Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **5**, September **2017**

SVQR : A Novel Secure Visual Quick Response Code and Its Anti-counterfeiting Solution

Shi-Jian Liu[1,2], Jing Zhang[1,2], Jeng-Shyang Pan[1,2] and Cai-Jie Weng[1]

[1]School of Information Science and Engineering
[2]Key Laboratory of Big Data Mining and Applications of Fujian Province
Fujian University of Technology
No3 Xueyuan Road, University Town, Minhou, Fuzhou, Fujian, 350118, China
liusj2003@fjut.edu.cn; jing165455@126.com; jspan@cc.kuas.edu.tw

Received May, 2017; revised July, 2017

Abstract. *With the development of information science and increasingly demands for convenient communication, Quick Response (QR) codes are now popularly used all over the world. However, security problem is not considered in the designation of QR code, which makes it unsuitable for application requiring credibility. This paper presents an authentication solution to realize the anti-counterfeiting for message which is encoded following QR code standard. The solution includes a proposed secure and visual improved QR code involving digital signature and watermarking techniques, and a delicate authentication scheme. The effective and efficient of the proposed method are proved by experiments and analyses.*
Keywords: QR code, Digital signature, Watermarking, Anti-counterfeiting, Visual effect.

1. **Introduction.** With the popularity of mobile devices (e.g., cellphone) and online payment, Quick Response code now plays an important role in our daily lives. As an automatic recognition method with high accuracy, low-cost, high-speed reading and high-reliability, QR 2D bar code has been widely applied in many fields [1]. Another reason for the commonly use of QR code is that there has no secret for QR code encoding and decoding, it means every one can use it as long as some specified standards are followed. This open strategy makes QR codes popular, but it also causes serious security issues.

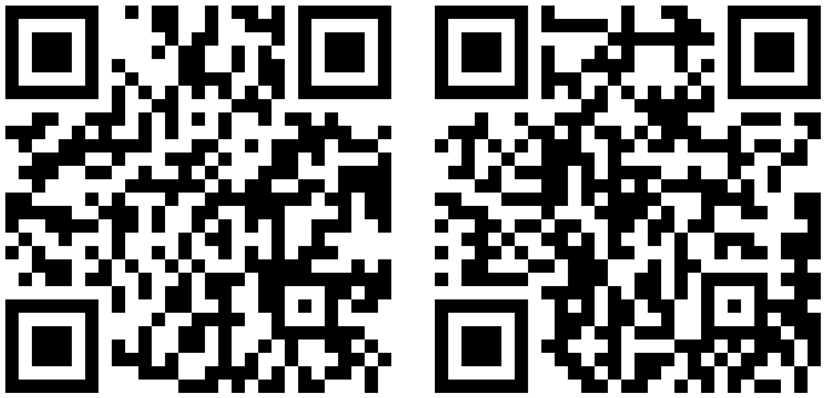


Figure 1. An example of QR code trap.

For example, aiming for stealing sensitive personal information such as bank account or credit card information, attackers may use forged QR code which encodes fraudulent Web site and pretends as the entrance of a legitimate one to confuse the users and induce them to reveal important data. Fig. 1 shows such an instance, where the two QR codes seems no difference for us but contains definitely not the same messages. Besides, the lack of semantic function is another obstacle when employing QR codes as communication medium. Because QR code generally appears as a combination of chaotic distributed small black-white squares, which makes the encoded message hardly be presumed. For this reason, annotations, such as the strings below QR codes showed in Fig. 1, have to be added as the interpretations.

In order to simultaneously improve the visual effect and security of QR code without sacrifice its readability, a visual improvement strategy is firstly adopted to add a specified picture to the QR code as semantic background. Additionally, a security mechanism based on digital signature [2] and watermarking algorithms [3] is used to produce a Secure and Visual QR (SVQR) code. A novel anti-counterfeiting scheme based on the proposed SVQR code is also introduced for encoded message authentication.

The rest of the paper are organized as follows. In Section 2, basic principles and works related to ours are introduced. Section 3 presents the proposed method in details. Experiments and results are given in Section 4. Section 5 concludes the paper.

2. **Fundamental and Related Work.**

In this section, we first provide a brief introduction to QR code standard (Section 2.1), then methods related to security improvements (Section 2.2) and visual effect improvements (Section 2.3) for QR codes are discussed successively.

2.1. **The standard.**

As showed in Fig. 1, QR codes are two-dimensional bar codes that encode message in both vertical and horizontal direction, which was developed by the Japanese Denso-Wave Company in 1994 [4]. A classic QR code structure consisting of function patterns and encoding region can be seen in Fig. 2(a). Messages (or data) can be encoded into QR code and decoded from it abiding by some well accepted standards, such as the "ISO/IEC 18004" [5] introduced by the International Organization for Standardization, in which totally 40 versions of QR codes are defined with different modules size and data capacities. The term "module" is referred to as the smallest black/white square region in equal size which represents 1/0 accordingly (see Fig. 1). And from Version 1 to 40, the number of modules in QR code increases from 21×21 to 177×177 in steps of four modules per side [5]. Fig. 2(b) shows an example of QR code of version 2.

QR codes have many good features, for example, they are readable from different angles. Additionally, thanks to the Reed-Solomon Codes [6] based Error Correction (EC) mechanism, data can be decoded successfully even if the code is partially covered or damaged. Actually, there are four error correction levels for each version, which are referred to as L (Low), M (Medium), Q (Quartile) and H (High) in increasing order of correction capacity allowing recovery of up to 7%, 15%, 25% and 30% of codewords respectively. For example, QR code shown in Fig. 2(b) has EC level equals M. The term "codeword" is referred to as specific region consisted of 8 modules, such as $D1$ and $E1$ depicted in Fig. 2(b). Messages are encoded in the data codewords while Reed-Solomon Codes are encoded in the EC codewords.

2.2. **Security improvement.**

Information security has always been an attractive area for people all over the world, it is because most of us care so much about the safety of our properties such as private personal information and so one, and QR code based communication is no exception. The published QR code security methods can be classified

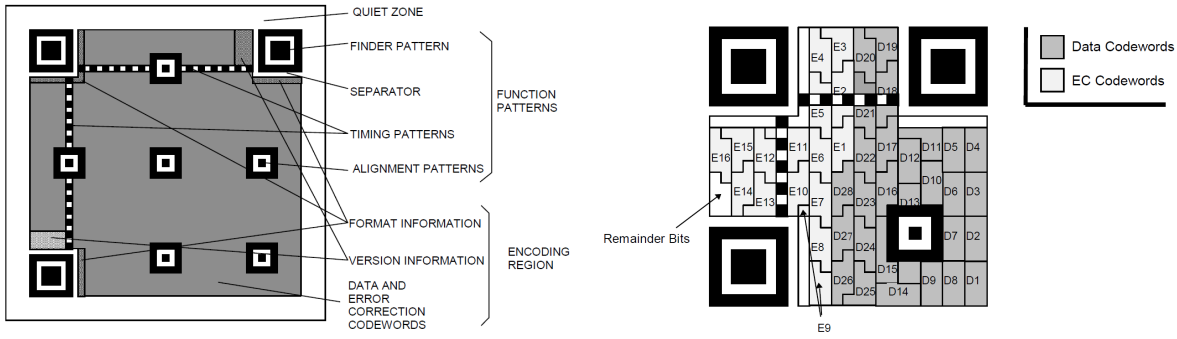


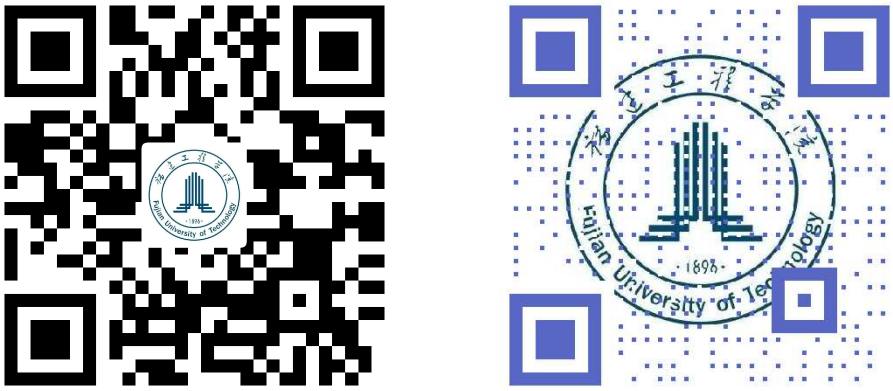
FIGURE 2. Standard of QR code [5]. (a) Structure of a QR Code. (b) A QR code of version 2 with Medium EC level.

into two categories in our perspective. Methods in the first group pay attention to QR code based private message sharing. For example, the secret message may be encoded into a QR code and embed into the spatial domain [7, 8] or the frequency domain [9, 10] of a cover image. In this case, QR code acts just as a ordinary medium and nothing is changed to the code itself, so they are meaningless with regards to QR code improvements. On the contrary, Bui et, al. [11] and Lin et, al. [12] both use the EC capacity of the QR code to hide secret message. In other words, the bits encoded in the standard QR code will be replaced with errors from which secret message can be recovered. In a word, these methods achieve the private message sharing by sacrificing the possibility of error correction.

The second group focuses on QR code based message authentication. For instance, the encoded message may be released by a trustworthy merchant but propagated in an insecurity environment, the question is how to prove the safety of received QR code in the view of customers. To solve this problem, most methods use watermarking based schemes. Specifically, a watermark will be embedded into the frequency domain of a QR image with Discrete Wavelet Transform [1, 13], Discrete Cosine Transform [14] and Discrete Fourier Transform [15] to protect the copyright of a QR image. Considering the limitation of low power and low computational capability barcode devices, the computational complexity will become one of the major drawbacks for the frequency domain based methods. Different from them, a two-level QR code is proposed by Tkachenko et, al. [16], they embed private data by replacing the black modules by specific textured patterns, which are sensitive to the print-and-scan process. For this reason, the document authentication can be achieved.

Our work also achieves authentication, but with different methodology. Firstly, we aim to certificate message encoded in the QR code. Secondly, digital signature and watermarking method in spatial domain are combined in the proposed method. Additionally, to the best of our knowledge, among the published methods, none of them uses colored QR code for authentication. This is probably because print-and-scan of color image is more expansive, but with the popularity of paperless environment, security requirements for colored QR code as proposed in this paper will be booming.

2.3. **Visual improvement.** There are many solutions to improve the visual effect of QR code. Among them, the most popular one is referred to as logo embedded method in this paper (see Fig. 3(a)), because there is a specified small logo embedded at the center of QR code in the solution. In other words, some modules are erased in order to show the visual



(a) (b)

FIGURE 3. QR code visual improvement method. (a) The logo embedded method which covers a small logo in the center of QR code; (b) A picture is added to the entire QR code region as a background.

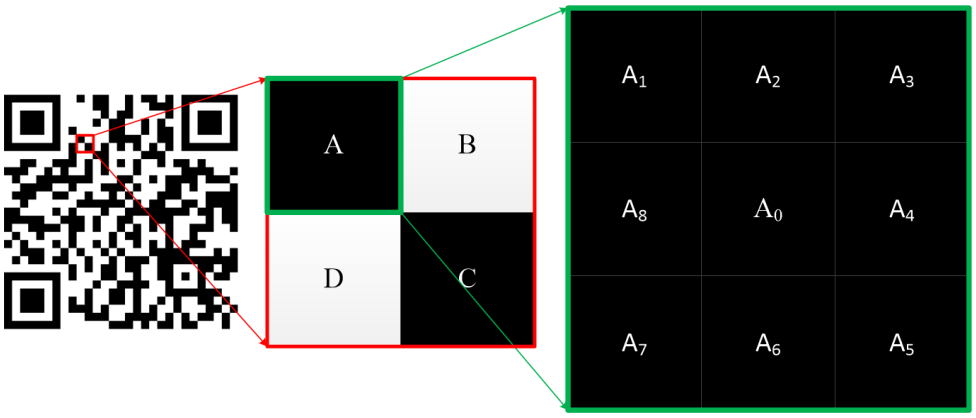


FIGURE 4. The strategy of subdividing each module in order to add background picture to a QR code.

information on the condition that the missing data can be recovered by above described EC mechanism. From Fig. 3(a) we can see that the visual unpleasant problem is relieved to some extent, but it would be much better if we can add a picture to the entire QR code region as a background (see Fig. 3(b)) comparing to module modification in a small area. To achieve the purpose, one feasible solution is to equally divide every module into 9 parts. For example, we can split the module A showed in Fig. 4 into $A_0, A_1, ..., A_8$. When covering the QR code on a background picture, we shall always keep the A_0 part and do whatever we want to others. This strategy has already been commercialized by a software company named Visualead in Israel [1], but the implementation details are unpublished.

Others, such as methods proposed in [17, 18, 19], prefer to sacrifice EC function for visual improvement, which may harm to their decoding rate more or less. Other than pursuing optimize visual effect, the subdivision based method is adopted in our work, since anti-counterfeiting solution with high decoding rate is the major concern of this work.

[1] http://www.visualead.com

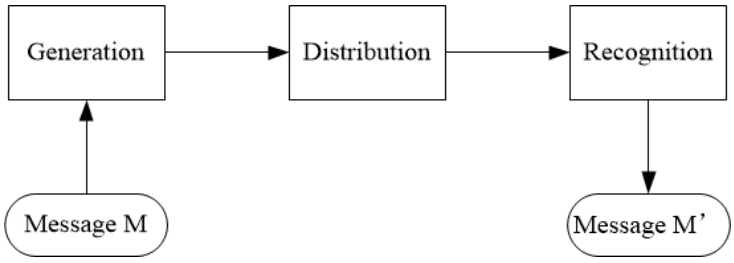


FIGURE 5. The cycle of QR code usage.

3. **The Proposed Method.** As a information medium, QR code is born to be distributed from one to another during the communication. Fig. 5 depicts the cycle of QR code usage from its generation to the recognition. The most possible period for attackers to forge the code is during the distribution time, when anyone can receive the QR code and pretend to be the authors. While, the aim of this work is to find a robust solution in order to make the proposed SVQR code capable of anti-counterfeiting. Specifically, safety strategies will be designed for the generation and recognition/authentication phase to make sure any unauthorized modification will be found and alerted. The generation and authentication of the proposed SVQR code will be introduced in Section 3.1 and 3.2 respectively.

3.1. **The generation phase.** Let M be the message which is going to be shared by QR code. Traditionally, M will be encoded and delivered to whoever interested without information safety guarantee. In order to generate a QR code with authentication ability, we introduce the Fig. 6 demonstrated generation scheme. Besides M, the inputs of the generation phase also include a background color image I and a pair of key, namely a private key K_{pri} and a public key K_{pub} offered by a trusted certificate authority (CA). The output is a SVQR code C_{sv}.

As showed Fig. 6, on the one hand M will be transformed into digest D using hash operation, then encrypted to form a signature S using K_{pri}. On the other hand, it will be encoded following QR code standard and then formed a visual QR code C_v with I. Finally, C_{sv} is obtained by watermarking S into C_v.

It is worth point out that, the use of I is optional in our scheme. But since the image can not only increase the difficulty of counterfeiting, but also greatly improve the semantic expression, it is highly recommended by us. Besides, there are quantity of color image based watermarking algorithm could be used.

After the SVQR code has been generated, it may propagate within an unknown communication environment and be treated as the input of a authentication procedure (see next Section).

3.2. **The authentication phase.** The workflow for SVQR code authentication is depicted in Fig. 7. As the figure shows, as soon as both the SVQR code and its associated public key K_{pub} are available for the users, two digest D_1 and D_2 can be obtained from the decoded message M' and extracted watermark (i.e., the signature S') respectively. The idea is, since the digital signature is proved to be safe, then if D_1 equals D_2, it means M' is trustworthy and equals to the M. Otherwise, the SVQR code must be modified.

A interest phenomenon is that the certification can be achieved for SVQR codes with different background images as long as the signatures the same. In this case, authors can use SVQR codes in different appearances to delivery the same message, which is a commonly adopted way. For example, different posters may be painted on the cans of same goods.

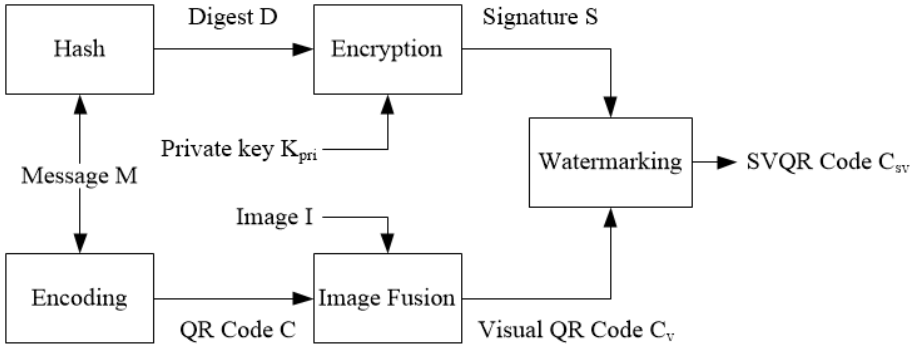


FIGURE 6. Workflow for SVQR code generation.

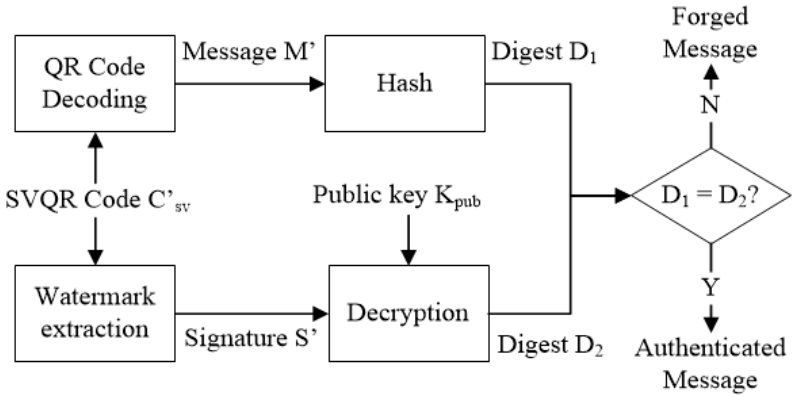


FIGURE 7. Workflow for SVQR code authentication.

4. **Experiments and Results.** In order to validate the proposed method, various experiments are carried out, and their results are illustrated in this Section.

4.1. **Readability.** As a medium for communication and information sharing, the proposed SVQR code should firstly be readable using general QR code scanning softwares. Therefore, SVQR codes in different versions with different background images are generated as shown in Fig. 8. In this experiment, the key pairs generation, encryption(for signature) and decryption are implemented by Crypto++ [2], SHA-1 [20] is used as the hash operation, watermarking is realized based on the Least Significant Bit (LSB) strategy [3], and QRencode [3] is adopted for the encoding. General tools aiming for QR code decoding involved in the experiments include WeChat, which is a famous social software in China, and others implemented based on ZXing [4] and ZBar [5], etc. And tested SVQR codes can be decoded successfully and correctly.

4.2. **Efficiency.** We also record the average time consumptions for SVQR code generation and authentication. The authentication is tested on a common laptop computer (CPU: Intel Core 2.2GHz, Memory: 8GB). Fig. 9 shows that the average time consumption for generation of SVQR code is nearly 0.04 seconds, and the average time consumption for SVQR code based authentication is about 0.14 seconds, which means the proposed method is a very efficient solution.

[2]https://www.cryptopp.com
[3]https://github.com/fukuchi/libqrencode, https://fukuchi.org/works/qrencode/manual
[4]https://github.com/zxing/zxing
[5]https://github.com/ZBar/ZBar

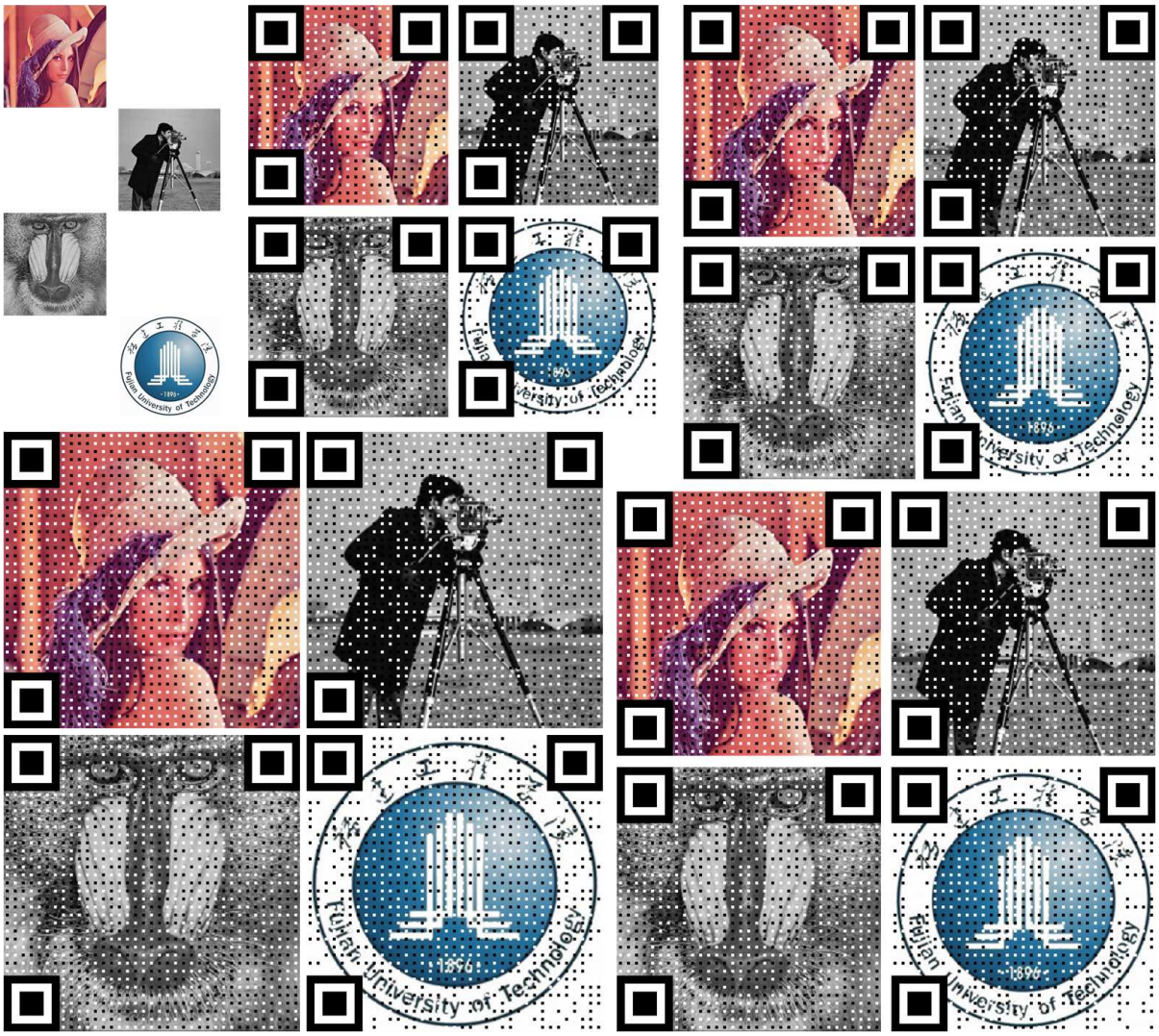
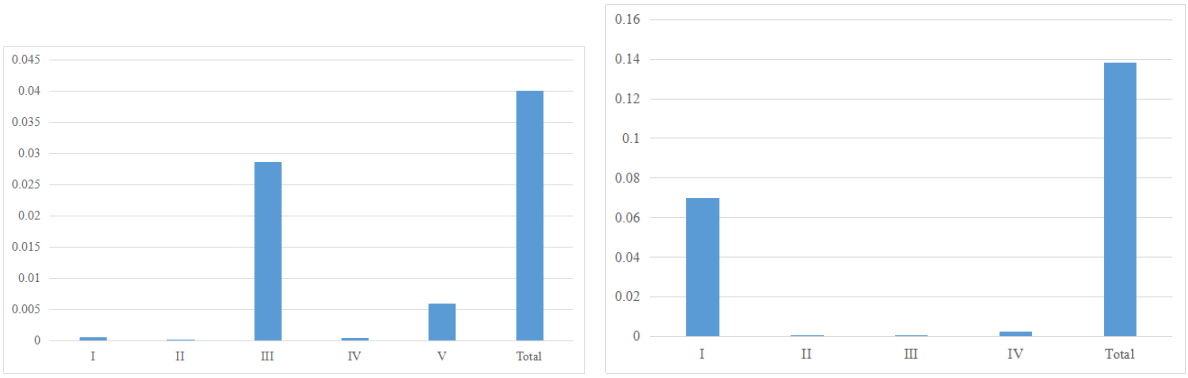


FIGURE 8. SVQR codes in different versions for readability tests.



(a) (b)

FIGURE 9. Time records for the SVQR code based anti-counterfeiting. (a) The average timing (recorded in seconds) for (I) encoding, (II) hash, (III) signature, (IV) Visual improvement, (V) watermarking and (Total) the entire generation procedure; (b) The average timing (recorded in seconds) for (I) decoding, (II) hash, (III) watermark extraction, (IV) signature extraction & verification and (Total) the entire authentication procedure.

4.3. **Analysis of the anti-counterfeiting scheme.** Since a SVQR and its associated public key are the only two inputs of the authentication process, and we assume that the public key offered by CA is always be faithful, therefore the SVQR code is critical to the certifications. And the proposed method can make sure there is no way for attacker to forge the original message, because the D_1 and D_2 won't be equal if :

1. the message is right but the signature (i.e., watermark) has been changed;
2. the message has been modified, while the signature is right;
3. both message and signature have been modified.

The first two conditions can easy be understood, while the last one is true because after changing the message, the attacker has to forge the signature simultaneously to make sure one digest equal to the other, which is impossible because the matched signature can only be found by encrypting D_1 with the right private key, and it is unknown to others except the author and CA.

5. **Conclusion and Future work.** The usage of QR code for communication becomes fashion all over the world recently. However, problems such as unpleasant visual effect and lack of security mechanism may become obstacles of its applications. In order to solve these problems, an improved QR code and its authentication scheme are proposed in this paper. Based on the digital signature and watermarking techniques, the proposed SVQR code has the ability of anti-counterfeiting. It is also capable of semantic expression, because the SVQR code can take a meaningful color image as its background. Experiments and analyses demonstrate the effective of the proposed SVQR and authentication scheme.

The proposed method do not support the print-and-scan SVQR code currently, which is a limitation resulting from the usage of LSB based watermarking. The problem may solved by involving new watermarking technique which support embedding and extracting watermark from printed image. And it will be one of the future directions of our research.

Acknowledgment. This work is supported by the Scientific Research Project in Fujian University of Technology (GY-Z160130, GY-Z160138, GY-Z160066), the Natural Science Foundation of Fujian Province of China (2017J05098), Young and Key Project of Fujian Education Department Funds (JZ160461) and Project in Fujian Provincial Education Bureau (JAT160328). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] R. Xie, C. Hong, S. Zhu and D Tao, Anti-counterfeiting digital watermarking algorithm for printed QR barcode, *Neurocomputing*, vol.167, no.C, pp.625–635, 2015.

[2] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the Acm*, vol.26, no.2, pp.120–126, 1983.

[3] J. S. Pan, H. C. Huang and L. C. Jain, *Intelligent Watermarking Techniques*, World Scientific, 2004.

[4] Denso-Wave Inc., *QR code standardization*, Available: http://www.qrcode.com/en/index.html, 2003

[5] *Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification*, ISO/IEC 18004:2006, 2006.

[6] S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Applications*, John Wiley & Sons, Inc. 1999.

[7] H. C. Huang, F. C. Chang, and W. C. Fang, Reversible data hiding with histogram-based difference expansion for QR code applications, *IEEE Transactions on Consumer Electronics*, vol.57, no.2, pp.779C-787, 2011.

[8] S. Dey, K. Mondal, J. Nath and A. Nath, Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm, *International Journal of Modern Education & Computer Science*, vol.4, no.6, pp.59C-67, 2012.

[9] C. H. Chung, W. Y. Chen, and C. M. Tu, Image Hidden Technique Using QR-Barcode, *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, pp.522–525, 2009.
[10] W. Y. Chen and J. W. Wang, Nested image steganography scheme using QR-barcode technique, *Optical Engineering*, vol.48, no.5, pp.057004-01C-057004-10, 2009.
[11] T. V. Bui, N. K. Vu, T. T. P. Nguyen, I. Echizen, and T. D. Nguyen, Robust Message Hiding for QR Code, *10th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process (IIH-MSP)*, pp.520-C523, 2014.
[12] P. Y. Lin, Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code, *IEEE Transactions on Industrial Informatics*, vol.12, no.1, pp.384–392 , 2016.
[13] M. Sun, J. B. Si and S. H. Zhang, Research on embedding and extracting methods for digital watermarks applied to QR code images, *New Zealand Journal of Agricultural Research*, vol.50, no.5, pp.861C-867, 2007.
[14] L. Li, R. L. Wang and C. C. Chang, A Digital Watermark Algorithm for QR Code, *International Journal of Intelligent Information Processing*, vol.2, no.2, pp.29C-36, 2011.
[15] S. Rungraungsilp and M. Ketcham, Data Hiding Method for QR Code Based on Watermark by compare DCT with DFT Domain, *Int. Conf. Comput. Commun. Tech. (ICCCT'2012)*, Phuket, pp.144–148, 2012.
[16] I. Tkachenko, W. Puech, C. Destruel, O. Strauss, J. M. Gaudin and C. Guichard, Two-Level QR Code for Private Message Sharing and Document Authentication, *IEEE Transactions on Information Forensics & Security*, vol.11, no.3, pp.571–583, 2015.
[17] H. K Chu, C. S. Chang, R. R. Lee and N. J. Mitra, Halftone QR codes, *Acm Transactions on Graphics*, vol.32, no.6, pp.1–8, 2013.
[18] S. S. Lin, M. C. Hu, C. H. Lee and T. Y. Lee, Efficient QR Code Beautification With High Quality Visual Content, *IEEE Transactions on Multimedia*, vol.17, no.9, pp.1515–1524, 2015.
[19] L. Li, J. Qiu, J. Lu and C. C. Chang, An aesthetic QR code solution based on error correction mechanism, *Journal of Systems & Software* vol.116, no.C, pp.85–94, 2016.
[20] D. Eastlake and P. Jones, *US Secure Hash Algorithm 1 (SHA1)*, RFC Editor, 2001.