文章编号：2095-2163(2020)08-0014-05 中图分类号：TP309.7 文献标志码：A

基于隐写和 VSS 的二维码安全认证技术研究

燕雨薇[1]，余 粟[2]
（1 上海工程技术大学 电子电气工程学院，上海 201620；2 上海工程技术大学 图文信息中心，上海 201620）

摘 要：快速响应码(QR 码)以存储信息量大、编解码速度快、安全性高等特点，广泛应用于各个领域。但 QR 码本身并不具备安全保护能力，通过分析其编解码原理，本文提出一种结合信息隐藏和可视秘密共享的 QR 码安全认证技术，可应用于用户信息传递及身份认证。实验证明本方法具备可行性，且具有透明性高、计算成本低、效率快等优点，提高了信息传递的安全性。

关键词：QR 码；信息隐藏；消息认证；LSB；可视秘密共享

Research on security and authentication technology of two-dimensional code based on steganography and visual secret sharing

YAN Yuwei[1], YU Su[2]
(1 School ofElectrical and Electronic Engineering, Shanghai University of Engineering Science, Shanghai 201620, China;
2 Library and Information Center, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】 Quick Response(QR)code is widely used in various fields because of its large storage capacity, fast codec and high security. But the QR code itself does not have the security capabilities. By analyzing its codec principle, a new kind of QR code security authentication technology combining information hiding and visual secret sharing is proposed, and it can be applied to the transmission of user information and identity authentication. Firstly, user information is used to generate standard QR code. Secondly, the redundancy characteristic of error correction code system is utilized to realize the hidden of authentication information. At last, to realize secret sharing and ensure that information is available only with the permission of both parties, the obtained QR code is divided into two sub-images by using visual secret sharing technology.The experiments show that this method is feasible and it has the advantages of high transparency, low cost, low efficiency and quick calculation.What's more, by using this method the security of information transmission is improved.

【Key words】 QR code; steganography; message authentication; LSB; visual secret sharing

0 引 言

QR 码(快速响应码)是一种矩阵式二维码，以识别效率高、存储信息量大、纠错能力强等特点，广泛应用于数据传输、产品营销、支付系统、信息管理等方面。QR 码传输具有便利性，但所携信息存在很大的安全隐患，如信息泄露、伪造、篡改等。目前，针对提高二维码安全性的研究已有众多成果。例如，先将信息加密[1]再编码，能够有效提高 QR 码携带信息的安全性；牛夏牧等人利用隐写技术将机密信息隐藏在二维码中[2]；Jen-Bang Feng 等人提出使用基于图像的可视秘密共享技术来传输秘密信息[3]等等。

本文利用 QR 码的冗余特性，结合隐写术和可视秘密共享技术，将 QR 码应用在用户身份的安全认证中。该方法加解密过程效率高，无需额外传递密钥，在提高 QR 码的真实性和机密性、实现身份认证的同时，有效地保证了信息的安全。并且，只有在用户许可的前提下，管理员才能获取到用户信息，保证了用户信息不被泄露。

1 基础理论知识

QR 码编码包括信息编码、纠错编码等过程，具体流程如图 1 所示。与传统一维条码不同，使用 Reed-Solomon (RS)纠错码，使 QR 码具有很强的容错纠错能力。

图 1 QR 码编码流程

Fig. 1 The coding process of QR Code

1.1 Reed-Solomon (RS)纠错码

Reed-Solomon (RS)是一种纠错算法，对原始

基金项目：上海市科委资助项目(17511110204)。

作者简介：燕雨薇(1995-)，女，硕士研究生，主要研究方向：计算机应用技术；余 粟(1962-)，女，硕士，教授，主要研究方向：计算机仿真应用研究。

收稿日期：2020-04-25

数据进行计算得到的校验码即是纠错码。在纠错能力范围内，根据冗余的校验码可以确保原始数据的可恢复性。其基本原理如下：

假设原始数据 $D=(d_1, d_2,\cdots,d_n)$，希望通过计算得到冗余校验数据 $C=(c_1,c_2,\cdots,c_m)$，能够容纳 m 份数据错误。

(1)通过多项式计算得到冗余数据：

$$F*D=\begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \cdots & \cdots & \vdots & \cdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{pmatrix} * \begin{pmatrix} d_1 \\ d_2 \\ \cdots \\ d_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \cdots \\ c_m \end{pmatrix} = C. \tag{1}$$

(2)可以将 F 定义为 $m\times n$ 矩阵，令 $(x_1-1, x_2=2,\cdots,x_n=n)$，并且由 F 构造矩阵 A，得到如下等式：

$$A*\begin{pmatrix} d_1 \\ d_2 \\ \cdots \\ d_n \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \vdots & \cdots \\ 0 & 0 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & n \\ \cdots & \cdots & \vdots & \cdots \\ 1 & 2^{m-1} & \cdots & n^{m-1} \end{pmatrix} * \begin{pmatrix} d_1 \\ d_2 \\ \cdots \\ d_n \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ \cdots \\ d_n \\ c_1 \\ c_2 \\ \cdots \\ c_m \end{pmatrix}, \tag{2}$$

其中，A 由一个 n 阶单位矩阵和 $m\times n$ 的 Vandermonde 矩阵组成。A 中任意 n 行都与线性无关，所以当错误数据小于 m 时，A 均是可逆的，从而计算恢复出原始数据。实际应用中，RS 编码器中的计算均是在伽罗华域进行。

1.2　最低有效位(LSB)隐写技术

LSB(least-significant-bit)是一种信息隐藏技术[4]，即将信息嵌入到静止图像中。图像是由许多像素组成，利用 LSB 修改像素的最低位，使人眼不易察觉。以图 2 所示，将字母‘A’隐藏到部分图像中为例，简要说明 LSB 原理。

一个好的隐写技术要有良好的视觉或者统计上的不可感知性，以及足够的有效载荷。本文采用的隐写方法是改进后的 LSB 技术，提高了原始 LSB 的隐蔽性，该方法每次对两个像素进行操作。选取完成信息隐写后图像的两个像素，其像素值分别为 y_i，y_{i+1}。根据像素值可以得到两位隐藏的信息，分别用 s_i, s_{i+1} 表示。第 i 位信息等于 y_i 的最低有效位，第 $i+1$ 位信息等于由 y_i，y_{i+1} 表示的函数，公示表示为

$$\begin{cases} s_i = LSB(y_i), \\ s_{i+1} = f(y_i, y_{j+1}. \end{cases} \tag{3}$$

其中，$f(y_i,y_{i+1}=LSB(\lfloor y_i/2\rfloor + y_{i+1})$，相比于原始 LSB 方法，改进后的方法给原始图像带来的变化较小，且降低了隐秘信息被侦测到的概率。其隐写方法使用伪代码表示如下。

图 2　信息隐藏示例

Fig. 2　The example of information hiding

表 1　改进的 LSB 算法伪代码

Tab. 1　The pseudo-code of improved LSB algorithm

输入：待隐藏图像的任意两个像素值 x_i，x_{i+1}；两个隐藏信息位 s_i，s_{i+1}

输出：信息隐藏后图像对应的两个像素值 y_i，y_{i+1}

```
if s_i = LSB(x_i)
  if s_{i+1} ≠ f(x_i, x_{i+1}
    y_{i+1} = x_{i+1} ± 1
  else
    y_{i+1} = x_{i+1}
  end
else
  if s_{i+1} = f(x_i - 1, x_{i+1})
    y_i = x_i - 1
  else
    y_i = x_i + 1
  end
    y_{i+1} = x_{i+1}
  end
```

1.3　可视秘密共享(VSS)技术

可视秘密共享技术是一种基于图像的信息隐藏技术，可将信息隐藏在多个子图像中。通过合成图像即可得到秘密信息，无需秘钥。秘密共享，也称为 (k,n) - *VSS* 门限方案[5]，即将秘密图像加密成 n 个分享图像，分别由 n 个人保管，解密时需要至少 k 个人将各自的分享图像合成才能获得秘密信息，否则将无法正确显示。

本文采用的是基于随机网格的 (2,2) - *VSS* 门限方案。由于 QR 码为黑白图像，即二值图像，故本文只讨论针对二值图像的 (2,2) - *VSS* 方案。在二值图像中，数值 1 代表黑色像素，数值 0 代表白色像素。需要将秘密图像加密成 2 个分享图像，也就是

将一个像素分为两个子像素,可分为四种情况[6],如图 3 所示。

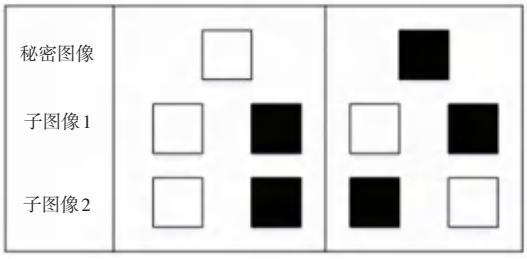


图 3 (2,2)-VSS 原理图

Fig. 3 Schematic diagram of (2,2)-VSS

假设秘密图像的任意一个像素值为 p,两个分享图像的对应值 p_1,p_2 的生成及解密过程如下:

(1)随机生成 p_1,其值为 0 或 1;

(2) p_2 的值由等式(4)计算得出。由图 3 可知,若 $p=0$,则 p_1 和 p_2 相同,若 $p=0$,则 p_1 和 p_2 相反,其中 $\bar{p}_1$ 表示 p_1 的按位互补操作;

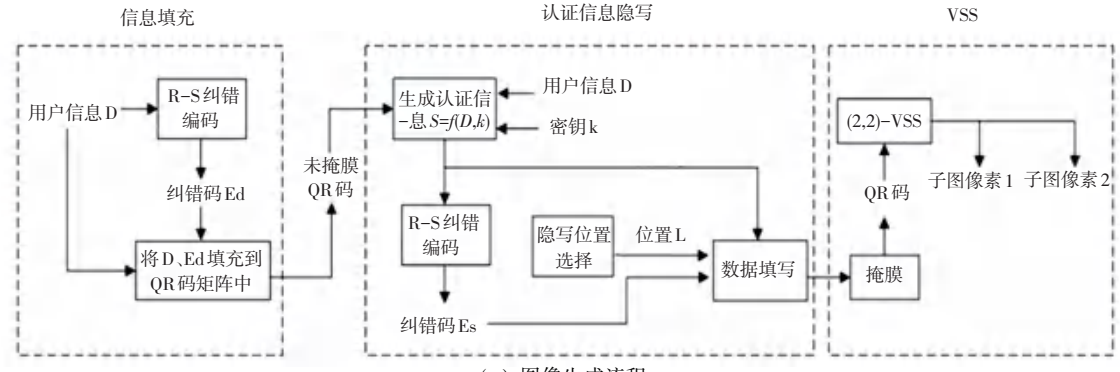
$$p_2=\begin{cases}p_1, & \text{if } p=0;\\ \bar{p}_1, & \text{if } p=1.\end{cases} \tag{4}$$

(3)根据 p_1,p_2 的值,按等式(5)可解密得到 p'。

$$p'=p_1\otimes p_2. \tag{5}$$

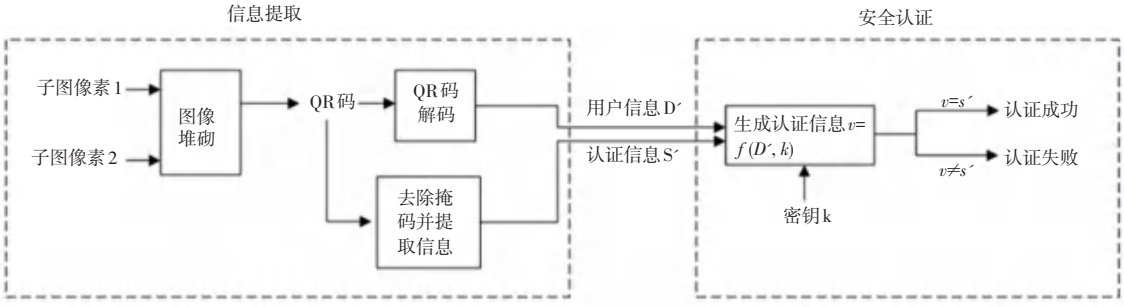
2 QR 码安全认证

选择 QR 码作为加密和认证载体,是因为 QR 码编解码速度快,且用其隐藏加密信息效率高,能够快速解密。为实现安全认证功能,首先对用户信息进行编码,初步生成 QR 码;其次根据用户信息生成认证信息并隐写入 QR 码中;最后利用可视秘密共享技术,将所得 QR 码分为两个子图像,所得子图像由用户和管理员分别保留。具体流程如图 4 所示。



(a) 图像生成流程

(a) Process of image production



(b) 安全认证流程

(b) Process of Safety certification

图 4 安全认证实现流程

Fig. 4 Process of security authentication implementation

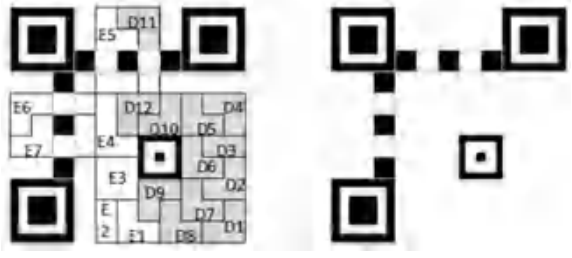
2.1 图像生成

图像生成包括 QR 码信息填充、认证信息隐写、可视秘密共享三大步骤,如图 4(a)所示。其中,信息填充时不对 QR 码矩阵进行掩膜操作,当数据信息隐写完成后才对其进行掩膜操作。目的是保证 QR 码黑白像素分布更加均衡。具体步骤如下:

(1)信息填充。将用户信息作为输入信息,进行数据编码以及纠错码编码,并将所得信息序列分块填充到相应规格的 QR 码矩阵中,如图 5 所示。其中,$D_1,D_2,\cdots,D_m$ 和 $E_1,E_2,\cdots,E_n$ 分别表示数据码块和纠错码块。

(2)认证信息隐写。认证码的产生主要分为消

息认证码(MAC)和散列函数(Hash)[7]两大类。消息认证码是以消息和密钥作为公开函数的输入，产生一个定长的输出，并以此作为认证码。散列函数是一个无需密钥的公开函数，它将任意长度的输入信息映射成固定长度的输出值，将此作为认证标识。本文采用基于 DES 的消息认证码(CBC-MAC)，将用户信息 D 以及密钥 k 作为输入信息。其中密钥 k 是双方共享的，由系统管理密钥。采用 DES 加密算法对 D 进行加密，把加密后的最后 64 位数据分组作为消息认证码 s，生成的消息认证码需要进行纠错编码，得到纠错码 E_s。



(a) QR 码原始图　　(b) 功能图形

(a) The original image of QR code　(b) The functional image

图 5　QR 码结构图

Fig. 5　Structure chart of QR Code

QR 码共有 40 个版本，L、M、Q、H 四种纠错等级。由于不同版本、纠错等级，所能容纳的错误位数不同，需要根据用户信息、认证码及其纠错码的数据位，选取适合版本及纠错等级的 QR 码。考虑到功能图形，如位置检测图形、定位图形、校正图形等是 QR 码正确识别的重要依据，不适合用来隐藏信息。再者，虽然格式和版本信息存在冗余设计，但占比很小，且信息隐藏可能会破坏这些信息导致译码失败，故也不适合。最终选取数据码块中数据码字的最低有效位作为信息隐藏位置。数据码块隐藏空间大，并且可以提高 QR 码版本增加隐藏的信息量。不同版本和纠错等级的 QR 码对应的信息隐藏容量如图 6 所示。在确认隐写位置后，将消息认证码 s 和纠错码纠错码 E_s 隐写入 QR 码中。本文使用的隐写方法是基于改进后的 LSB 技术，实现认证信息的隐藏。

(3) VSS。信息隐写完成后，对生成的图像进行掩膜，得到最终的 QR 码。若直接对 QR 码进行识读，就能读取到用户信息。为了保证在用户许可的条件下，仅有管理员可获取用户信息，本文采用基于二值图像的 (2,2) - *VSS* 门限方案。将 QR 码加密成两个分享图像，由用户和管理员分别保存，只有在二者同时呈现图像时，才能合成 QR 码获取用户信息。

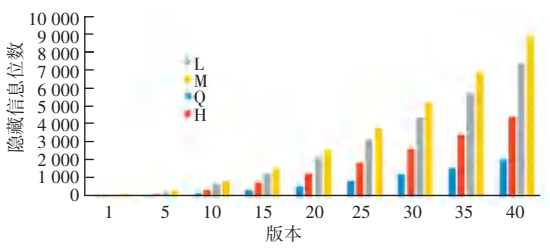


图 6　不同版本和等级 QR 码信息隐藏容量

Fig. 6　Different versions and levels of information hiding capacity of QR Code

2.2　安全认证

安全认证与子图像生成的过程相反，可分为信息提取和安全认证两步，如图 4(b)所示。首先将用户和管理员持有的子图像进行合成得到 QR 码，再利用隐写过程的逆过程得到认证信息。确认认证信息是否与原先的认证码相同，即可判断用户身份的真实性。具体认证过程如下：

(1)信息提取。首先，扫描用户和管理员持有的图像，将两个分享图像进行合成，就是将图像对应像素进行异或操作，即可得到 QR 码；使用专用识别设备，对 QR 码进行识读，得到用户信息 D；最后将识别到的 QR 码去除掩膜，并提取出隐藏的认证信息 s。

(2)安全认证。利用用户信息 D 和共享密钥 k，以同样的方法生成消息认证码 V。若 V 和 S 相同，则认证成功，说明用户信息正确未被篡改，反之则失败。

此方法的验证过程安全高效，其优势在于无需传递密钥。因密钥由系统进行管理，可自动完成解密工作，不需要第三方参与，极大地减少了信息泄露的风险。由于采用可视秘密共享技术，若有一方信息泄露或者被篡改，没有另一方的许可，则不能通过安全认证，有效地保证用户信息的安全性。

3　实验结果分析

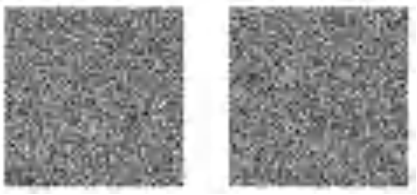
为了验证上述信息隐藏和安全认证方法的可行性及性能，对提出的方法进行实验。本文所提出的信息隐藏和安全认证算法，与 QR 码的编码标准密切结合，同时利用了 QR 码的纠错冗余特性。试验选择基于 C++的 QR 码标准编码器，可以生成标准的 QR 码。在此基础上，对源代码进行修改，在纠错编码以及数据块填充的代码后，添加认证信息生成以及信息隐写代码，最后再进行掩膜操作。

图 7(a)是未经修改的编码器生成的 QR 码图像，编码信息为“上海工程技术大学电子电气工程学院”，版本号是 11，纠错等级为 M。图 7(b)是将认证信息隐写后的 QR 码。可以发现，二维码本身无法看出其携带的信息，能够很好地保护信息不外

泄;另一方面,该信息隐藏方法不会改变图像的视觉质量,无法察觉隐藏的信息。

(a) 原始 QR 码 (b) 隐写后的 QR 码

(a) The original QR code (b) QR code after steganography



(c) 子图像 1 (d) 子图像 2

(c) The subimage1 (d) The subimage2

图 7 实验结果图

Fig. 7 Experimental result diagram

上文最终生成的 QR 码虽然在一定程度上能够保证信息不外泄,但使用普通的识读设备,如手机等移动设备仍能够快速获取其包含的用户信息。因此,本文最后采用基于二值图像的 (2,2) - *VSS* 门限方案,将 QR 码加密成两个子图像,如图 7(c)、(d)所示。因此,单独任何一个子图像均不能得到用户信息,仅当两个子图像合成时才能得到 QR 码,再进行解码获取认证信息,如图 8 所示。

图 8 认证结果图

Fig. 8 Certification result image

4 结束语

本文在分析 QR 码纠错机制的基础上,利用纠错编码的冗余特性,结合改进后的 LSB 技术,实现认证信息的隐藏。采用基于二值图像的 (2,2,) - *VSS* 门限方案,实现秘密共享,确保在双方许可的条件下才能获取信息。该方法使用改进后的 LSB 技术,改善了原始 LSB 技术对原图像改动较大的缺点;采用基于 DES 的消息认证码(CBC-MAC),进一步确认消息的完整性;最后利用可视秘密共享技术,既实现秘密共享,又保证了信息的机密性。实验结果表明,本文采用的方法,计算成本较低,能够高效地保护用户信息,且具有很好的透明性。

参考文献

[1] 于英政. QR 二维码相关技术的研究[D]. 北京:北京交通大学,2014.

[2] 牛夏牧,黄文军,吴迪,等. 基于二维条码的信息隐藏技术[J]. 中山大学学报(自然科学版),2004(S2):21-25.

[3] FENG J B, WU H C, TSAI C S, et al. Visual secret sharing for multiple secrets[J]. Pattern Recognition, 2008, 41(12):3572-3581.

[4] LUO Weiqi, HUANG Fangjun, HUANG Jiwu. Edge Adaptive Image Steganography Based on LSB Matching Revisited[J]. IEEE Transactions on Information Forensics and Security, 5(2):201-214.

[5] 丁海洋. 一种基于秘密分享的高质量(k,n)可视加密算法[J]. 计算机应用研究,2019,36(8):2449-2453.

[6] YAN X, LU Y. Applying QR Code to Secure Medical Management [J]. 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 2018:53-56.

[7] 徐津,温巧燕,王大印. 一种基于 Hash 函数和分组密码的消息认证码[J]. 计算机学报,2015,38(4):793-803.

[8] 冯国柱,李超,吴翊. 基于视觉密码的身份认证方案[J]. 计算机应用,2006(10):2318-2319.

[9] 傅俊. QR 码图像信息隐藏技术及其隐秘通信系统研究与实现[D]. 湖南大学,2018.

[10] 张雅奇,张定会,江平. 一种提高 QR 码安全性的方法[J]. 信息技术,2012,36(11):90-92.

(上接第 13 页)

[7] SUBRAMANIAN S, WANG T, YUAN X, et al. Neural models for key phrase detection and question generation[J]. arXiv preprint arXiv:1706.04560.

[8] ZHAO Y, NI X, DING Y, et al. Paragraph-level neural question generation with maxout pointer and gated self-attention networks [C]//Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing. 2018: 3901-3910.

[9] SONG L, WANG Z, HAMZA W, et al. Leveraging context information for natural question generation. In Proceedings of the 2018 Conference of NAACL,2018:569-574.

[10] LIU B, ZHAO M, NIU D, et al. Learning to Generate Questions by LearningWhat not to Generate[C]// In The World Wide Web Conference (pp. 1106-1118).

[11] DUAN N, TANG D, CHEN P, et al. Question generation for question answering[C]//Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing. 2017: 866-874.

[12] KUMAR V, JOSHI N, MUKHERJEE A, et al. Cross-lingual training for automatic question generation [J]. arXiv preprint arXiv:1906.02525, 2019.

[13] SCIALOM T, PIWOWARSKI B, STAIANO J. Self-attention architectures for answer-agnostic neural question generation[C]// Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. 2019: 6027-6032.

[14] CHAN Y H, FAN Y C. BERT for Question Generation[C]// In Proceedings of the 12th International Conference on Natural Language Generation,2019:173-177.