International Journal of Hybrid Information Technology
Vol. 9, No.10 (2016), pp. 109-116
http://dx.doi.org/10.14257/ijhit.2016.9.10.11

Certificate Anti-counterfeiting System Based on QR Code and Digital Watermarking

MuSheng Chen[1, 2]

[1]*College of physics and Information Engineering,Quanzhou Normal University,Fujian,China,362000*
[2]*Key Laboratory of Information Functional Material for Fujian Higher Education, Fujian, China,362000*
mushengchen@163.com

Abstract

Focusing on solving the problems of increasing certificate counterfeiting, a novel certificate management system based on two-dimensional barcode technology was developed in the present work. The system, which was compiled using JAVA programming language, can achieve the two-dimensional barcode encoding and decoding for plain texts, images and information included in a certificate (the combined information of texts and images). To improve the security in practical applications, the scrambling algorithm and watermarking encryption algorithm were added, and accordingly, the security of the information contained in two-dimensional barcodes can be ensured. The whole system consists of three modules-encoding, encryption and decoding. To be specific, before encoding, the scrambling transformations should be performed on the certificate image while the number of scrambling transformations is adopted as the secret key. With respect to the generated two-dimensional barcode, we can embed the existing binary images or the signature messages of the certificate holder on this platform into the space domain, contributing to a significantly enhanced anti-counterfeiting performance of the certificate. The certificate information and watermarking information are extracted during the decoding process, i.e., only when the number of scrambling transformations is accurately input, the watermarking information can be extracted and used for identify whether the certificate is counterfeit. The simulation results indicate that, by combing with digital watermarking technology, the security of the two-dimensional barcodes and the included information can be greatly improved while the anti-counterfeiting of certificates can be indeed achieved. Finally, with the student's certificates as the example, we performed simulations on the whole system. It can be concluded that the developed system can be promoted in the other application fields only when some appropriate changes are made.

Keywords*: QRcode; 2-D barcode; digital watermarking; certificate*

1. Introduction

Two-dimensional barcode is characterized by large information capacity, high information density, strong coding ability, low cost of application and easy operation. The information such as pictures, texts, fingerprints and signatures can be encoded with QRcodes, while the database is unnecessary during decoding[1-2].Owing to their excellent advantages, the QR codes are quite applicable for certificate management systems and anti-counterfeiting systems, which now have also been becoming the development tendency. With the use of QR codes, not only can the certificates be automatically recognized, but also the counterfeits of certificates can be effectively avoided [3-5].

ISSN: 1738-9968 IJHIT

The specific procedure is to create a QR code by encoding the personal information (such as name, serial number, address and *etc*.) and the photograph of the certificate-holder which are generally printed on a certificate, and then to attach the generated QR code on the certificate. During the inspection of certificates, the related information can be extracted from the attached QR code on the certificate, so that the authenticity of the certificate can be verified and a more-efficient certificate management is achieved [6-7].

Currently, in the applications of QR codes, we mainly take full advantage of their large storage capacity as well as favorable anti-counterfeiting and secrecy performances. Strictly speaking, the two-dimensional barcode technology is not an anti-counterfeiting technology in principle but just a simple bitwise XOR operation; *i.e.*, with regard to the QR codes, their own anti-counterfeiting characteristics were used[6]. Once the criminals master encoding principle of QR codes, they can counterfeit the identical QR code according to the information included in the certificate. Likewise, the barcodes can easily to be identified. Accordingly, the two-dimensional barcode technology, although exhibiting the anti-counterfeiting function to a certain degree, is actually not a specialized information security technology and thus cannot be regarded to be outstanding in term of anti-counterfeiting. Aiming at achieving wide applications in security field, the two-dimensional barcodes should be combined with the other anti-counterfeit techniques. Image watermarking technology refers to hiding the information in the digital images, while the hidden information can be extracted from the host media. The combination of two-dimensional barcode technology and digital watermarking can significantly improve the anti-counterfeiting performance of two-dimensional barcodes, which has also become an emerging technology and a research hotspot in security field[8-9].

In the present work, by combining with digital watermarking technology, an all-purpose certificate management platform based on two-dimensional barcode was designed. Using the student's certificate as the development model, the while system includes three steps: encoding, decoding and encryption of QR codes. In encoding process, the hybrid encoding which contains both text information and photos is achieved. At the beginning, the scrambling transformation should be performed on the certificate photos, with the number of scrambling transformations adopted as the secret key. The existing binary images or the signature messages of the certificate holders are then embedded into the space domain of generated barcodes, by which the anti-counterfeiting performance of the certificates can be significantly improved. Subsequently, in decoding process, the information included in certificates and watermarks are correctly extracted. For one certificate, a clear certificate photo can be acquired only when the number of scrambling transformation is accurately input. According to the extracted watermarking information, we can identify whether the certificate is true or counterfeit. Using the developed software, the plain texts, images as well as the certificate information (the combined information of texts and images) can all be encoded with QR codes and decoded. In order to improve the security of practical applications, the scrambling algorithm and watermarking encryption algorithm are added and thus the security of QR codes can be ensured. Besides, since it was compiled by using Java programming language, the software is characterized by favorable cross-platform property and good security. Moreover, the software is easy to learn and simple to operate, exhibiting bright application prospects.

2. Design of the System Application Platform

The while system can be divided into three steps, namely, the encoding of QR codes, the decoding of QR codes as well as the embedding and extraction of digital watermarking.

2.1. Encoding

In a QR code, the information including more than 1000 characters can be stored. When applied in a certificate, the information of the certificate including texts, digits and images are all contained in a QR code [2-4]. With regard to the texts and digits, we should design a table according to the main contents of the certificate, mainly including the related information of the certificate holder (such as name, date of birth, address, gender and *etc*.). With regard to the image information, the certificate photo of the certificate holder is input. Aiming at improving the anti-counterfeiting performance of the certificate, we should perform scrambling transformations on the images before encoding, while the number of scrambling transformations N is set by the certificate holder. In decoding process, only the accurate value of N is input, the clear image can be extracted. Finally, the QR codes are generated by encoding using QR code generator. Figure 1 displays some interfaces for encoding, in which the parameters of QR codes are configured, mainly including the version number, correction capacity for error codes, encoding modes, the setting of number of scrambling transformations, the generation of watermark images, and *etc*.

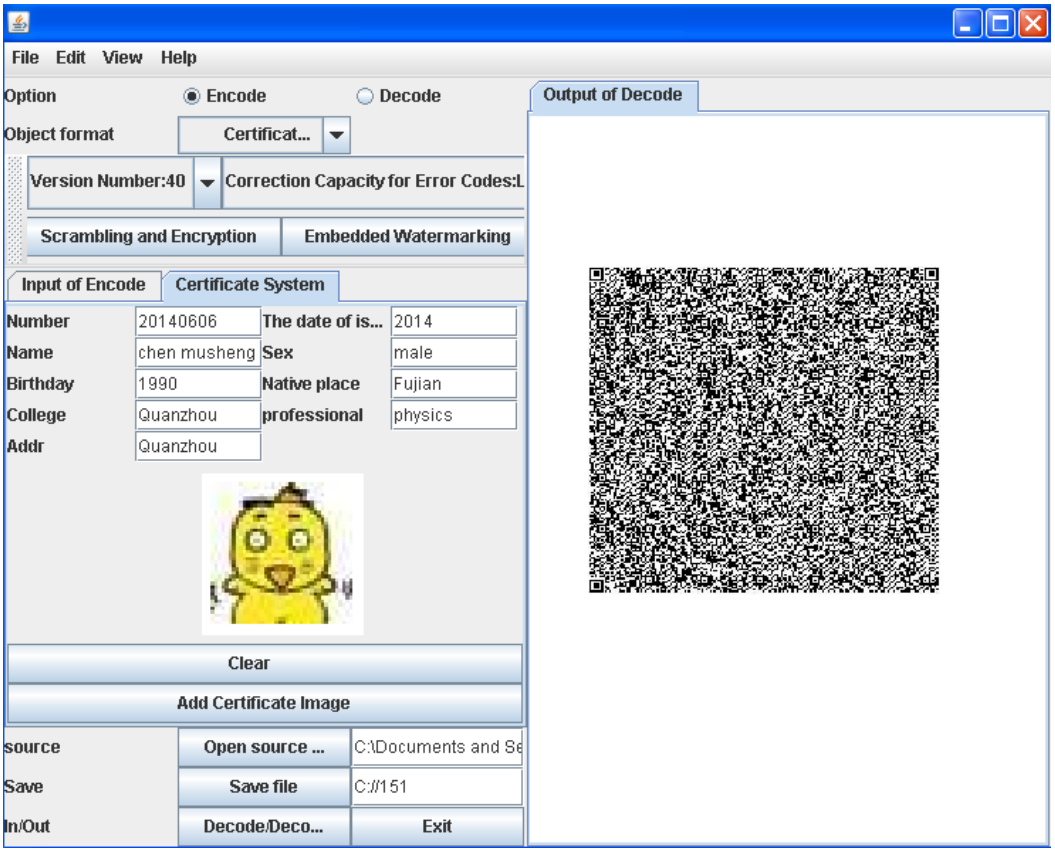

Figure 1. Student Card Management System

2.2. Decoding

If the secret key is accurately input, the related information and images of the certificate can be extracted and regained from the generated QR code. Moreover, the watermarking information can also be extracted from the generated QR code, which is used for identify whether the certificate is true or counterfeit.

2.3. Embedding of Digital Watermarking

In order to improve the anti-counterfeiting performances of the QR codes and the included contents, the digital watermarking technology is applied. There are two methods to generate digital watermarks, one is to firstly generate digital watermarking embedding for the contents to be encoded and then to generate the QR code by encoding; and the other is to perform embedding of digital watermarks for the generated QR code [6-7]. The latter method is adopted in the present work. For the embedded watermarking information, there are two choices; one is the images with special meaning imported by system, and the other is the personalized signatures by certificate holders. The digital watermarking platform is displayed in Figure 2 while the developed personalized signatures platform is displayed in Figure 3. Figure 4 shows the watermark images containing the signature information, which will be embedded in QR codes.

Figure 2. Watermarking Platform

Figure 3. Personalized Signatures System

Figure 4. Watermarking Image

3. Watermarking Embedding and Detection

In the algorithm, for watermark embedding, the QRcode image is divided into sub-images, and then one bit of the watermark information is embedded into each sub-image repeatedly by quantization. For watermark detection, the watermarked image is divided into sub-images, and then one bit of the watermark information of each sub-image is obtained by majority rule from watermarked QRcode. The algorithm is simple and detected rapidly, the quantity of embedded watermark information is large and the original image is not needed for watermark extracting[10].

3.1. Watermark Embedding

This digital watermarking technique inserts an $m \times n$ invisible watermark W into an $mk \times nk$ original image X, the watermark embedding is shown as follows:

(1)The original image X is partitioned into $m \times n$ blocks

$X_{ij}\ (i=1,2,\mathrm{L}\ ,m;\ j=1,2,\mathrm{L}\ ,n)$, the size of the sub-image X is $k\times k$.

(2)One bit of the watermark information W_{ij} was embedded into the sub-image W_{ij} accordingly; the follow equations show the watermark embedding method.

$$\lambda_{ij}=round\left(\frac{p_{ij}}{\delta}\right) \tag{1}$$

$$P_{ij}^{'}=\begin{cases}\left(\lambda_{ij}-\frac{1}{2}\right)\delta, \lambda_{ij}+w_{ij}=1(\mathrm{mod}\,2)\\ \left(\lambda_{ij}+\frac{1}{2}\right)\delta, \lambda_{ij}+w_{ij}=0(\mathrm{mod}\,2)\end{cases} \tag{2}$$

Here, p_{ij} is the image intensity values of sub-image X_{ij}, λ_{ij} is the quantization values, δ is the quantization parameter, round denotes the round operation (the nearest integers to the given number), $P_{ij}^{'}$ is the resulting encrypted block.

(3) Each bit of the watermark information W_{ij} is embedded into the sub-image X_{ij} accordingly and repeatedly with the step 2, and all the results of $P_{ij}^{'}$ is gained.

(4) All the blocks of $P_{ij}^{'}$ are incorporated and the watermarked image $X^{'}$ is gained.

3.2. Watermark Detection

Watermark information is detected by majority rule from watermarked image.

(1) The watermarked image $X^{'}$ is partitioned into $m\times n$ blocks $X_{ij}^{'}\ (i=1,2,\mathrm{L}\ ,m;\ j=1,2,\mathrm{L}\ ,n)$

(2) One bit of the watermark information is obtained by majority rule from watermarked sub-image $X_{ij}^{'}$, the follow equations show the Watermark detection method.

$$\lambda_{ij}^{'}=floor\left(\frac{X_{ij}^{'}}{\delta}\right) \tag{3}$$

$$w_{ij}^{'}=\begin{cases}1, \lambda_{ij}^{'}=1(\mathrm{mod}\,2)\\ 0, \lambda_{ij}^{'}=0(\mathrm{mod}\,2)\end{cases} \tag{4}$$

Here, floor denotes the floor operation (defined as the smallest integer smaller than or equal to the given number), δ is same value as the watermark embedding, $w_{ij}^{'}$ is the binary image of $\lambda_{ij}^{'}, \lambda_{ij}^{'}, w_{ij}^{'}$ is the matrix with size of $k\times k$.

(3) We recite numerals of "1" in binary image $w_{ij}^{'}$, if the number of "1" larger than half of the total numerals ($k^2/2$), the detected watermark information $W_{ij}^{'}=1$, else $W_{ij}^{'}=0$.

(4)The detection method is used for each sub-image $X_{ij}^{'}$ repeatedly with the step 2 and step 3, and given all the watermark information $W_{ij}^{'}$, and the detected watermarked image $W^{'}$ is gained.

4. Results of System Simulations

Owing to its strong security, platform independence, hardware structure independence, concise language, object-oriented properties, Java possess incomparable advantages over the other programming languages, which is thus selected in the development of certificate management platform in our study. Figure 5 and Figure 6 display the developed software platform. To testify the validity and reliability of the platform, we selected the student's certificates and performed simulations. During the simulations, the input texts and the added pictures as shown in Figure 1 were adopted as the encoding information; the number of scrambling transformations was set as N = 12; while the generated QR code (*i.e.*, the signature of the certificate holder, as shown in Figure 4) was embedded in the watermarks. The experimental simulation results as listed below. Specifically, Figure 5 displays the watermarked QR code by encoding; Figure 6 displays the decoding results when the input of the number of scrambling transformations was 12 while the extracted watermark image is shown in Figure 7. When N = 10 was input, the image of the certificate holder cannot be accurately identified, as shown in Figure 8. The results indicate that, using the developed platform, the watermark image can be accurately extracted while the decoding results are correct only when the number of scrambling transformations is accurately input. When the input of N is incorrect, the decoding of certificate image cannot work; *i.e.*, the number of scrambling transformation can be employed as an effective encryption key for certificate images. On the other hand, when the watermarked image was partly damages, as shown in Figure 9, the certification information as presented in Figure 6 as well as the watermarked information as presented in Figure 7 can still be accurately extracted. Conclusively, both the certificates with the adoption of two-dimensional barcodes and the encrypted watermarks on two-dimensional barcodes have strong shearing resistance performance.

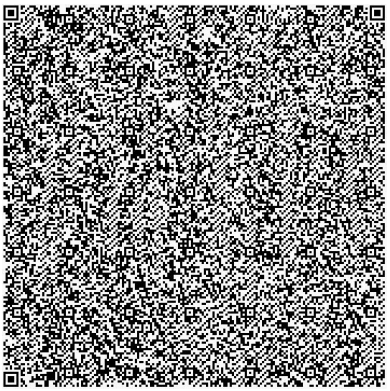

Figure 5. Encode Result

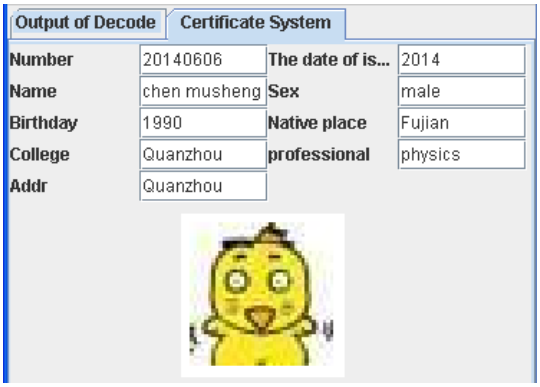

Figure 6. Decode Result of N=12

Figure 7. Extracted Watermarking

Figure 8. Result of N=10

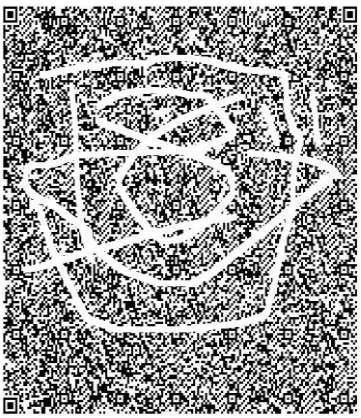

Figure 9. QR Code with Partly Damages

5. Conclusion

Owing to their excellent characteristics such as high information density, low costs of applications, easy operation and desirable security, the two-dimensional barcodes are fairly suitable for the applications of certificate management and anti-counterfeiting systems. By embedding the digital watermarking information into the two-dimensional barcodes, the certificates can possess double anti-counterfeiting functions, *i.e.*, the anti-counterfeiting performance of the certificates can be significantly improved. In the present work, the digital watermarking encryption technique and two-dimensional barcode technology were combined and applied in the certificate anti-counterfeiting system, which will pose a positive impact on the current certificate management and anti-counterfeiting systems in China. Consequently, the developed platform exhibits a broad application prospect. In future, we can make some appropriate changes on this platform so that it can be applicable for the other systems with high security requirements such as ticket system.

Acknowledgement

This work is supported by the Science and Technology Project of FuJian Province (Grant No: JA13262).

References

[1] L. Wang and X. Liu, "An Improved Two dimensional Code Encoding Approach for Publications", 2010 2nd International Conference on Signal Processing Systems (ICSPS), vol.2, **(2010)**,pp.533-536.
[2] K. Thomas, K. Tobias and Eva Carolina Pataki, "2D-Codes Technology and Application", Business & Information Systems Engineering, no.1, **(2011)**, pp.45-48.
[3] M. Kelly Schultz, "A case study on the appropriateness of using quick response (QR) codes in libraries and museums", Library & Information Science Research, vol.34, [].2, **(2013),**pp.207-215.
[4] L. Tarjan, I. Šenk and S. Tegeltija, "A readability analysis for QR code application in a traceability system", Computers and Electronics in Agriculture, vol.109, **(2014)**, pp.1-11.
[5] D. Lorenzi, J. Vaidya and S. Chun, "Enhancing the government service experience through QR codes on mobile platforms", Government Information Quarterly, vol.31, no.3, **(2014)**, pp.31:6-16.
[6] R.-S. Xie, K.-S. Wu and G.-P. Xu, "Research on Anti-Counterfeiting Quick Response 2D Barcode Techniques Based on Digital Watermark", Shanghai Jiaotong Univ., vol.18, no.4, **(2013)**, pp.443-447.
[7] Y. Fang, H. Fu and Y. Zhagn, "Twodimension Barcode and Fingerprint Identification", Computer and Digital Engineering, no.1, **(2009)**, pp.111-117.
[8] Z.-P. Wang, S. Zhang and H.-Z. Liu, "Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code", Optics Communications, vol.332,

(2014), pp.36-41.
[9] Espejel-Trujillo, Castillo-Camacho and Nakano-Miyatake. Identity Document Authentication Based on VSS and QR Codes. Procedia Technology, vol.3, **(2012)**, pp.241-250.
[10] X. Li, "Geometric Attack Resistant Image Watermarking in Spatial Domain", Acta Automatica Sinica, vol.34, no.7, **(2008)**, pp.832-837.

Author

Musheng Chen, he received his Master degree in 2005 from Jinan University. Now he is a associate professor of Quanzhou Normal University. His current research interests include 2-D barcode digital watermarking and image processing.

