Anti-fake Digital Watermarking Algorithm Based on QR Codes and DWT

Jiaohua Qin, Ruxin Sun, Xuyu Xiang, Hao Li and Huajun Huang
(Corresponding author: Jiaohua Qin)

College of Computer and Information Engineering, Central South University of Forestry and Technology
Changsha 410004, China
(Email: qinjiaohua@163.com)

(Received Sep. 16, 2015; revised and accepted Nov. 15 & Nov. 30, 2015)

Abstract

This article proposes an anti-fake QR codes watermarking algorithm based on the DWT and SVD, aiming at the security problem of QR code in the actual application. Firstly, this paper analyses the advantage of QR code as well as its problems. Secondly, the principle of the chaos encryption and discrete wavelet transform are introduced in detail. Then, we design a new watermarking barcode by the combination of chaos encryption and singular value decomposition and discrete wavelet transform. Experimental results show that the proposed method is significantly superior to the prior arts on the anti-fake performance and watermarking quality.

Keywords: Chaotic encryption, discrete wavelet transform, QR code, watermark barcode

1 Introduction

In the research of 2D barcode, QR code with the advantages of strong error correcting ability, large capacity, being identified easily, becomes a more outstanding member in the barcode family, and it is also widely used. Except the characteristics that other 2D barcodes have, QR code has the advantages of high reliability, Chinese characters and image information representation ability, confidentiality and security, high reading speed, big data density, small occupied space and full reader. Therefore, QR codes are widely concerned interiorly, becoming a hot research and application of two dimensional barcode [2]. However, just like other barcode, the opening coding mode makes it perform badly in privacy as the lack of security methods in the strict sense.

According to “The global mobile phone security report in the first quarter of 2014”, a total of 41199 models of the mobile malware were killed with a year-on-year growth of 63.9% [12]. The two-dimensional code technology has become a new channel of mobile phone viruses and phishing web site communication.In order to get rid of the hidden trouble of safety and protect the security of the information about the users, the two-dimensional code technology and information security technology must be combined to research and develop a safe and reliable two-dimensional code.

Spatial domain watermarking is an edge pixel expansion or reduction of the depth graphics module of the two-dimensional code. The use of two-dimensional code recognition algorithm for depth graphics module allows a certain error, and there exists many reservations module and no coding modules [13]. Coding these modules will not affect the correct recognition of two dimensional code, and can get the realization of embedded secret information. He et al. [5] proposed QR code digital watermarking method based on the least significant bit and its improved algorithm. The scheme embedded watermark into the least significant bit of QR code, its improved algorithm was for gray image. Because the QR code itself was binary image, the robustness of watermark bar code was poor as the embedding of the LSB, so it is difficult to extract the watermark when suffering attack. Zhu et al. [16] proposes the matrix coding based on the LSB algorithm, which can reduce the bits of the least significant bit that need to be modified. Since the scheme is based on the LSB algorithm of two-dimensional codes, so the robustness of the algorithm performs poor. Xie et al. [14] used chaotic mapping to control the position of watermark embedding QR code, which adapt strategy of the chaotic key adaptive adjustment, improved the capacity and robustness of watermark embedding. Since the scheme uses a key adaptive strategy, the watermark embedding process is not stable, needs repeated embedding and verification, and when the watermark information gets too large, chaotic key adjustment times and the algorithm consuming time will increase.

With the spreading spectrum and mapping for hidden information, Chao et al. [1] hide information by the strip and the space of the fine-tuning code according to the structural characteristics of two-dimensional barcode. G. Prabakaran et al. [9] extracted I component of the video and did SVD decomposition by using singular value decomposition and discrete wavelet transform technology, then inserted the logo into a diagonal matrix of SVD decomposition, at last the video watermark logo can be obtained after reverse changes. Liu et al. [6] did DCT block transformation to vector images by using the discrete cosine transform and singular value decomposition of matrix, then did SVD decomposition on the coefficient matrix obtained by transformation, then did watermark embedding in the diagonal matrix. The algorithm has good invisibility and robustness, but it is complex and difficult to implement.

In this paper, we proposes an anti-fake QR codes watermarking algorithm based on the DWT and SVD. In Section 2, we introduce the detail algorithm of watermark barcode based on QR and DWT, and the experimental results and analysis is shown in Section 3. The conclusion is given is Section 4.

2 Watermark Barcode Based on QR and DWT

This paper took the QR code as the carrier, the binary image as the watermark information. Firstly, we encrypted watermark information by chaotic encryption. Secondly, we did 3 layers of the discrete wavelet transform to the QR code, then we went on with the singular value decomposition on diagonal components of high frequency after the wavelet transform. The final, we embedded chaotic encryption watermark information into the obtained diagonal matrix.

2.1 Chaotic Encryption

Chaos is a kind of complex dynamical behavior with special properties. It has the characteristics of extreme sensitivity to initial conditions and system parameters, movement track irregularity, intrinsic randomness, boundness, ergodicity. Therefore we can construct the encryption system by these characteristics [15].

Encryption system is very sensitive to initial value and parameters, it can provide a set of keys, and fully meet the demand of chaotic system tested by the cryptographic binary sequence. The uniform distribution of 0 and 1 satisfied the random numbers requirements, can be regarded as a random sequence. Stream cipher includes the chaos encryption and it is ineffective for block cipher attack method. Due to the unidirectional and the iterative of chaotic signal processing, the operated key stream is almost impossible to infer for the chosen plain text and cipher text attack method.

This paper uses chaos mapping to generate a chaotic sequence and transforms it into the dual-value matrix with the same size of watermarking, and do XOR operation on watermark to get the watermark encryption. In order to enhance the security of the watermark and the robustness, we can also carry out the scrambling operation on watermark. The encryption algorithm is as follows:

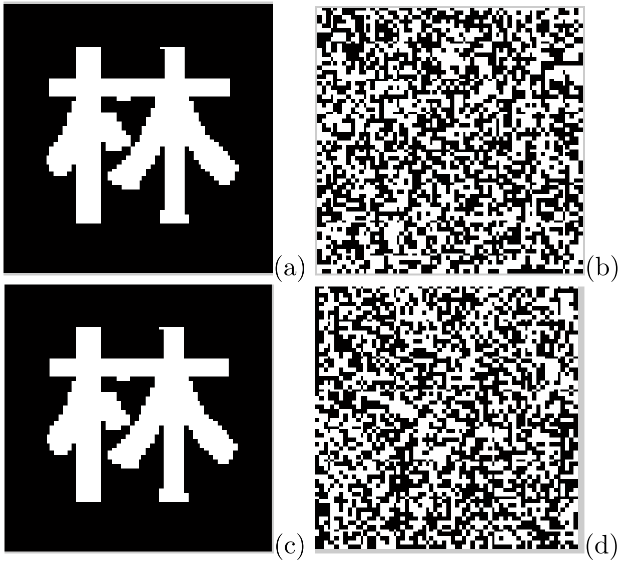

Figure 1: The watermarked image after using chaos encryption and decryption: (a) Original image, (b) The chaotic encrypted image, (c) Decryption image, (d) The error decrypting image

Step 1. Input the encrypted initial value.

Step 2. Generate a chaotic sequence with the same size of watermark by chaotic mapping formula. The adapted chaotic equation is as follows:

$$\begin{aligned} L(1) &= key, key \in (0,1) \\ L(i) &= 1 - 2 \times L(i-1) \times L(i-1), \\ i &= 2, 3 \cdots m \times n \end{aligned}$$

Where key is the initial key, $m * n$ is the size of the watermark image.

Step 3. Converted the generated sequence into 0, 1 sequences.

$$\begin{cases} L'(i)=1, L(i) \geq 0 \\ L'(i)=0, L(i) < 0 \end{cases}$$

Step 4. Do XOR operation on the generated 0, 1 sequence and the watermark.

Decryption is the reverse process of encryption. Decryption process needs to know the secret key, chaotic equation and the encrypted watermark image. The chaotic sequence is obtained through the chaotic formula and the secret key. Convert the chaos sequence into 0, 1 sequence and XOR with the encrypted watermark image, then image can be decrypted. If we use an error secret key, we will not get the decrypted watermarking image. The image chaotic encryption and decryption are shown in Figure 1.

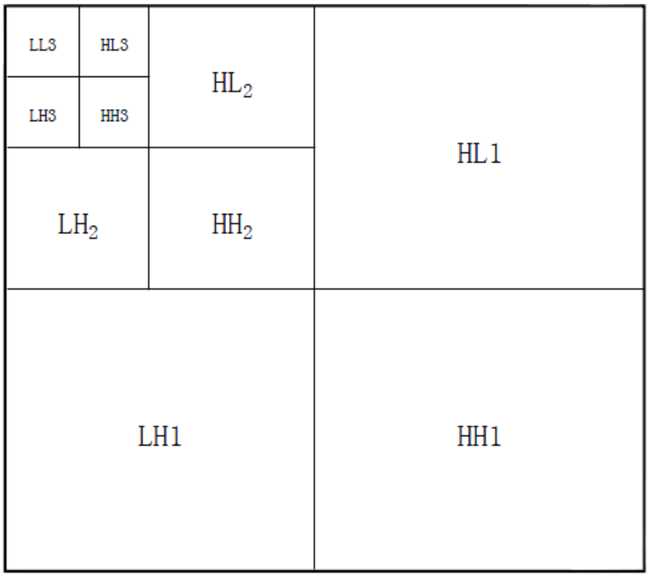

Figure 2: Decomposition diagram based on DWT

2.2 The Discrete Wavelet Transformation

The discrete wavelet transformation (DWT) means the discretization of the expansion factor a in the discretization continuous wavelet function and the translation factor b [10]:

$$a = a_0^m (a_0 > 1), b = nb_0 a_0^m (b_0 \in R, (m, n) \in Z^2) \qquad (1)$$

Then

$$\varphi_(m, n)(t) = a_0^{m/2} \varphi(a_0^m t - nb_0)$$

In general, $a_0 = 2, b_0 = 1$:

$$\varphi_(m, n)(t) = 2^{m/2} \varphi(a^m t - nb)$$

For the discrete wavelet transform for arbitrary function $\varphi(t) \in L^2(R)$:

$$W_f(m, n) =< f, \varphi_{m,n} >= \int_{-\infty}^{+\infty} f(t) \times \overline{\varphi_{m,n}(k)}$$

If $f(t)$ is discrete, recorded as $f(k)$, then:

$$w_f(m, n) = \sum_k f(k) \times \overline{\varphi_{m,n}(k)}$$

From the wavelet multi-resolution and decomposition of the image signal characteristics, the principle of wavelet transform is in accordance with the octave to separate the signal spectrum, and the obtaining final signal is a low frequency sub-band in these octave band and several high frequency sub-band data [8].

Figure 2 is the multi resolution wavelet decomposition, and it is the decomposition figure after 3 times discrete wavelet transform. After the 3 times discrete wavelet transform, the LL$_3$ band is the low frequency sub-band. HH$_K$, LH$_k$, HL$_k$ ($k = 1, 2, 3$) and several other bands is the high frequency sub-band. The HL$_k$ band is a sub-band obtained by going through a low-pass filtering firstly in the row direction on the upper level low frequency sub-band, and then a high-pass filteringin the column direction. So, the HL$_k$ band mainly contains information of details of the signal in the horizontal direction on the vertical direction, HL$_k$ is the horizontal detail sub-band. In the third layer wavelet decomposition, the low frequency sub-band LL$_3$ contains the lowest resolution information of the original images. HL$_3$, LH$_3$, HH$_3$ are the fine information data of LL$_3$. Because of the characteristics of multi-resolution decomposition of wavelet transform, wavelet analysis of the image has a very good directional selectivity, and can combine with the human visual system very well.

2.3 Watermarking Algorithm Based on DWT and QR Code

In this paper, watermark embedding algorithm is based on DWT and singular value decomposition. The watermark information after processing will be embedded into the three layer wavelet transformed the diagonal components, which reduces the influence from the image watermarking to the QR code.

2.3.1 The Watermark Embedding

This paper selects the QR codes as the carrier image of watermark embedding. The watermark information is a binary image. QR codes are generated by software. The watermark embedding process is shown in Figure 3:

The specific embedding procedure is as follows:

Step 1. Generate the QR code image to do discrete wavelet transform. Do three level discrete wavelet transforms to the QR code image. Get the parameters of LL_3, LH_3, HL_3, HH_3.

Step 2. Singular value decomposition to high frequency diagonal coefficient HH_3. On the HH_3 singular value decomposition, we can get the transformation matrix U, V and diagonal matrix D. D will be regard as the embedding position of the watermark.

Step 3. Chaotic encryption of watermark image W. By the singular value decomposition of chaotic encrypted watermark image, we will get the maximum singular values of watermark image, used to determine the embedding factor.

Step 4. The watermark embedding. The watermark should be embedded into the high frequency diagonal coefficient HH_3 of the QR code according to the embedding factor.

$$HH_3 w(i, j) = HH_3(i, j) + \alpha \times$$
$$HW(mod(i - 1, wm) + 1, mod(j - 1, wn) + 1)$$

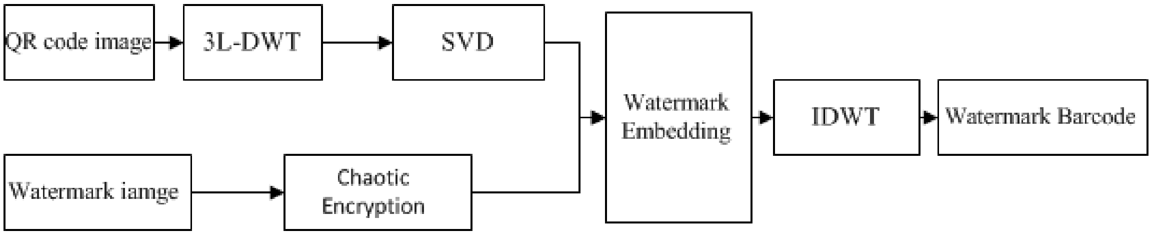

Figure 3: The flow-process diagram of watermark

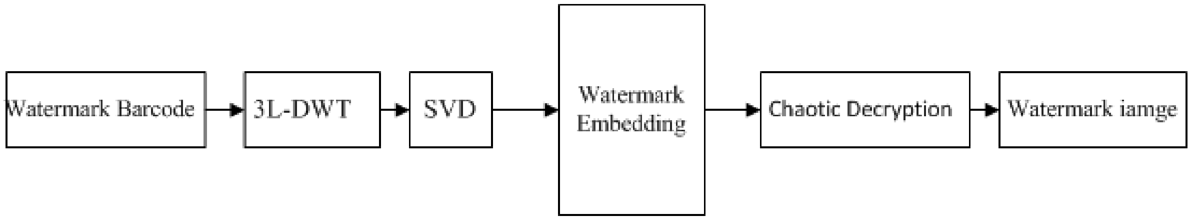

Figure 4: The watermark embedding process diagram

Among them, α is the embedding factor. We value it 0.01 and wn is the size of watermark image.

Step 5. SVD transformation on the obtained matrix. By the SVD transformation to Watermark embedded diagonal matrix D, we will obtain matrix U_1, V_1 and the diagonal matrix D_1. Do inverse SVD transformation on the first SVD transformed matrix U, V and the second SVD transformed diagonal matrix D_1.

$$HH_{W3} = U * D_1 * V$$

Step 6. Get the watermark barcode by inverse wavelet transform.

2.3.2 The Watermark Extraction

The watermarking extraction algorithm is the inverse process of the embedding algorithm. Specific process is shown in Figure 4:

Extraction Specific steps are as follows:

Step 1. Do three layers of discrete wavelet transform on the watermark barcode to obtain the diagonal high-frequency coefficient wHH3.

Step 2. Do singular value decomposition on the high frequency coefficients to get the diagonal matrix D2.

Step 3. Use the inverse formula of watermark embedding formula to get the encrypted watermark information.

Step 4. Do chaotic decryption on the encrypted watermark information to obtain the watermarking image.

2.3.3 The Strength of Watermark Embedding

Because the maximum singular value determines the image quality, then we can make full use of properties of singular value to determine the embedding strength [14]:

1) The low-frequency approximation sub graphs have a large number of singular value coefficient;

2) The largest singular value is larger than the second largest singular value coefficient of the low-frequency approximation sub graphs;

3) The watermark image singular value coefficient is basically bigger than the singular value coefficient of the sub graph;

4) The maximum singular value coefficient of the three sub-bands sub graphs is small, and the modification of the maximum singular value coefficient can not be too large, not more than 1/2 of itself. Otherwise, it will lead to the occurrence of serious deformation of the watermarked image.

Based on the above basis, we can embed intensity a in the diagonal belt of QR code image, determined by the follows:

$$\alpha = \frac{1}{50}[\frac{\lambda^{w}_{max}}{\lambda^{HH_3}_{max}}] \qquad (2)$$

$\lambda^{HH_3}_{max}$ is the largest singular value coefficient of the diagonal belt after three layer DWT decomposition of the QR code image. λ^{w}_{max} is the largest singular value coefficient of watermark image. By the use of strength factor determined by Equation (2) to embed the watermark, the watermark QR code image can not only get the embedded watermark imperceptibility, but also has the very high PSNR.

Table 1: Contrast of the watermark PSNR and the QR code PSNR in different embedding factor

Embedded factor	Watermark PSNR	QR code PSNR	Embedded factor	Watermark PSNR	QR code PSNR
0.1	39.9825	55.7234	0.009	41.1290	55.7251
0.09	39.2029	55.7239	0.008	41.1650	55.7251
0.08	39.2029	55.7239	0.007	41.2002	55.7251
0.07	38.5651	55.7241	0.006	41.2654	55.7251
0.06	37.8698	55.7243	0.005	40.2329	55.7252
0.05	37.0222	55.7245	0.003	40.1655	55.7252
0.04	37.8219	55.7247	0.002	40.7303	55.7252
0.03	40.1965	55.7248	0.001	40.3763	55.7252
0.02	40.6210	55.7250	0.0005	40.3944	55.7252
0.01	41.0931	55.7251	0.0001v	41.3533	55.7252

3 Experimental Results and Analysis

The experiment uses the Matlab 7.8 environment, the original image is the QR code image with 512×512 pixels, and the watermark image is a binary image with 64×64 pixels, as shown in Figure 5.

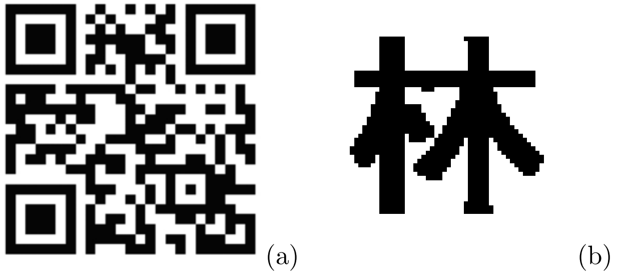

Figure 5: The original QR code and watermark image: (a) The QR code image; (b) The watermark image

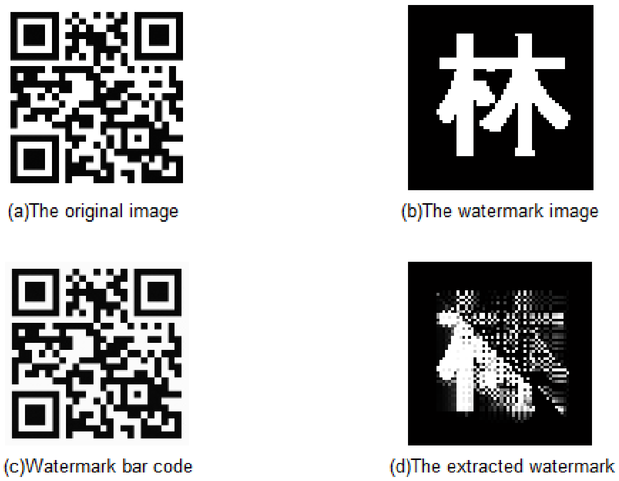

Figure 6: The watermarked image by DWT and the extracted watermark image

By running simulation program and selecting the QR code image and watermark image, we can get the experimental results shown in Figure 6. The results meet the watermark imperceptibility and it can be extracted correctly.

In order to ensure the robustness of the watermark, we must make the watermark embedding strength large enough, but not damage the visual quality of the image, so choosing a proper watermark embedding strength factor is the key to design the watermark barcode.

We use a number of different embedding factors for the watermark embedding in the experiments, for example, embedding factoris 0.1, 0.05, 0.01, 0.001, as shown in Figure 7. With the development of embedded factor reduction, the watermark experiments extracted gets clearer, and the water marked image is not significantly affected by QR code. When the embedded factor is equal to 0.01, the effective of the reduction on the extraction of the watermark becomes small gradually.

According to different embedded factors, we calculated the peak signal to noise ratio of the watermark and the QR code. The experimental results show that, when embedded factor is 0.01, the watermark barcode is well formed, and the extracted watermark can be identified well. When the embedded factor is larger than 0.1, it is difficult to identify the extracted watermark image. In the range of 0.1 to 0.001, with decreasing the intensity of embedded factor, the peak signal to noise ratio of the extracted watermark first decreases and then increases gradually, the peak signal to noise ratio of the watermark bar code shows a linear growth, when the embedding factor reaches down to 0.01, the peak signal to noise ratio tends to be stable. The experimental results are in Table 1.

4 Conclusions

This paper proposes a watermarking algorithm of anti-fake figure based on DWT and QR code. This article uses chaos XOR algorithm for encryption of watermark to ensure the security of the watermark. The new water-

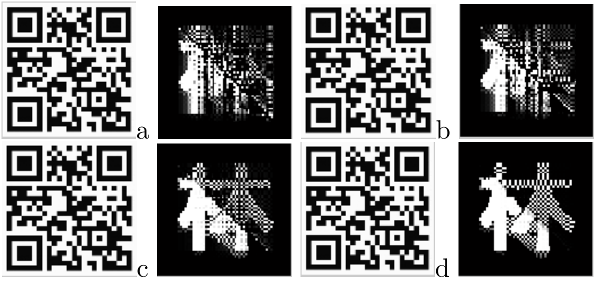

Figure 7: Watermark barcode with different embedding factor and extracted watermark: (a) Embedded factor 0.1 ; (b) Embedded factor 0.05; (c) Embedded factor 0.01; (d) Embedded factor 0.001

marking barcode is designed by doing three layer wavelet decomposition to the QR code image, and by combinating the chaos encryption and singular value decomposition. The simulation results show that the method works well on the watermark embedding and its extracted, can obtain the correct content from the watermarked QR image and can also satisfy the invisibility of watermarking. Next, we will extend image segmentation [17] and learning-based method [3, 4, 7] to QR code watermarking in the future.

Acknowledgments

This project is supported by the National Nature Science Foundation of China (No. 61202496, 61304208), Hunan Provincial Natural Science Foundation of China (No. 13JJ2031), Science and Technology Program of Hunan Province (No. 2014SK2025). The "12.5" education planning project of Hunan province (No. XJK013CXX014), Hunan province and decision-making consulting research (No. 2013BZZ54).

References

[1] Y. Chao, L. Liu, L. Xue, et al., "Information hiding algorithm based on PDF417 barcode," *Computer Engineering*, vol. 36, no. 9, pp. 131–133, 2010.

[2] Denso Wave, The characteristics of QR code [EB/OL] 2013.

[3] B. Gu, V. S. Sheng, K. Y. Tay, "Walter Romano, and Shuo Li, Incremental Support Vector Learning for Ordinal Regression," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26. no. 7, pp. 1403–1416, 2015.

[4] B. Gu, V. S. Sheng, Z. Wang, D. Ho, S. Osman, S. Li, "Incremental learning for ν-Support Vector Regression," *Neural Networks*, vol. 67, pp. 140–150, July 2015.

[5] X. He, A. Hu, W. Zhang, et al., "QR barcode digital watermarking based on improved LSB algorithm," *Computerand Information Technology,* pp. 1–4, 2010.

[6] L. Liu, Y. Zhou, B. Zhang, "The QR code digital watermarking algorithm based on DCT and SVD," *Infrared and Laser Engineering*, vol. 42, no. S2, pp. 304–311, 2012.

[7] J. Li, X. Li, B. Yang, X. Sun, "Segmentation-based Image Copy-move Forgery Detection Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507–518, 2015.

[8] J. Liu, X. Li, "Fuzzy Chaotic watermarking algorithm based on wavelet domain," *Computer Engineering*, vol. 37, no. 8, pp. 132–134, 2011.

[9] G. Prabakaran, R. Bhavani, M. Ramesh, "A Robust QR code video watermarking scheme based on SVD and DWT composite domain," in *International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pp. 21–22, 2013.

[10] S. Rungraungsilp, M. Ketcham, P. Surakote, and S. Vongpradhip, "Data hiding method for QR code based on watermark by comparing DCT with DWT domain," in *International Conference on Computer and Communication Technologies*, pp. 26–27, May 2012.

[11] V. Seenivasagam, R. Velumani, "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud," *Computational and Mathematical Methods in Medicine*, vol. 2013, no. 2013, pp. 1–16, 2013.

[12] The global mobile phonesecurity report in the first quarter of 2014: Chinese rank stop in the mobile phone virus infection [EB/OL], 2014.

[13] S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain," In *IEEE 9th International Conference on ICT and Knowledge Engineering*, pp. 47–52, 2012.

[14] R. Xie, H. Zhao,Y. Chen, "Anti-fake electronic ticket digital watermarking method based on QR codes," *Journal of Xiamen University*, vol. 52, no. 3, pp. 38–342, 2013.

[15] S. Xue, X. Chen, "Digital image watermarking algorithm based on chaotic encryption and SVD," *Computer Engineering*, vol. 38, no. 19, pp. 107–110, 2012.

[16] B. Zhu, "Study on digital watermarking algorithm for QR code based on LSB," *Journal of Chengdu Information and Technology University*, vol. 27, no. 6, pp. 541–546, 2012.

[17] Y. Zheng, B. Jeon, D. Xu et al., "Image segmentation by generalized hierarchical fuzzy C-means algorithm," *Journal of Intelligent and Fuzzy Systems*, vol. 28, no. 2, pp. 961–973, 2015.

Jiaohua Qin received her BS in mathematics from Hunan University of Science and Technology, China, in 1996, MS in computer science and technology from National University of Defense Technology, China, in 2001, and PhD in computing science from Hunan University, China, in 2009. She is a professor at College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. Her research interests include network and information security, image processing and pattern recognition.

Ruxin Sun received his BS in computer science and technology from Central South University of Forestry and Technology, China, in 2013. He is currently pursuing his MS in computer technology at College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include information security, image processing and pattern recognition.

Xuyu Xiang received his BS in mathematics from Hunan Normal University, China, in 1996, MS degree in computer science and technology from National University of Defense Technology, China, in 2003, and PhD in computing science from Hunan University, China, in 2010. He is a professor at Central South University of Forestry and Technology, China. His research interests include network and information security, image processing, and internet of things.

Hao Li received his BS in computer science and technology from Zhengzhou University, China, in 2015. He is currently pursuing his MS in computer application technology at College of Computer Science and Information Technology, Central South University of Forestry and Technology, China. His research interests include information security and image processing.

Huajun Huang is currently a faculty member in the college of Computer and Information Engineering at Central South University of Forestry & Technology. His overall research area include of webpage information hiding and hidden information detection, XML watermarking, anti-phishing, mobile device forensics. Dr. Huang received his Ph.D. from Hunan University in 2007, M.S. degrees from Hunan University in Software Engineering (2004), and a B.A. in Applied Physics from Yunnan University (2001).