doi:10.3969/j.issn.1672-4348.2019.03.010

基于 QR 码模块边界偏移的信息植入与提取方法

刘石坚[1],翁才杰[1],邹峥[2]

(1. 福建工程学院 信息科学与工程学院,福建 福州 350118;
2. 福建师范大学 数学与信息学院,福建 福州 350007)

摘要:提出一种基于 QR 码(quick response,快速响应)模块边界多方向偏移的信息植入及提取方法,应用于 QR 码编码信息认证中。该方法具有较高的容量、较强的抗干扰能力,适用于通过数字媒体、印刷媒体传播的 QR 码场景。通过植入数据容量评估实验和裁剪攻击实验验证了方法的有效性。

关键词:QR 码;信息安全;编码信息认证;数字签名

中图分类号:TP301 **文献标志码**:A **文章编号**:1672-4348(2019)03-0259-08

Information embedding and extraction method based on module boundary offset of QR codes

LIU Shijian[1], WENG Caijie[1], ZOU Zheng[2]

(1. School of Information Science and Engineering, Fujian University of Technology, Fuzhou 350118, China;
2. College of Mathematics and Information, Fujian Normal University, Fuzhou 350007, China)

Abstract: An information embedding and extraction method based on multi-directional module boundary offset of QR (quick response) codes is proposed, which can be applied in message authentication of encoded QR codes. The method has such advantages as high capacity and anti-disturbance, and it is applicable for transmission scenarios of QR codes through both digital and print mediums. The effectiveness and efficiency were proved by experiments including embedding capacity evaluation and occlusion attack analysis.

Keywords: quick response code; information security; encoded message authentication; digital signature

随着移动智能终端和互联网技术的迅猛发展,二维条码以空前的速度占领了信息时代的至高点。作为二维条码技术的典型代表,快速响应(quick response,QR)码被广泛应用于各行各业,从移动支付[1]到身份认证[2-3]。人们在享受 QR 码带来的便捷服务时,对敏感信息的安全问题却感到不安,因为任何人都可以通过遵循开放标准的解码软件轻松获取标准 QR 码的编码信息。因此,如何实现 QR 码编码信息的篡改检测,是一个值得研究的问题,具有重要的社会和经济价值。

与直接加密编码信息或将认证信息与编码信息一同编码的传统方法不同,在基于 QR 码模块边界多方向偏移的信息植入与提取方法中,编码信息的数字签名将通过所提出的植入方法与 QR 码一同分发,并在解码的同时被提取出来用于编码信息的篡改检测。

1 国内外相关工作

1.1 QR 码

QR 码是目前应用最为广泛的二维条码技术之一,具有较高的编码容量、较小的打印尺寸、丰富的编码字符集、强大的自纠错能力、任意角度可读等特点。尽管 QR 码具有诸多优点,但其遵循开放设计原则因而没有对编码信息的安全性做出

收稿日期:2018-11-11;修回日期:2019-03-18
基金项目:福建省属高校科研专项项目(JK2017029);福建工程学院校级科研项目(GY-Z160138,GY-Z160130)
第一作者简介:刘石坚(1983-),男,湖南长沙人,讲师,博士,研究方向:计算机图形学,信息技术。

明确规定,加之制作和传播成本极为低廉,使其常常成为不法分子的攻击目标。文献[4]深入分析了与 QR 码有关的信息安全问题。

1.2 现状分析

针对 QR 码的信息安全问题,国内外学者纷纷给出了不同的解决方案。其中,传统方法包括利用各种加密技术对编码信息进行加、解密[5-8]以确保编码信息的安全性,该方法虽有效,但需要对终端用户(即执行解码操作的用户)进行身份认证。让编码信息不可见虽可以实现其认证功能,却有悖认证信息公开的原则。另外有一类问题的关注点是实现与 QR 码所关联对象的认证[9],而非研究涉及的 QR 码自身编码信息的认证研究。在不改变编码信息的情况下,Yao 等人[10]提出利用第三方知识库实现编码信息的认证。显然,该方法对第三方知识库的依赖性是其主要的局限所在。

另一种思路是使用额外的认证信息(例如消息认证码、数字签名)来实现编码信息的防伪,其关键在于设计切实有效的认证信息分发策略。现有方法虽未对编码信息进行修改,但大多将认证信息同样编码到 QR 码中[11-12],而编码信息的增加往往意味着编码容量需求的增加,以及解码效率的降低。与之相比,空间域[13-14]以及频率域[15]数字水印技术可以在不改变给定 QR 码编码内容的条件下实现认证信息的植入。前者的缺点是不能用于印刷媒体传播的 QR 码,因为数字水印信息无法在经历打印、扫描操作之后正确还原;后者的计算开销对于计算资源和电力储备有限的移动设备非常不利。

除使用传统的数字水印技术进行数据植入外,Barmawi 等人[14]以牺牲 QR 码自身纠错能力为代价提出了一种基于模块操作的数据植入方法,其植入容量为纠错码字容量的 1/2。在文献[14]方法的基础上,Lin 等人[16]提出了一种植入容量更优的私密信息分发方法。文献[17]通过对 Lin 等人的方法进行分析研究得出结论,其信息植入容量取决于所采用 QR 码纠错码的长度。文献[18]认为,由于采用 LSB 方法进行数据植入,Lin 等人所提出的方法确实较之前的方法具有更高的植入容量。但同时,文献[19]也指出,由于使用标准 QR 码中的部分模块进行信息植入,该信息植入方法是以牺牲标准 QR 码的纠错能力为代价的。

受上述方法的启发,提出一种基于模块边界多方向偏移的信息植入及提取方法,并将其应用于 QR 码编码信息的认证。本方法具有植入信息容量高、抗干扰能力强等优点,适用于通过数字媒体、印刷媒体传播的 QR 码场景。

2 提出方法

2.1 问题描述及解决思路

给定原始信息 E1,遵照开放标准(如 ISO/IEC 18004:2006[20]等)对 E1 进行编码得 QR 码,令其为 Q1。Q1 通过印刷、互联网等媒体进行分发以后被终端用户获取,令用户获得的 QR 码为 Q2,解码所得信息为 E2。“QR 码编码信息认证”问题可以理解为:如何有效实现 QR 码编码信息的认证,即确认 E2 是否与 E1 一致。以此为动机,提出一种基于数字签名植入的 QR 码编码信息认证框架,核心方法为基于模块边界多方向偏移的信息植入及提取,以实现认证信息和 QR 码的关联,主要针对的问题包括(1)信息植入阶段的容量设计方法,以保证大容量的植入需求;(2)信息提取阶段的纠错机制设计,以保证方法的鲁棒性。

本方法基于以下观察:标准 QR 码是由一系列随机排列的黑、白模块构成的矩形区域,不同色块之间存在一条明显的分界线。如赋予某些分界线以“偏移”能力,则可通过其偏移或非偏移来表达二进制 0 或者 1。这些分界线称作可偏移边界,并定义如下:

定义 1 可偏移边界

对于 QR 码 Q 中任意两相邻模块 M1 和 M2 之间的边界 b 来说,当且仅当 M1、M2 代表 Q 中不同的二进制信息(或者说具有不同的颜色)时 b 为可偏移边界。

假设图 1(a)中的黑、白矩形区域为某 QR 码中两相邻模块,则箭头所指位置即为满足定义 1 的一个可偏移边界,其“偏移”行为定义如下:

定义 2 边界偏移

对于可偏移边界 b 来说,令 M1 和 M2 为定义 b 的两个 QR 码模块,C(M1)表示 M1 的颜色,R(M2)为包含于 M2 中且与 b 相邻的局部区域,那么边界 b 在从 M1 至 M2 方向上的偏移 $O(b,\overrightarrow{M1M2})$ 被定义为将 R(M2)的颜色更改为 C(M1)。

定义 2 所述的 R(M2)选取问题，在实际操作中可以有多种设计方案。其共同的步骤为对每个模块进一步作 3×3 等分，如图 1(a)中 B0-B8 和 W0-W8 所示。差别在于：对只存在一个方向偏移的情况来说，将 R(M2)设计为如图 1 中区域 W1、W8 和 W7 的合集(此时 W0-W8 为 M2)。

定义 3　二进制 0/1 数据植入或提取

对于可偏移边界 b 来说，在某个方向上植入(或提取)二进制信息 1 被定义为在该方向上对 b 执行边界偏移(或检测到存在边界偏移)；在某个方向上植入(或提取)二进制信息 0 被定义为在该方向上不执行边界偏移(或检测到不存在边界偏移)。

在上述定义的基础上，提出信息植入和提取方法：根据定义 1 找到给定标准 QR 码的可偏移边界集合 B；根据定义 3 将给定二进制信息应用于 B 中特定的可偏移边界以实现信息植入，或者通过检测 B 中特定可偏移边界的偏移状态以实现信息提取。例如，在图 1(b)中，可以通过置 W1、W8 和 W7 为黑色来植入 1；通过保留 W1、W8 和 W7 为白色来植入数值 0。

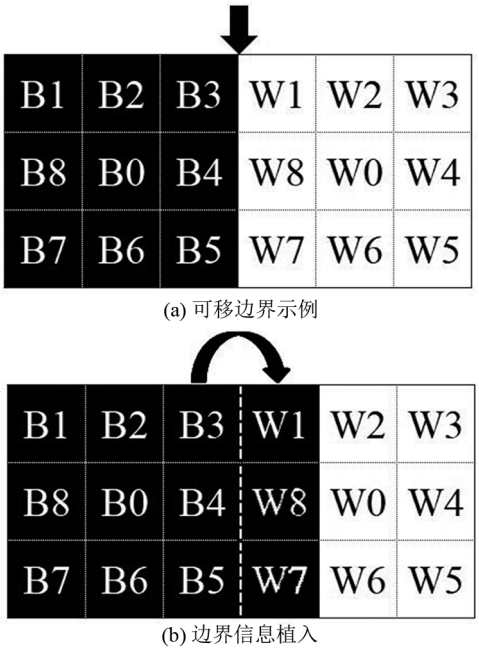

图 1　可偏移边界及其信息植入方法展示

Fig.1　Boundary offset and information embedding method

值得指出的是，本方法的可行性是建立在以下几点假设的基础上：(1)QR 码模块所对应的区域通常大于 1 个像素大小；(2)在保证模块中心位置像素不变的情况下对其他区域进行修改，通常不会影响 QR 码编码信息的正常读取[21]；(3)可偏移边界的数量是稳定的。其中，假设(1)用于保证模块能够进一步细分。鉴于过小的模块将导致识别效率偏低的问题，假设(1)在实际应用中是普遍存在性。假设(2)用于保证模块边界偏移不会影响原始 QR 码的正常读取，其论证可参考文献[21]；假设(3)用于为植入数据的容量提供保证，其有效性可由 QR 标准所定义的掩码(Mask)操作予以证实[20]，该操作确保标准 QR 码中不同色块在数量和空间分布上较为平均，而可偏移边界即与之相关。

2.2　信息植入方法

2.2.1　容量设计

植入容量是信息植入方法设计中的一个重要问题，为获得更多的植入容量，可以将图 1(b)所示单方向偏移情况扩展至多方向。这是由于矩形模块存在 4 条边，所以模块边界偏移可以同时出现在上下左右 4 个方向上。显然，多方向偏移比单方向偏移能够表达更多的二进制数，即提供更大的植入容量。

为应对可偏移边界在两个相反方向上同时存在可偏移性的情况，将使用如图 2 所示的方案来替代图 1 方案。即使用 W1 和 B5 分别表示定义 2 中所述向右和向左方向上的“局部区域”，其颜色是否改变依植入信息的不同而异。

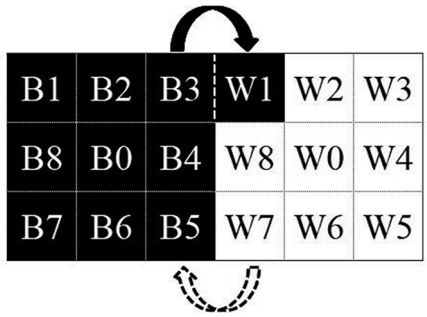

图 2　多方向信息植入方法展示

Fig.2　Multidirectional information embedding method

在有多个可偏移方向可选的情况下采用哪几个方向进行偏移是实际应用中遇到的另一个问题。显然，这是一个排列组合问题，一共有 N(N 满足公式 1)种可能性。

$$N = \sum_{i=1}^{n} c_n^i \tag{1}$$

其中 n 表示可偏移的方向数，c_n^i 表示从 n 个方向中取 i 个方向的组合。本例中，$n = 4$，即上下左右四个方向，因此 $N = 15$，且每一种可能性对应于不同的植入容量。

受 QR 码中版本和纠错等级设计的启发，按照上述多方向偏移可能性以及等级越高、容量越大的原则将植入容量划分为 15 个等级，供用户以选择的权力。

2.2.2 方法流程

如图 3 所示，给定 QR 码 Q1，二进制植入信息 S1，首先按照定义 1 识别 Q1 中所有的可偏移边界 B，然后采取相关措施防止植入数据溢出。具体来说，令 C_B 为可偏移边界的个数，L_{S1} 为 S1 的长度，那么只要 C_B 不小于 L_{S1}，就可以继续执行下一步骤；否则，需要通过提升 QR 码版本等方式获得更大的植入容量。接下来，从头到尾依次遍历 S1 中的每一个二进制数，并依照定义 3 所述的规则在对应的可偏移边界位置逐个进行植入，直至 S1 中的所有数都遍历完为止。为保证后续植入信息提取的顺利进行，在信息植入环节将引入纠错编码环节。任意一种块码(block code)技术都可用作纠错编码，RS 编码即其中的典型代表。图 4 展示了该方法的效果，其中左侧是给定的标准 QR 码，中间是在向右和向下两个方向上植入信息后的结果，右侧对两者的差异进行了标记。

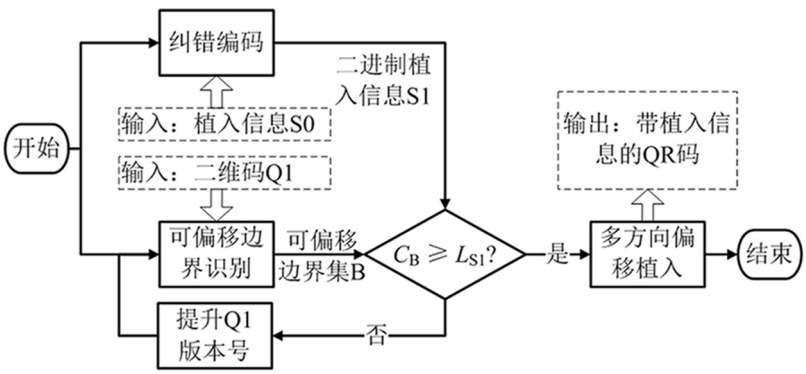

图 3 基于多方向偏移的信息植入方法流程图

Fig.3 Workflow of the multidirectional offset based information embedding method

图 4 植入效果展示

Fig.4 Embedding result

2.3 信息提取方法

2.3.1 纠错机制设计

对上述多级偏移方式所植入的信息进行提取并非简单的逆向操作，因为即使在未遭受恶意攻击的情况下，噪声、遮挡、污损等干扰也会导致终端用户获取的 QR 码遭到破坏。标准 QR 码中采用 RS 纠错机制来保障数据的正确性，本方法同样将利用纠错码技术，但面临的问题比标准 QR 码多。

本方法面临的挑战在于：既要考虑 ERA(Erasure，即将 0 识别为 1 或者将 1 识别为 0)错误，又要应对 ERR(Error，即数据位丢失，例如由于遮挡等原因错将图 5 中左侧实心箭头所示的 4 位数据识别为右侧实心箭头所示的 2 位数据)错误。标

准 QR 码只需要考虑 ERA 错误，因为一旦确定其版本和尺寸，就可以获得其模块大小，亦即编码数据的长度不会丢失。植入信息提取的关键是识别可偏移边界及其偏移情况。一旦有一个偏移边界没有被正确识别到，就会产生一个 ERR。例如，图 5 左为标准 QR 码中 5 个黑白相间、左右相邻的模块，假设由于遮挡干扰的发生，所识别到的对应模块如图 5 右侧所示，此时 QR 码编码信息的总位数并没有变，仅产生 1 个 ERA（右侧空心箭头标识）。相比之下，由于部分可偏移边界的消失，原本嵌入的 4 位二进制数（左侧箭头标识，从左向右单向偏移）最终只识别到 2 位（右侧实心箭头标识），即产生 2 个 ERR。与此同时，记 t 为 RS 纠错码的长度，就可纠错的数量来说，ERA 与 ERR 的上限分别为 t 和 $\lfloor t/2 \rfloor$。也就是说，在 RS 码长度确定的情况下，ERR 对纠错能力的消耗更大。因此单纯依靠 RS 码来实现纠错很难达到理想的效果。

为增强方法的纠错能力，提出一种准确识别携带植入信息 QR 码中所有可偏移边界的方法，以消除所有的 ERR，具体流程如下：

2.3.2　方法流程

如图 6 所示，令 Q2 表示终端用户获取到的携带植入信息的 QR 码，从中解码得到 E2，本方法的纠错策略是：重新对 E2 进行编码，得到标准 QR 码 Q1′，从 Q1′中（而非 Q2 中）获取所有的可偏移边界 B′，然后结合 B′以及 Q2 来提取植入信息 S2，最后采用植入信息环节相同的纠错码技术对 S2 进行纠错，实现植入信息的准确提取。

值得说明的是，上述流程中借助了标准 QR 的纠错机制，从而保证 B′与 2.2.2 节所述的 B 一致。因此，方法以标准 QR 码的正常解码为前提，这也正好切合本研究实现编码信息认证的出发点，因为在编码信息无法正常获取的情况下谈其认证是毫无意义的。另外，S2 中虽然消去了所有的 ERR，但可能存在 ERA，因此最后仍然需要对其进行纠错处理。

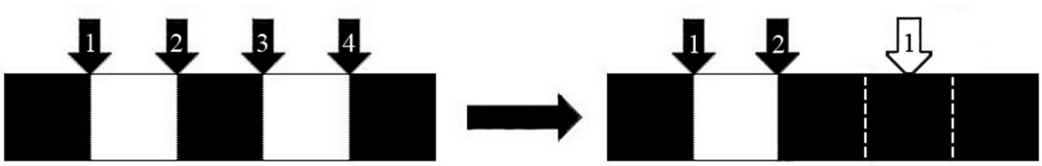

图 5　同一遮挡攻击下标准 QR 码的消除错误与本方法的数据位丢失错误比较

Fig.5　Comparison between the erasure error for standard QR code and the missing digits error for this method under the same occlusion attack

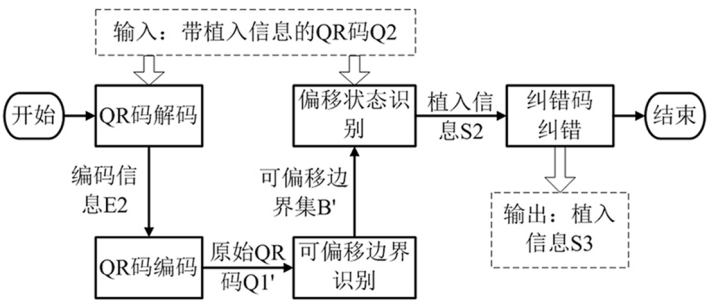

图 6　多方向偏移植入信息提取流程图

Fig.6　Workflow of the extraction of message embedded by the proposed multidirectional offset

2.4　编码信息认证框架

基于上述多级偏移的信息植入及提取方法来实现 QR 码编码信息的认证功能，其主要流程如图 7 所示。给定 QR 码 Q1，其编码信息为 E1，为实现编码信息的认证，在生成环节将对 E1 进行签名操作（包括生成摘要及其加密），并将得到的签名信息通过所提出的方法植入 Q1 中。然后该带签名信息的 QR 码将进入传播环节直至其被终端用户获取到。

由于传播环节的未知性，令获取到的 QR 码为 Q2，通过常规解码方法将得到编码信息 E2。在认证环节，将 E2 与 E1 的一致性问题转化为摘

要 D1 和 D2 的一致性问题予以解决,其中 D1、D2 分别是对 E2 进行哈希和对 Q2 中的签名信息解密所得到的。一方面,数字签名技术确保了该认证方法的有效性,另一方面,所提出的多级偏移信息植入方法为植入高容量的认证信息及其准确提取提供了可靠的解决方案。

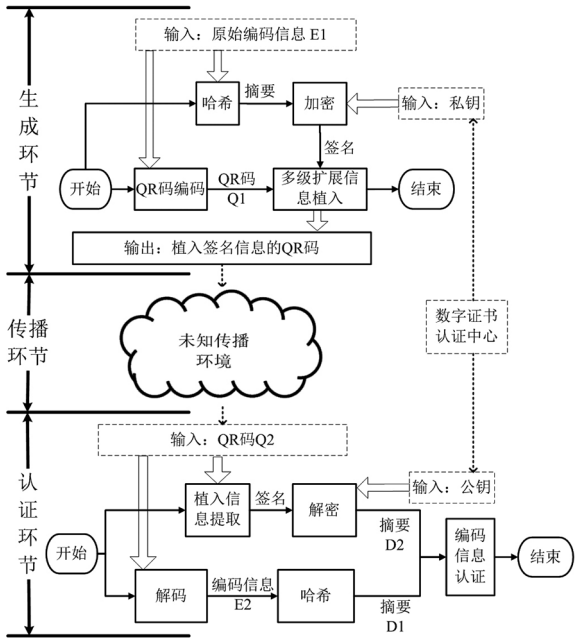

图 7 基于多级偏移植入数字签名的 QR 码编码信息认证方法框架

Fig.7 Authentication framework of encoded message of QR code based on hierarchical offset digital signature embedding

3 实验

为验证所提出方法的可行性和有效性,进行了各种类型的实验,主要对其中的植入数据容量评估和裁剪攻击测试结果进行阐述和讨论。

3.1 实验数据及环境

实验是在一台具有 Intel Core i5(3.3 Hz)CPU、8G 内存的普通台式电脑上进行的,编程环境为 MATLAB。实验采用 ZXing 库的标准 QR 码编码和解码,其编码信息、植入信息均为随机生成,QR 码的个数、编码/植入信息的长度、纠错等级等设置因实验目的不同。

3.2 植入数据容量评估

植入容量的大小是衡量数据植入算法的核心指标之一。该方法的植入容量与给定的 QR 码模块分布及所使用的方向数有关。为保证评估的客观性,随机生成 4 000 个标准 QR 码作为输入信息(其编码信息由包含于 ASCII 码中的字符组成,长度在 9~2 900 之间的,覆盖所有 4 个纠错等级以及 40 个版本号),分别测试使用 1、2、3、4 个方向进行信息植入情况下的植入容量(分别记为"本方法-1、2、3、4")。以给定 QR 码的编码信息容量(单位为比特)为基准,将该方法与 Barmawi 等人[14]的方法及 Lin 等人[16]的方法进行比较,其结果绘制于图 8 中。可见,以植入容量作为衡量标准,该方法明显优于另外两种方法。如果使用 2 个方向进行信息植入,该方法将具备与 QR 码编码信息相当的容量;如果采用 4 个方向进行植入,该方法的平均植入容量是 QR 码编码容量的 2.2 倍、Lin 等人方法的 6.4 倍、Barmawi 等人方法的 6.7 倍。

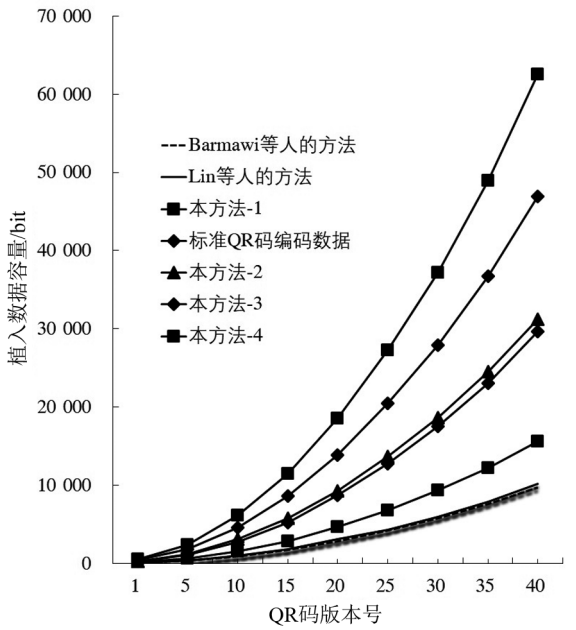

图 8 植入容量的比较

Fig.8 Comparisons of the embedding capacity

3.3 裁剪攻击实验

为测试方法的鲁棒性,进行了两组裁剪攻击实验。鉴于所提出的纠错方法是建立在 QR 码自身纠错机制的基础上,因此实验对象选取为纠错等级 H(即最高等级)、版本号 4 的 1 000 个标准 QR 码。为模拟 QR 码在实际应用中可能遭遇的各种遮挡情况,在第一组实验中,使用以图 9 所示为代表的裁剪攻击进行测试,实验结果表明本方法具有良好的植入信息提取能力。

图 9　裁剪攻击示例

Fig.9　Demonstration of different kinds of occlusion attacks

为进一步量化方法的纠错性能，在第二组实验中，将 352 比特的信息（其中 128 比特为有效信息，其余为纠错码）植入给定的 1 000 个 QR 码中。然后将遮挡区域定义为不同尺寸（占 QR 码图片面积从 5%至 30%不等）的矩形区域，同时将其以滑动窗口的形式依次遮盖 QR 码的不同区域，然后执行提取操作，并通过公式 2 计算得到植入信息提取的成功率 R 。

$$R = \frac{N_{\text{cor}}}{N_{\text{tot}}} \times 100\% \qquad (2)$$

其中 N_{cor} 是植入信息被成功提取的次数，N_{tot} 是窗口滑动的次数。最终的平均成功率 R_{avg} 是对1 000 个 QR 码进行测试所得结果的平均值。

表 1 展示了在不同方向上进行植入的提取成功率结果，该结果是在对应 QR 码能够成功解码的前提下得到的。此外，表中还记录了相同实验情况下，对应 QR 码自身编码信息解码的成功率，用以作为本方法成功率的参照基准。从表 1 可知，遮挡面积越小，植入信息提取的成功率越高。另外，由于使用 1 个方向进行植入较 4 个方向的植入数据分布更为分散，因此提取的成功率也更高。

4　结语

提出一种基于多级模块边界偏移的信息植入和提取方法，将其与数字签名技术相结合，可以在不改变给定 QR 码编码信息的情况下，实现 QR 码编码信息的篡改检测功能，从而保证用户的财产信息安全。该方法的创新点在于：1）提出了一种多级模块边界偏移的 QR 码信息植入方法；2）实现了一种有效应对数据位丢失错误的纠错策略；3）将信息植入和提取方法与数字签名技术相结合，构建出一套 QR 码编码信息认证框架。通过实验验证了方法的可行性和有效性。但受限于 QR 码自身纠错性能，该方法中植入信息的提取成功率仍有待进一步提升，需要更加深入研究。

表 1　不同摘挡尺寸情况下的植入信息平均提取成功率

Tab.1　Average success rate for embedded message extraction under different sizes of occlusion

遮挡面积/%	R_{avg}/%		
	1 个方向	4 个方向	标准 QR 码
5	100.00	100.00	90.70
10	100.00	99.37	87.96
15	90.09	55.51	76.58
20	52.02	8.07	38.55
25	35.85	0.53	3.57
30	0.00	0.00	0.00

参考文献：

[1] 马慰. 一种基于双因素认证的 QR 码安全移动支付方案研究[J]. 现代金融，2016(4)：42-44.

[2] 潘璐. 基于二维码的证件认证技术研究与实现[D]. 北京：北京邮电大学，2015.

[3] 徐剑, 赵英南, 田永纯, 等. 融合二维码与人脸识别的会议身份认证系统研究[J]. 信息网络安全, 2015(4): 13-18.
[4] KROMBHOLZ K, PETER F, KIESEBERG P, et al. QR code security: A survey of attacks and challenges for usable security[C]// International Conference on Human Aspects of Information Security, Privacy, and Trust. [S.l.]: Springer International Publishing, 2014: 79-90.
[5] GOEL N, SHARMA A, GOSWAMI S. A way to secure a QR code: SQR[C]// International Conference on Computing, Communication and Automation. Noida: IEEE, 2017:494-497.
[6] HUSNY H R M, ABDULLAH N Y, ISMAIL W H W, et al. Encrypted QR code system[J]. Journal of Computing Technologies and Creative Content, 2017, 8: 82-92.
[7] 杨丽娟, 孙红艳, 李瑛. RSA 算法在 QR 码防伪技术中的应用[J]. 北华航天工业学院学报, 2014, 24(2): 24-27.
[8] 安吉旺, 徐凯宏. 基于 RSA 和密钥的二维码加密编码的研究[J]. 森林工程, 2014, 30(2): 125-129.
[9] 解龙, 杜艳平, 程明智, 等. 基于加密 QR 二维码的商品包装防伪技术[J]. 北京印刷学院学报, 2013, 21(4): 16-20.
[10] YAO H, SHIN D. Towards preventing QR code based attacks on android phone using security warnings [C]//Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. Hangzhou: ACM, 2013: 341-346.
[11] 闫涛. 基于数字签名二维码认证技术的研究与实现[D], 北京: 北京印刷学院, 2017.
[12] 肖本海, 郑莹娜, 龙建明, 等. 基于 SHA512 哈希函数和 Rijndael 加密算法 QR 二维码信息安全设计[J]. 计算机系统应用, 2015, 24(7): 149-154.
[13] LIU S J, ZHANG J, PAN J S, et al. SVQR: a novel secure visual quick response code and its anti-counterfeiting solution [J]. Information Hiding & Multimedia Signal Processing, 2017, 8(5): 1132-1140.
[14] BARMAWI A M, YULIANTO F A. Watermarking QR code [C]// 2nd International Conference on Information Science and Security (ICISS). Seoul: IEEE Computer Society, 2015: 1-4.
[15] XIE R, HONG C, ZHU S, et al. Anti-counterfeiting digital watermarking algorithm for printed QR barcode [J]. Neurocomputing, 2015, 167(C): 625-635.
[16] LIN P Y, CHEN Y H. High payload secret hiding technology for QR codes [J]. EURASIP Journal on Image & Video Processing, 2017, 2017(1): 14.
[17] YESILTEPE M, KURULAY M. Fake and real massaging at the same time with QR code in web services for different users [J]. Security and Communication Networks, 2018(7): 1-10.
[18] HUANG P C, LI Y H, CHANG C C, et al. Efficient scheme for secret hiding in QR code by improving exploiting modification direction [J]. TIIS, 2018, 12(5): 2348-2365.
[19] CHENG Y, FU Z, YU B. Improved visual secret sharing scheme for QR code applications [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(9): 2393-2403.
[20] Information technology. Automatic identification and data capture techniques. QR Code 2005 bar code symbology specification[S]. ISO/IEC 18004, 2006.
[21] CHU H K, CHANG C S, LEE R R, et al. Halftone QR codes [J]. ACM Transactions on Graphics, 2013, 32(6): 1-8.

(责任编辑: 方素华)