVD (singular value decomposition) transformation on the matrix A, and then get three matrices U, D, V from $A = U×D×V^T$.

(6) Transform the watermarking image W with the formula: $D`=D+a×W$.(a is the embedding strength factor, let a = 0.001 in this paper).

(7) Process SVD (singular value decomposition) transformation on the matrix D`, and then get three matrices $U_1$，$D_1$，$V_1$ from $D`=U_1×D_1×V_1^T$.

(8) Get the matrix A` by SVD inverse transformation, $A`=U×D_1×V^T$.

(9) We can get image Ґ by IDWT transformation.

(10) Replace the region of position detection patterns and separators for position detection patterns of Ґ with original QR code image Q.
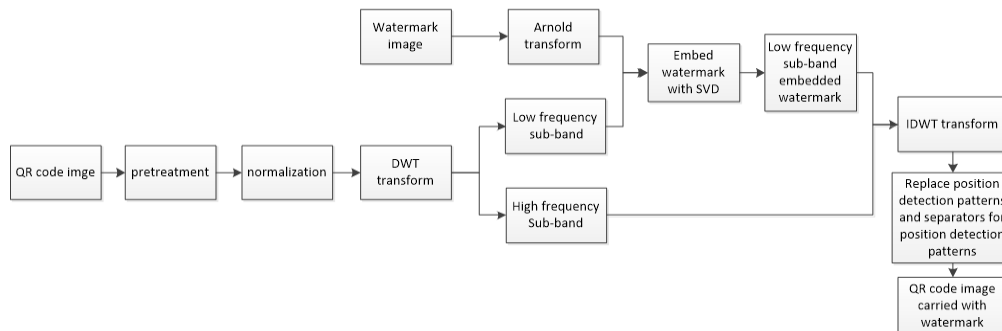
Figure 6. Flow Chart of Embedding Watermark

2.4. Watermark Extraction Algorithm

The watermark extraction is an inverse process of watermark embedding. There are some interference points after multiple changes in extracted watermark image, we call it "noise" here as shown in Figure 7:
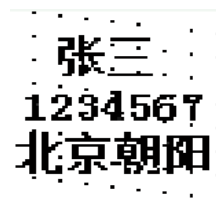
Figure 7. The Watermark Image with "Noise"

Although the distribution of these "noise" are relatively sparse, it can disturb the people's judgment of the watermark image. So it is necessary to remove the "noise" from

the extracting watermark image, in this paper, we removes "noise" of the watermark image depending on density. Specific algorithms are as follows:

(1) After corresponding attacks for carrier image embedded watermark, we get the image I to be detected.

(2) Replace the region of position detection patterns and separators for position detection patterns with blank region, then image I' is obtained.

(3) By applying DWT transformation to image I', we take the LL region of transformed image as A*(64*64).

(4) By applying SVD transformation to A*, we get U*，D*，V*.

(5) Take the matrices U_1，V_1，D* for SVD inverse transformation and get the matrix named D**(D**=U_1*D**V_1T, where U_1 and V_1 come from step 7 in watermark embedding algorithm), then obtain the image W* from formula W*=(D**-D)/a.

(6) By applying Arnold inverse transformation to W* , we get the watermark image W.

(7) Clear the "noise" in image W and obtain the final watermark image we want. The steps for clearing "noise" is like this:

1) Find the "gray points" that pixel value less than 70 in image W.

2) Calculate the number of "gray points" in the eight points around a certain gray point, if the number is zero, then we call this point as "noise".

3) To every "gray point", we center on this point and extend to four sides(up, down, left, right) with a certain radius, radius value is 2 in our experiment, and then get a square region S.

4) Calculate the number of "gray points" in region S, we call them as "density".

5) Calculate the "density" of "gray points" in watermark image W, if "density" is less than the threshold Value Of Density (threshold Value Of Density = 3) then we also call this points as "noise".

6) Modify the pixel value of all singular points as 255, we get the final watermark image W_{final}.
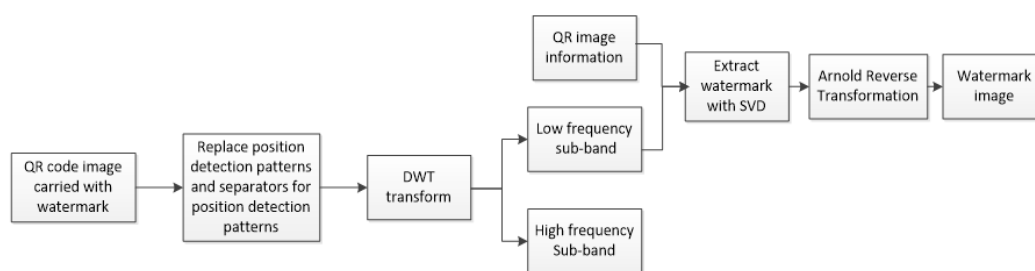
Figure 8. Flow Charts of Extracting the Watermark

3. Experiment and Analysis

In order to verify feasibility of the proposed algorithm, the simulation experiment was carried out in R2010b Matlab. Through a series of attacks, the experimental results showed that the image carried with watermark does not appear obvious distortion of visibility, and the watermark can be extracted if there is no attack.
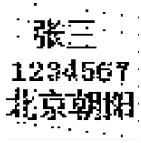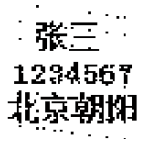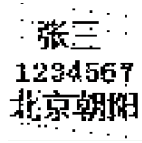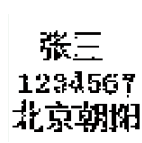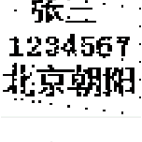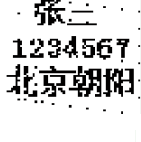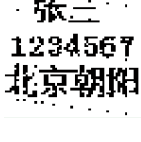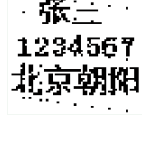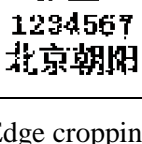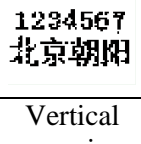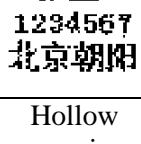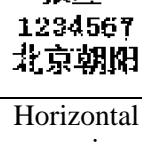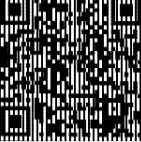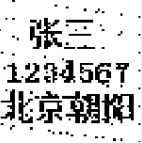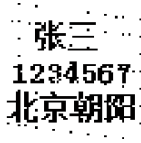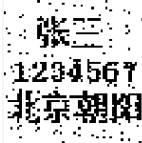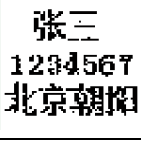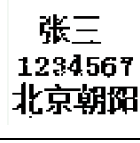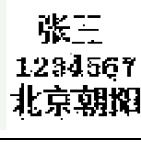
Table 1. A Contrast between Embedding and Extraction of Images

Original image	Image carried with watermark image	Watermark image	Extracted watermark image
		张三 1234567 北京朝阳	张三 1234567 北京朝阳

In order to verify the robustness of the watermarking algorithm, we added some common attacks to QR code in the experiment. The experimental results were shown in the following Table 2:

Table 2. Extracted Results of Common Attacks

JPEG compression Attack	Quality factor 20	Quality factor 50	Quality factor 80	Quality factor 100
Attacked image				
Extracted watermark with "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Extracted watermark without "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Salt and pepper noise attack	Density value 0.005	Density value 0.05	Density value 0.02	Density value 0.1
Attacked image				
Extracted watermark with "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Extracted watermark without "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳

Gaussian noise attack	Variance 0.005	Variance 0.05	Variance 0.1	Variance 0.01
Attacked image				
Extracted watermark with "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Extracted watermark without "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Rotation attack	Angle of rotation 15°	Angle of rotation 30°	Angle of rotation 45°	Angle of rotation 90°
Attacked image				
Extracted watermark with "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Extracted watermark without "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Crop attack	Edge cropping	Vertical cropping	Hollow cropping	Horizontal cropping
Attacked image				
Extracted watermark with "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳
Extracted watermark without "noise"	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳	张三 1234567 北京朝阳

As demonstrated by the experiments carried out, it was the watermark extraction result after some attack, and there was a contrast between "with noise" and "without noise" of extracted watermark. The watermark can be extracted without adding in noise removal algorithm, but it influences visual reading. Removing the uncorrelated noise appeared in the image can effectively guarantee the quality of the watermark.

Besides, the new algorithm has good ability when some common attacks is applied to the carrier image respectively, and the algorithm can withstand two kinds and more than attacks at the same time. In summary, the digital watermarking method for QR code images based on DWT and SVD has strong robustness.

4. Conclusion

QR code is widely used in many fields now, and its technology is relatively mature. So QR code combined with bill can be used to hold more information and reduce the production cost. But its security is the key problem for the further popularization and application of the two-dimensional code, digital watermarking can effectively solve this problem. Taking into account the needs of practical applications, this paper presents a concrete scheme that combined QR code and digital watermarking to the bill. In the digital watermarking algorithm, the simulation experiment showed that the algorithm can withstand common attacks such as rotation, compression and so on. It can effectively improve the performance of QR code encryption watermark, and safeguard the security of bill.

Acknowledgements

References

[1]   T. Xu, "Research and application of document management based on two dimensional code", Thesis of Xi'an University of Science And Technology, (2011), pp.13-64.
[2]   S. Bing, G. Meifeng, "Application of quick response code in anti-counterfeiting technology", Network and Computer Security, (2010), pp.6-9.
[3]   P. Kieseberg, M. Leithner, M. Mulazzani, L.Munroe, S. Schrittwieser, M. Sinha, E. Weippl. QR code security. In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, (2010), pp.430-435.
[4]   F. Hui, "Research of Certificate Anti-Counterfeiting System Design based on Digital Watermarking", Computer Security, (2011), pp.11-12.
[5]   X. Rongsheng, H. Chaoqun, Z. Shunzhi, T. Dapeng, "Anti-counterfeiting digital watermarking algorithm for printed QR barcode", Neurocomputing, 167(C), (2015), pp.625-635
[6]   Z. Li, "Research and implementation of binary image digital watermarking algorithm based on Wavelet Transform", Thesis of South-Central University For Nationalities, (2011), pp.13-43
[7]   L. Li, W. Ruiling, "A digital watermarking method for QR codes", sJournal of Hangzhou Dianzi University, vol. 3, no. 2, (2011), pp.46-49
[8]   A. V. Durga, S. Srividya, "A New Algorithm for QR Code Watermarking Technique or Digital Images Using Wavelet Transformation", International Journal Of Engineering and Computer Science, (2014), pp.776-778
[9]   D. Anli, "Research on encryption and decryption algorithm of QR code watermarking", Wireless Internet technology, vol. 10, (2013), pp.122-123
[10]   J. Zhujun, "Digital watermarking technique based on two dimensional barcode", Thesis of Wuhan University of Technology, (2012), pp.5-57
[11]   L. Li, Z. Yajian, "Digital watermarking for QR code images based on DCT and SVD. Infrared and Laser Engineering", (2013), pp.304-311

Authors
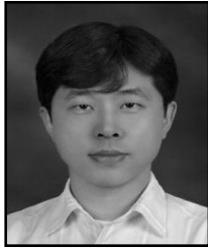
De Li, received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, feature recognition, digital watermarking, and digital forensic marking.

XueLi Gao, is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas of Information Hiding, digital right management, zero watermarking, feature recognition.

YuChao Sun, is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas of Information Hiding, zero watermarking, feature recognition, digital forensic marking.

LiHua Cui, received the Ph.D. degree from KookMin University, major in Financial Management in 2008. She is currently a professor of Dept. of Financial Management at Yanbian University in China. Her research interests are in the areas of Statistical analysis, Information hiding, Pattern recognition, copyright protection technology.