doi:10.3969/j.issn.1001-4616.2025.02.012

基于扩展汉明码的二维码秘密分享方案

曹雪花[1],仲鑫玮[1],吉根林[2]

(1.江阴职业技术学院计算机科学系,江苏 无锡 214405)
(2.南京师范大学计算机与电子信息学院,江苏 南京 210023)

[**摘要**] 秘密分享作为隐私保护的重要手段,近来在云计算、物联网等领域迅猛发展. 二维码作为当下极为流行的信息载体,其使用频率远超传统图像,因此秘密分享技术在二维码上的应用前景广阔. 然而,由于二维码常以纸质形式呈现,容易遭受污渍沾染或破坏;同时,隐写二维码在传输过程中可能遭到攻击者篡改. 这些情况必然导致隐写二维码中出现误码,而现有研究方案无力实现无损重构秘密信息. 鉴于此,本文提出一种基于扩展汉明码的二维码秘密分享方案. 该方案不但确保了载体的高嵌入容量,还实现了隐写二维码的可纠错性,能够准确检测并纠正隐写二维码中的误码,进而恢复秘密信息. 理论分析与实验充分证明了该方案的有效性和实用性.

[**关键词**] 秘密分享,二维码,误码,扩展汉明码,纠错
[**中图分类号**]TP309.7　[**文献标志码**]A　[**文章编号**]1001-4616(2025)02-0112-12

Quick Response Code Secret Sharing Scheme Based on Extended Hamming Code

Cao Xuehua[1],Zhong Xinwei[1],Ji Genlin[2]

(1.Department of Computer Science,Jiangyin Polytechnic College,Wuxi 214405,China)
(2.School of Computer and Electronic Information,Nanjing Normal University,Nanjing 210023,China)

Abstract:Secret sharing,as a crucial method for privacy protection,has seen rapid development in fields such as cloud computing and the Internet of Things in recent years. As a very popular information cover at present,Quick Response Code(QR Code)is used far more frequently than traditional images,so the application of secret sharing in QR Code has highly promising. However,because the QR Code is often presented in paper form,it is easy to be stained or damaged;At the same time,stego-QR codes may be tampered by attackers during transmission. These issues will inevitably lead to bit errors in stego-QR code,and the existing research schemes are unable to recover the secret losslessly. To address this,this paper proposes a QR Code secret sharing scheme based on Extended Hamming Code. This scheme not only ensures high embedding capacity but also implements error correction capability of stego-QR Codes,which can accurately detect and correct bit errors in the stego-QR Code,and then recover the secret. Both theoretical analysis and experimental results demonstrate the effectiveness and practicality of this scheme.

Key words:secret sharing,Quick Response Code,bit errors,Extended Hamming Code,error correction

2022 年 1 月,国务院发布《“十四五”数字经济发展规划》,明确坚持“创新引领、融合发展,应用牵引、数据赋能,公平竞争、安全有序,系统推进、协同高效”的原则. 这在加速推动数据价值最大化的同时,也亟须行业迅速提升数据安全、个人信息保护的安全水准. 数据资产与其他资产明显不同的是,很容易被拷贝复制,因此直接的明文数据流通必定有显著危害,如何平衡数据要素的发展和个人信息的保护已成为现实挑战. 这正意味着安全隐私已从行业奢侈品变成必需品,数据密态时代已经开启.

数据密态时代中,隐私保护技术一直承载着保护关系到国计民生各行各业数据安全的使命. 而秘密分享作为隐私保护中的一个重要手段,最近在云计算、物联网等领域得到快速发展[1-2]. 在之前的数据安全方案中,隐私数据通常被用户保存在一个单独的存储设备中,如果数据丢失或被恶意篡改,隐私数据将

收稿日期:2024-11-03.
基金项目:2024 江苏省十四五规划重点课题“‘三融’视角下高职计算机专业赋能新质生产力的实施路径研究”(B-b/2024/02/28).
通讯作者:仲鑫玮,硕士,助教,研究方向:信息安全. E-mail:mxinm163@163.com

永远无法恢复. 而拷贝多份隐私数据副本并分发到多个存储设备,将会增加隐私数据受到安全威胁的可能性[3]. 因此,1979 年 Shamir[4] 与 Blakley[5] 率先提出了秘密分享(secret sharing,SS)方案以解决上述问题. 在 SS 方案中,秘密信息被分享成一系列的片段,这些片段通常被称为份额或阴影. 最后,该秘密可以通过一系列合格的份额重构. 因此,如果有些份额丢失,原始秘密依然可以顺利地重构. 这样避免了秘密集中在单个用户手中,达到了分散风险和容忍入侵的目的[6]. 所以,我们可以认为秘密分享将是未来能够助力行业、迎接数据密态时代挑战的重要技术方向之一.

最近,二维码(Quick Response Code,QR Code)因其高容量、读写方便、数据表示形式多样化等特点,成为信息领域最受欢迎的载体之一,并已经在移动支付、登录、防疫等领域得到广泛应用[7-8]. 然而,由于二维码的编码与解码规则采用的是国际标准化组织 ISO 发布的通用标准[9],任何人都可以轻松获取二维码中载有的公共信息. 因此,当传输或保存包含隐私信息的二维码时,会缺乏对隐私的安全性保护[10-11]. 因此,二维码与秘密分享结合的方案已然成为研究热点.

当前二维码秘密分享方案的研究趋势主要集中在载体二维码的嵌入容量与验证能力等方面. 但是,在隐写二维码的实际应用过程中,二维码经常会受到一些遮挡,如二维码被纸质化后,容易沾染上一些污渍等;此外,秘密重构过程中或许存在一些不诚实的参与者,他们故意篡改隐写二维码中的信息从而阻止秘密信息的恢复. 对于上述这些情况,秘密信息必然无法恢复. 因此,亟需一种秘密分享方案来避免上述问题,该方案不仅能够检测隐写二维码的真实性,而且当隐写二维码中存在一些误码时,可以实现这些误码的纠正从而保证秘密信息被准确的恢复.

基于上述分析,如果这些误码能够在验证阶段得到纠正,二维码秘密分享技术的效率将会得到显著提高. 因此,本文提出了一种将二维码秘密分享技术与纠错编码相结合的方案以解决上述问题. 本文的贡献主要如下:

(1)当具有纠错能力的隐写二维码在传输、存储或被攻击者篡改从而导致误码时,可以通过检测并纠正隐写二维码中的这些误码来重构秘密信息.

(2)秘密信息通过二维码的同态性质实现嵌入,在确保实现高嵌入容量的同时,不牺牲二维码的任何功能.

(3)验证信息通过二维码的结构性质实现嵌入,不会因为验证信息的嵌入破坏二维码的纠错功能.

1 相关工作

1.1 国内外研究现状

1979 年 Shamir[4] 与 Blakley[5] 率先提出了(k,n)门限秘密分享方案. 在(k,n)门限 SS 方案中,秘密信息由可信任的分发者通过合适的分享算法划分成 n 个无意义的片段,这些片段通常被称为份额或阴影,然后分发给 n 个对应的参与者进行管理. 最终,大于或等于 k 个合格的份额可以通过重构方法合作恢复出原始的秘密信息. 值得注意的是,少于 k 个合格的份额无法重构出任何的秘密信息.

2010 年,Chuang 等[12] 率先发现秘密分享方案在二维码领域具有广阔的应用前景,于是提出了一种基于二维码的秘密分享方案. 在该方案中,秘密被分享成一系列的份额,并根据这些份额生成一系列二维码,载有份额信息的二维码通常被称为隐写二维码. 虽然他们避免了无意义的份额直接暴露在公共信道或存储设备中,但是忽略了二维码的编码与解码规则是统一的,任何人都可以通过一个标准的二维码解析器来获取二维码中载有的信息. 因此,载有份额信息的二维码依然会在传输或存储时引起攻击者的注意从而增加秘密信息泄露的可能性. 为了解决这一安全性问题,2016 年 Chow 等[13] 提出了一种新颖的二维码秘密分享方案,他们将载有秘密信息的二维码看作分享的对象,然后以异或运算作为分享方法,将秘密二维码分享到各个载体二维码的纠错冗余中,嵌入秘密后的载体二维码可以正常读取其原本的公共信息,从而减小了受到攻击者注意的可能性. 之后,2018 年 Cheng 等[14] 通过改善 Chow 方案中的划分算法来提高份额的安全性. 但是这些方案中一旦隐写二维码受到一些遮挡或损坏,二维码中的公共信息将无法再被解析,极大地降低了方案的实用性. 此外,这些方案没有考虑份额的验证能力,无法防止虚假的份额参与秘密重构过程.

近期,Lin 等[15] 提出了一种基于湿纸编码(Wet Paper Code,WPC)的秘密分享方案. 在该方案中,以 WPC 作为嵌入方法,将份额与验证信息嵌入到二维码的纠错冗余中. 然而,Lin 方案中的验证方法存在设

计缺陷,在隐写二维码的真实性检测过程中,如果某个参与者提供虚假的验证密钥,整个验证过程将会失效. 此外,Huang 等[16]指出 Lin 方案中载体二维码的实际嵌入容量仅有 1~1 215 bits.

1.2　二维码

二维码是由黑白模块组成的二值图像,因为它可以被机器快速识别,如今已在各个领域得到十分广泛的应用. 根据存储在二维码中信息长度的不同,有 40 个版本的二维码供用户选择. 当二维码被部分损坏时,存储在二维码中的信息仍然可以被扫描设备读取,这是因为二维码具有一定的纠错能力. 针对不同的实际应用,有四种纠错级别可供用户选择,分别为 L、M、Q、H,对应的纠错能力分别为 L~7%、M~15%、Q~25%、H~30%.

图 1 展示了二维码的基本结构. 特别的是,对二维码中剩余位的修改,不会影响二维码的正常使用.

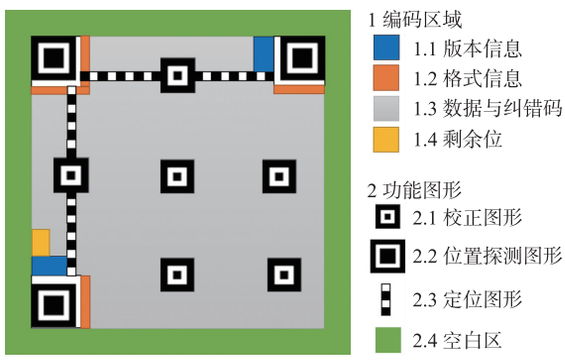


图 1　二维码的基本结构

Fig. 1　Basic structure of Quick Response Code

二维码编码区域由信息区域、补齐区域与纠错区域组成,其中信息区域与补齐区域统称为数据区域. 当数据区域未被公共信息的码字完全填充时,根据二维码标准需要对剩余区域填充补齐码. 填充补齐码的区域称为补齐区域,补齐区域中码字的内容不会影响二维码扫描仪解析的结果. 此外,用于实现二维码纠错功能的 Reed-Solomon(RS)编码具有同态性质[17]. 如果将数据通过 RS 的同态性质嵌入到补齐区域,嵌入后的二维码不会破坏原有的任何功能并能够正常的解析.

表 1　RS 编码同态性质

Table 1　The homomorphic property of the Reed-Solomon code

Secret	10011001		
	信息区域	补齐区域	纠错区域
RSC1	10001000	00010001	10011001
RSC2	00000000	10001000	10001000
RSC	10001000	10011001	00010001

表 1 给出了一个具体的例子. 即将被嵌入到载体二维码补齐区域的秘密信息二进制流是 10011001. 假设载体二维码中编码区域码字称为 RSC1. 在嵌入过程中,首先需要根据秘密信息生成一个对应的 RS 码 RSC2. 在 RSC2 的生成过程中,先要在 RSC2 的信息区域填充与 RSC1 信息码等长的零. 其次,将秘密信息二进制流与 RSC1 中的补齐码字进行异或得到 RSC2 的补齐码字($RSC2_{补齐}=10001000$). 然后,RSC2 的信息码字与补齐码字根据 RS 算法生成对应的纠错码字($RSC2_{纠错}=10001000$),从而得到完整的 RSC2(RSC2=0000000010001000100010001000). 最后,将 RSC1 与 RSC2 进行按位异或运算,从而得到最终的 RS 码 RSC. 值得注意的是,最终的 RS 码并没有牺牲其纠错功能. 因此,当二维码被损坏时,存储在其中的信息仍然可以正常读取.

下面简单描述一个通过 RS 编码同态性质实现信息嵌入的二维码案例. 如图 2(a)所示,选择包含“Secret Quick Response Code”内容的二维码作为载体二维码. 通过二维码补齐比特长度计算公式可得补齐比特长度为 64 位. 二维码补齐比特长度计算公式如下:

$$l=8\times R-\sum_{j=1}^{p}(M_j+I_j+D_j)-T, \tag{1}$$



(a) 载体二维码　(b) 隐写二维码　(c) 被损坏的隐写二维码

图 2　基于 RS 编码同态性质的信息嵌入案例

Fig. 2　An example of information embedding based on the homomorphic property of the Reed-Solomon code

式中,l 表示二维码中补齐比特长度,R 表示数据区域中码元的总数,p 表示二维码中片段的总数,M_j 表示第 j 个片段中编码规则的位数,I_j 表示第 j 个片段中字符计数指示器的位数,D_j 表示第 j 个片段中数据的位数,T 表示的是数据区域终止符的位数. 二维码的数据区域结构如图 3 所示.

片段1 (Segment 1)			片段2 (Segment 2)			…	片段p (Segment p)				
编码规则1 (Mode indicator 1)	字符计数指示器1 (Character count indicator 1)	数据1 (Data 1)	编码规则2 (Mode indicator 2)	字符计数指示器2 (Character count indicator 2)	数据2 (Data 2)	…	编码规则p (Mode indicator p)	字符计数指示器p (Character count indicator p)	数据p (Data p)	终止符 (Terminator)	补齐码 (Padding codewords)

图 3　二维码数据区域结构

Fig. 3　Data area structure of QR Code

图 2(b)为根据 RS 编码同态性质嵌入信息后的隐写二维码;如图 2(c)所示,虽然隐写二维码的部分内容被损坏,但隐写二维码的纠错功能并没有被破坏. 当我们使用二维码解析器扫描该二维码时,依然可以读取里面存储的内容.

1.3　秘密分享方法

由于 Xiong 等[1]的分享方法具有适用范围广、分享能力强、无份额扩展等特点,已经成为秘密分享方法中普遍采取的一种分享方法. 因此,本文采取 Xiong 的秘密分享方法. 在该方案中,以有限域 GF(Galois Field)(2^8)为背景,首先选择一个(k-1)次多项式:

$$f(x)=(a_0+a_1x+\cdots+a_{k-1}x^{k-1})\bmod g(x), \tag{2}$$

式中,$g(x)=x^8+x^4+x^3+x+1$.

接着,将多项式中的 k 个系数分别替换为秘密信息的 k 个值. 由于是在有限域 GF(2^8),所以值的范围是在(0,255),对应秘密信息中一个字节的内容. 然后将 n 个输入值输入到多项式中,得到 n 个输出值 $f(1),f(2),\cdots,f(n)$,输出值 $f(1),f(2),\cdots,f(n)$ 为 n 个相应份额的元素. 然后重复上述步骤,直到秘密信息被分享完毕. 其中,生成份额的大小为秘密信息的 $1/k$ 倍,没有额外的信息扩展.

在恢复阶段,一系列合格的份额可以根据拉格朗日插值法(式(3))计算出原始的秘密信息.

$$f(x)=\sum_{a=1}^{k} y_{ia}\prod_{j=1,j\neq a}^{k}\frac{x-x_{ij}}{x_{ia}-x_{ij}}. \tag{3}$$

1.4　(8,4)扩展汉明码

汉明码是 Richard Hamming 于 1950 年提出的一种线性纠错码[18]. 汉明码自提出以来,因其高效、方便的特点在通信领域得到了广泛的应用. 由于汉明码编码与解码计算开销低,所以本文采取汉明码来保护秘密信息. 此外,由于二维码中的一个码字由 8 个黑白模块(类似二进制中的 bit)组成,所以本文选取(8,4)扩展汉明码(Extended Hamming Code,EHC)作为纠错编码.

一个完整的汉明码是通过在传输的消息中插入奇偶校验位而形成的. 在传输过程中,当汉明码中的某一位发生改变时,可以根据汉明码理论检测并校正该位误码. 但是,如果汉明码中存在多位误码,汉明码的校验功能将会失效. 而相比传统汉明码仅能检验单个误码的情况,扩展汉明码能够实现双位比特的错误检测[19].

下面阐述(8,4)汉明码的编码与解码过程. 汉明码全码码元长度 $l=2^b-1$,其中 b 表示纠错码元的长度;汉明码中信息的长度 $l_m=2^b-b-1$. 而扩展汉明码是在汉明码的基础上扩展了一位纠错码元,从而实现了双位比特的错误检测. 如果想要生成一个(8,4)扩展汉明码,首先由信息 $\boldsymbol{M}_4^{\mathrm{T}}=[m_3,m_2,m_1,m_0]^{\mathrm{T}}$ 根据生成矩阵 $\boldsymbol{G}_{4,7}$来生成一个(7,4)汉明码 $\boldsymbol{C}_7^{\mathrm{T}}$.

$$\boldsymbol{C}_7^{\mathrm{T}}=[c_7,c_6,c_5,c_4,c_3,c_2,c_1]^{\mathrm{T}}=[m_3,m_2,m_1,m_0,s_3,s_2,s_1]^{\mathrm{T}}=mod_2(\boldsymbol{M}_4^{\mathrm{T}}\times\boldsymbol{G}_{4,7})\boldsymbol{M}_4^{\mathrm{T}}=[m_3,m_2,m_1,m_0]^{\mathrm{T}}, \tag{4}$$

$$\boldsymbol{G}_{4,7}=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}, \tag{5}$$

式中,$\boldsymbol{G}_{4,7}$是(7,4)汉明码的生成矩阵,(m_3,m_2,m_1,m_0)是大小为 4 比特的信息,(s_3,s_2,s_1)为三位纠错码.

由于本文采取的是偶校验,所以可以将 C_7^{T} 的每位比特按位异或得到扩展纠错码元 s_0,最终获得扩展汉明码 $\boldsymbol{C}_8^{\mathrm{T}}=[c_7,c_6,c_5,c_4,c_3,c_2,c_1,c_0]^{\mathrm{T}}$:

$$\boldsymbol{C}_8^{\mathrm{T}}=[c_7,c_6,c_5,c_4,c_3,c_2,c_1,c_0]^{\mathrm{T}}=[m_3,m_2,m_1,m_0,s_3,s_2,s_1,s_0]^{\mathrm{T}}, \tag{6}$$

式中,$c_0=s_0=c_7\oplus c_6\oplus c_5\oplus c_4\oplus c_3\oplus c_2\oplus c_1$(⊕表示异或操作).

在扩展汉明码的解码过程中,扩展汉明码中的校验码元 $\boldsymbol{S}^{\mathrm{T}}=[s_3,s_2,s_1,s_0]^{\mathrm{T}}$ 可以通过校验矩阵来获得.

$$\boldsymbol{S}^{\mathrm{T}}=[s_3,s_2,s_1,s_0]^{\mathrm{T}}=\mathrm{mod}_2(\boldsymbol{H}_{4,8}\times D_8) \tag{7}$$

$$\boldsymbol{H}_{4,8}=\begin{bmatrix}0&1&1&1&1&0&0&0\\1&0&1&1&0&1&0&0\\1&1&0&1&0&0&1&0\\1&1&1&1&1&1&1&1\end{bmatrix} \tag{8}$$

式中,$\boldsymbol{H}_{4,8}$是校验矩阵,D_8 是被修改的汉明码.

$s_3s_2s_1s_0$ 为四位校验码元. 当 $s_3s_2s_1s_0=0000$ 时,表示接收的汉明码没有错误;当 $s_3s_2s_1s_0$ 的值为偶数时,表示码字中存在两个错误;当 $s_0=1$ 时,误码的位置如表 2 所示.

表 2　(8,4)汉明码的校验参数

Table 2　Check parameters of (8,4) Hamming Code

错位	s_3	s_2	s_1	s_0	错位	s_3	s_2	s_1	s_0
7	0	1	1	1	3	1	0	0	1
6	1	0	1	1	2	0	1	0	1
5	1	1	0	1	1	0	0	1	1
4	1	1	1	1	0	0	0	0	1

2　本文方法

2.1　算法框架

我们提出了一种(k,n)门限的基于扩展汉明码的二维码秘密分享方案(QR Secret Sharing with Extended Hamming Code,QRSS-EHC). 在 QRSS-EHC 中,验证位被嵌入到载体二维码的剩余位中,这样可以很容易地检测隐写二维码的真实性并且不会牺牲二维码任何的原始功能. 该方案的纠错能力是根据扩展汉明码(Extended Hamming Code,EHC)理论实现的,当隐写二维码存在误码时,其纠错能力可检测最多两位误码,并可纠错单位误码.

QRSS-EHC 的总体框架如图 4 所示. QRSS-EHC 包括四个阶段,即秘密分享阶段、嵌入阶段、验证阶段和秘密重构阶段. 在分享阶段中,以有限域 GF(2^8)为背景根据多项式对秘密信息进行分享,从而生成一

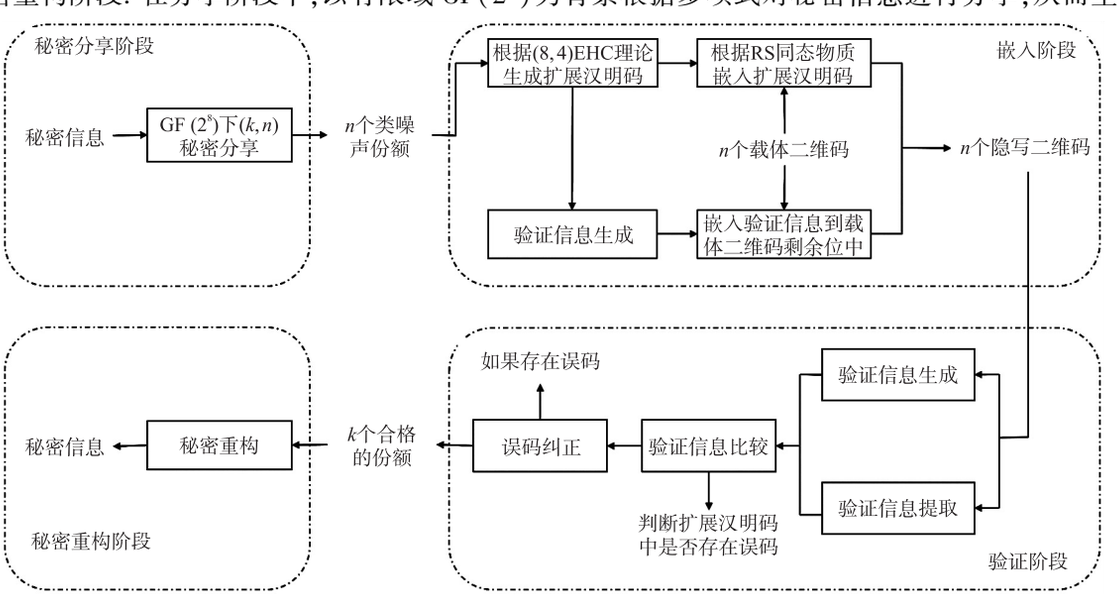


图 4　QRSS-EHC 框架图

Fig. 4　The framework diagram of QRSS-EHC

系列份额. 在嵌入阶段,根据份额生成对应的扩展汉明码,并根据生成的扩展汉明码得到验证信息;然后,将扩展汉明码通过 RS 同态性质嵌入到二维码的补齐区域,并将验证信息嵌入到二维码的剩余位中;在验证阶段,可以根据验证信息来验证隐写二维码的真实性. 如果验证结果已被篡改并且该二维码中某些码字存在单比特误差时,可以根据汉明码理论对这些码字进行校正. 最后,根据拉格朗日插值法,原始的秘密信息可以利用这些合格的份额进行重构.

2.2 分享阶段

假设秘密信息 $S(s_i,1\leqslant i\leqslant k\times m)$ 所占字节大小是 $k\times m$. 秘密信息中每 k 个字节内容可以替换多项式(式(9))中 k 个系数以此生成 n 个份额 H_i $(1\leqslant i\leqslant n)$. 由于一次分享过程需使用 k 个字节内容,所以生成的份额大小为 m 个字节. 图 5 展示了多项式构建及分享过程.

$$f(x)=(a_0+a_1x+\cdots+a_{k-1}x^{k-1})\bmod g(x),\quad(9)$$

式中,$g(x)=x^8+x^4+x^3+x+1$.

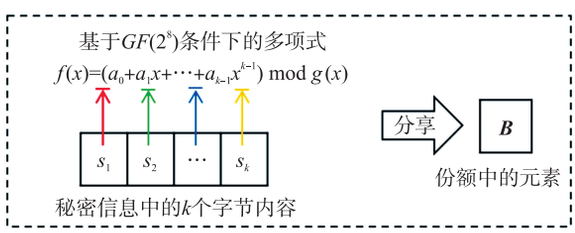


图 5 多项式构建及秘密分享过程

Fig. 5 The process of polynomial construction and secret sharing

2.3 嵌入阶段

为了实现该方案的纠错能力,需要根据份额 $H_i(1\leqslant i\leqslant n)$ 中的每个元素来生成对应的扩展汉明码. 对于一个份额 H_i,将其每个元素 $B(b_i,0\leqslant i\leqslant 7)$ 以二进制形式划分为高四位($b_7b_6b_5b_4$)和低四位($b_3b_2b_1b_0$),然后分别作为(8,4)扩展汉明码生成函数的输入(式(10))来获得扩展汉明码组 $CG_i=\{C_1,C_2\}$ $(1\leqslant i\leqslant m)$. 直到份额中的每个元素都被分享完成,最终得到嵌入到一个载体二维码中的扩展汉明码组 $CG_i=\{C_1,C_2\}$ $(1\leqslant i\leqslant m)$,而总共嵌入的扩展汉明码数量是 $2\times m$.

$$\begin{cases}C_1=F_{\mathrm{EHC}}(b_7b_6b_5b_4)\\C_2=F_{\mathrm{EHC}}(b_3b_2b_1b_0)\end{cases},\quad(10)$$

式中,$F_{\mathrm{EHC}}(\cdot)$ 表示扩展汉明码的生成函数.

在嵌入扩展汉明码组 CG_i 之前,需要选取合适的载体二维码来判定其是否有足够的补齐码冗余能够容纳 CG_i 的嵌入. 根据被选取载体二维码的补齐区域,CG_i 的可嵌入数量可以被计算. 扩展汉明码组可嵌入数量计算公式为:

$$l_{CG}=\left(8\times R-\sum_{j=1}^{p}(M_j+I_j+D_j)-T\right)\Big/(2\times 8),\quad(11)$$

式中,l_{CG} 表示扩展汉明码组的可嵌入数量,R 表示数据区域中码元的总数,p 表示二维码中片段的总数,M_j 表示第 j 个片段中编码规则的位数,I_j 表示第 j 个片段中字符计数指示器的位数,D_j 表示第 j 个片段中数据的位数,T 表示的是数据区域终止符的位数.

然后,根据里德-所罗门(Reed-Solomon,RS)编码同态性质将扩展汉明码组 CG_i 嵌入到载体二维码中. 假设被选取的载体二维码可嵌入汉明码组长度 $l_{CG}=m$. 在嵌入过程中,首先解码载体二维码补齐码 P_i $(1\leqslant i\leqslant l_{CG}\times 2)$,其中补齐码 P_i 的数量与扩展汉明码组 $CG_i=\{C_1,C_2\}$ $(1\leqslant i\leqslant m)$ 中的扩展汉明码数量相同. 再将补齐码 $(P_{2i-1}\parallel P_{2i})$ $(1\leqslant i\leqslant m)$ 与扩展汉明码组 CG_i $(1\leqslant i\leqslant m)$ 进行按位异或运算,得到异或后的结果比特流 O,方法如下:

$$O=\mathrm{XOR}((P_{2i-1}\parallel P_{2i}),CG_i),\quad(12)$$

式中,O 表示异或后的结果,XOR 表示异或运算.

然后,向异或后结果比特流 O 前端添加足够的零使比特流 O 的长度与信息区域的长度相同,补零后的结果比特流看作 O'. 由于二维码的数据区域总共由 R 个码元组成且每个码元由 8 个比特组成,因此需要填充零的个数为 $8\times R-(l_{CG}\times 2\times 8)$. 补零的计算过程如下:

$$O'=(0\cdots 0\parallel O),\quad(13)$$

式中,$\parallel$ 表示附加操作,附加零的个数是 $8\times R-(l_{CG}\times 2\times 8)$.

接着根据 RS 编码计算比特流 O' 对应的纠错码 E,并将得到的纠错码附加在比特流 O' 之后得到新的 RS 码 NR.

$$\mathrm{NR}=(O'\parallel E)=(O'\parallel F_{\mathrm{RS}}(O'))\,, \tag{14}$$

式中,$F_{\mathrm{RS}}(\cdot)$表示里德-所罗门编码的生成函数.

最终,将载体二维码中原本的 RS 码 OR 与新 RS 码 NR 进行异或得到最终可以嵌入的 RS 码 FR,并将载体二维码中原本的 RS 码 OR 替换为 RS 码 FR,方法如下:

$$\mathrm{OR}\leftarrow\mathrm{FR}=\mathrm{XOR}(\mathrm{OR},\mathrm{NR})\,, \tag{15}$$

式中,OR 表示原本载体二维码的 RS 码,NR 表示生成的新 RS 码,FR 表示最终可嵌入的 RS 码,XOR 表示异或运算,"←"为替换操作.

此外,为了防止攻击者或不诚实的参与者篡改份额致使恢复阶段无效,本文使用了基于哈希的消息验证码(Hash-Based Message Authentication Code,HMAC)来实现验证功能. 在我们的方案中,以份额生成的扩展汉明码组 $CG_i(1\leqslant i\leqslant m)$作为哈希函数的输入(在本文的实验中,哈希函数使用 SHA-1). 同时,为了防止攻击者利用其他参与者的隐写二维码破坏验证阶段,需要在哈希函数的输入中附加隐写二维码的标识 $ID_j(1\leqslant j\leqslant n)$. 因此,本文通过 HMAC 算法按位异或哈希函数的 160 位输出,以生成剩余位(remainder bits)长度 l_A 等长的载体二维码的验证信息 $U=\{u_i\mid 1\leqslant u_i\leqslant l_A\}$,验证信息计算公式为:

$$U=\mathrm{XOR}\langle F_K(CG_i^j\parallel ID_j)\rangle\,, \tag{16}$$

式中,CG_i^j 表示第 j 个份额生成的扩展汉明码组,ID_j 表示第 j 个隐写二维码的身份号,$\parallel$ 表示附加操作,$\mathrm{XOR}\langle\cdot\rangle$表示按组异或操作,$F_K(x)$表示 Hash 算法(本文中使用的是 SHA-1).

最终,将生成的验证信息嵌入到载体二维码剩余位的位置,从而得到最终隐写后的载体二维码 Q_i $(1\leqslant i\leqslant n)$. 待所有份额生成的扩展汉明码组与其验证信息嵌入完毕后,嵌入过程至此结束.

分享与嵌入过程的算法伪代码如算法 1 所示.

算法 1　分享与嵌入算法

输入:秘密信息 $S(s_i,1\leqslant i\leqslant k\times m)$,载体二维码 $O_i(1\leqslant i\leqslant n)$;
输出:隐写二维码 $Q_i(1\leqslant i\leqslant n)$.
1、 Foreach $i\in\{1,2,\cdots,n\}$ do
2、　Foreach $j\in\{1,2,\cdots,m\}$ do
3、　　$H_i(j)=(s_{k\times(j-1)+1}+s_{k\times(j-1)+2}\times i+\cdots+s_{k\times j}\times i)\bmod g(i)$;　//$H_i(j)$为第 i 个份额的第 j 位元素
4、 Foreach $i\in\{1,2,\cdots,n\}$ do
5、　Foreach $j\in\{1,2,\cdots,m\}$ do
6、　　$B=H_i(j)$;　//获取第 i 个份额的第 j 位元素
7、　　$B_1=(b_7b_6b_5b_4)$,$B_2=(b_3b_2b_1b_0)$;　//获取元素的高四位与低四位
8、　　$CG_j^i=\{C_1,C_2\}=\{F_{\mathrm{EHC}}(B_1),F_{\mathrm{EHC}}(B_2)\}$;　//根据份额中的元素生成两个扩展汉明码
9、 Foreach $i\in\{1,2,\cdots,n\}$ do
10、 $U^i=XOR\langle F_K(CG^i\parallel i)\rangle$;　//根据每个份额的扩展汉明码组生成对应的验证信息
11、Foreach $i\in\{1,2,\cdots,n\}$ do
12、 通过 RS 同态性质嵌入扩展汉明码组 CG^i 到载体二维码 O_i 中;
13、 嵌入验证信息 U^i 到载体二维码 O_i 的剩余位中;
14、输出隐写二维码 $Q_i(1\leqslant i\leqslant n)$.

2.4　验证阶段

在进行秘密重构之前,或许隐写二维码已经沾染上污渍或被攻击者篡改,所以需要对隐写二维码 $Q_i'(1\leqslant i\leqslant n)$的真实性进行检测,以避免秘密重构过程的失效. 在验证阶段,首先从隐写二维码的剩余位中读取之前嵌入的验证信息 U. 然后再根据隐藏在第 j 个隐写二维码中的扩展汉明码组 $CG_i^{j'}(1\leqslant i\leqslant m)$来生成验证信息 U'. 并将 U 与 U'进行比较,如果结果不一致,则表示隐写二维码存在误码. 验证信息 U'的计算公式如下:

$$U'=\mathrm{XOR}\langle F_K(CG_i^{j'}\parallel ID_j)\rangle\,, \tag{17}$$

式中,$CG_i^{j'}(1\leqslant i\leqslant m)$表示第 j 个隐写二维码中被嵌入的扩展汉明码组,$ID_j(1\leqslant j\leqslant n)$表示第 j 个隐写二维码的身份号,$\parallel$ 表示附加操作,$\mathrm{XOR}\langle\cdot\rangle$表示按组异或操作,$F_K(x)$表示 Hash 算法(本文中使用的是 SHA-1).

2.5　重构阶段

如果 U 与 U'的比较结果一致,则表示该隐写二维码未被攻击者篡改;否则,就意味着该隐写二维码已

被篡改. 如果隐写二维码已被篡改,即隐写二维码中存在单个误码,我们可以利用(8,4)扩展汉明码理论检测该码元并对其进行校正. 对于一个存在误码的码元 $C_i'(1\leqslant i\leqslant 2\times m)$,恢复的计算过程如下:

$$C_i''=F_{\mathrm{EHCC}}(C_i'), \tag{18}$$

式中,C_i''表示被纠正的扩展汉明码,$F_{\mathrm{EHCC}}(\cdot)$表示扩展汉明码的校正函数.

最后提取校正后码元 $C_i''=\{c_j|1\leqslant j\leqslant 8\}$ 中的高 4 位($c_7c_6c_5c_4$),每两个连续纠正后码元的高 4 位组成一个份额中的元素,从而提取出合格的份额. 然后,利用拉格朗日插值法通过 k 个份额来重构原始的秘密信息.

验证过程与秘密重构过程的算法伪代码如算法 2 所示.

算法 2　验证与重构算法

输入:隐写二维码 $Q_i'(1\leqslant i\leqslant k)$;
输出:秘密信息 S.
1、Foreach $i\in\{1,2,\cdots,k\}$ do
2、提取嵌入在隐写二维码中的验证信息 U^i;
3、提取隐写二维码中的扩展汉明码组 $CG^{i'}$;
4、根据扩展汉明码组 $CG^{i'}$ 生成验证信息 $U^{i}{}'$;
5、If $U^{i}{}'!=U^i$ do　//隐写二维码已被篡改
6、通过(8,4)EHC 理论纠正 $CG^{i'}$ 中的误码;
7、通过拉格朗日插值法恢复原始的秘密信息 S;
8、输出秘密信息 S.

3　实验与分析

本文中的所有实验均在 MATLAB R2021b v9.11 环境下开展,实验所采用的平台配置如下:处理器为 Intel(R)Core(TM)i9-13900H@ 2.60 GHz,内存为 32 GB DDR5 4800 MHz,操作系统是 64 位的 Windows 11 专业版.

本研究采用现有文献中广泛使用的 4-H 版本二维码作为载体,从嵌入容量、验证能力、纠错能力和鲁棒性四个维度展开实验对比分析. 嵌入容量决定了载体二维码能够承载的秘密信息容量;验证能力能够在秘密信息重构前,有效验证参与重构的二维码的真实性;纠错能力确保即使二维码存在部分损坏或遮挡,仍能准确恢复秘密信息;而鲁棒性则保证了隐写二维码图像在经历压缩、噪声干扰等处理后,其内部嵌入的秘密信息仍能被准确恢复.

3.1　实验结果

在实验部分,本文以(2,3)门限的 QRSS-EHC 方案为例,对实验结果进行详细的说明. 在实验中,本文使用内容为“Password:I Love JYPC!!!”的信息作为秘密信息,载有公共信息内容为“CoverCodei”($1\leqslant i\leqslant 3$)的 4-H(4 代表版本号,H 代表纠错能力)二维码作为载体二维码.

(2,3)门限 QRSS-EHC 方案实验结果如图 6 所示. 图 6(a)为秘密信息“Password:I Love JYPC!!!”,秘密信息长度共 24 个字节. 图 6(b)-(d)展示了三个 4-H 载体二维码. 根据 ISO/IEC 18004,他们的剩余位长度为 7 bits. 图 6(e)-(g)展示了本文通过算法 1 实现的三个隐写二维码. 这些隐写二维码即使被嵌入了秘密信息,我们依然可以通过二维码扫描仪读取其公共信息. 图 6(h)为重构后的秘密信息,秘密信息是根据隐写二维码中扩展汉明码里的份额重构的.

图 7 是我们对隐写二维码进行的遮挡实验,并与现有的研究方案[12-15]进行了对比,我们使用了一个“H”标识对各个方案的隐写二维码进行了遮挡. 图 7(a)为 Chuang 等的方案[12],在他的方案中,隐写二维码即使被遮挡了也能正常解析其公共内容,但是其公共内容是无意义的信息“537806412851701072 86”,所以容易引起攻击者的注意从而被攻击. 图 7(b-d)分别为 Chow 等[13]、Cheng 等[14]和 Lin[15]方案中的隐写二维码,由于他们的方案都是牺牲二维码的纠错冗余来实现信息的嵌入. 当二维码存在小部分遮挡时,二维码的公共信息将无法解析,这不仅极大地降低了方案的实用性,还会引起攻击者的注意. 图 7(e)为本文方案中的隐写二维码,即使我们的隐写二维码中存在部分遮挡,我们的公共信息也可以正常读取,并且秘密信息也可以通过该隐写二维码正常恢复.

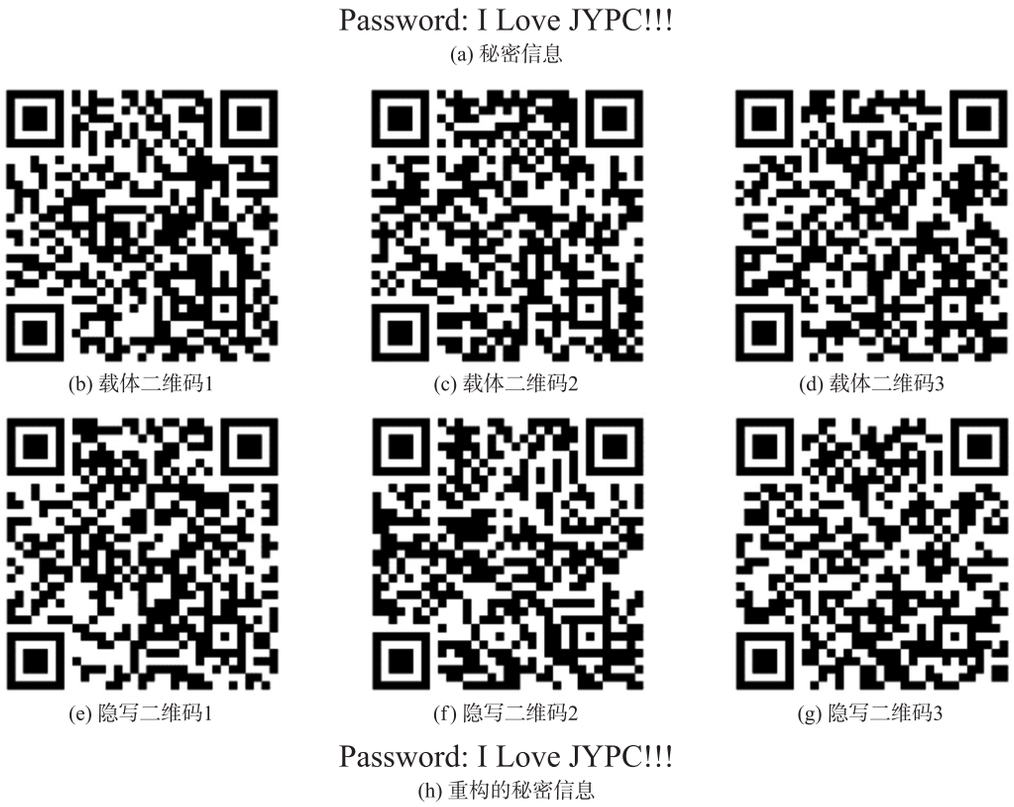


图 6　(2,3)门限 QRSS-EHC 方案实验结果

Fig. 6　The experimental result of (2, 3) threshold QRSS-EHC scheme



图 7　隐写二维码的遮挡实验

Fig. 7　The occlusion experiment of the steganographic QR codes

3.2　嵌入容量

本部分详细阐述了本方案中载体二维码的嵌入容量,并与现有的研究方案进行了比较[12-15],详细的嵌入容量比较如表 3 所示,其中二维码中的公共信息以 byte 模式进行存储. 在 Chuang 的方案[12]中,秘密信息被分享成一系列份额,并根据份额生成对应的二维码,所以 Chuang 方案中的嵌入容量就是存储在二维码中公共信息的长度. 具体来说,对于不同的版本和纠错级别,嵌入容量在(56,23624)bits 之间. 需要注意的是,Chuang 方案中生成的二维码由于载有的是份额,所以扫描器解析的结果是份额. 而份额是毫无意义的,这样在二维码传输或使用过程中容易吸引攻击者的注意从而存在暴露秘密信息的风险. 在 Lin 的方案[15]中,由于嵌入算法的随机性[16],实际的嵌入容量为(3,1215)bits. 在 Chow 等[13]和 Cheng 等[14]的方案中,由于他们是通过牺牲载体二维码的纠错冗余来实现信息的嵌入,所以他们方案的嵌入容量是二维码纠错冗余的大小,也就是(16,9720)bits.

表 3　嵌入容量比较

Table 3　The comparison of embedding capacity

方案	嵌入容量/bit	4-H QR 下(2,3)方案的嵌入容量/bit
[12]	(56,23624)	272
[13]	(16,9720)	256
[14]	(16,9720)	256
[15]	(3,1215)	32
本文	**(56,23624)-p**	**272-p**

值得注意的是,一旦二维码牺牲了纠错冗余,当二维码存在轻微污渍时,二维码也不能够被正常使用,这也会引起攻击者的怀疑从而被攻击者攻击. 我们的方案中,秘密信息借助二维码 RS 编码的同态性质嵌入到数据区域的补齐部分. 补齐部分指的是当二维码中公共信息的长度不足以填充满数据区域时,则需要在剩余部分填充补齐比特,以满足数据区域的长度要求. 这些补齐比特的内容不会影响二维码的正常解析. 补齐比特的长度与公共信息的长度之和等于数据区域数据的总长度,这意味着公共信息的长度越小,补齐比特的长度越大. 然而,二维码中必须包含一定量的公共信息,以确保二维码有实际意义. 假设载体是 4-H 版本二维码(数据区域大小为 272 bits),公共信息是常见的"google.com",存储该公共信息需要 10 bytes(80 bits),因此可嵌入的秘密信息大小为 272-80=192 bits;如果仅存储一个字符如"a",那么秘密信息大小为 272-8=264 bits. 由于本方案通过二维码中 RS 编码的同态性质实现信息嵌入,嵌入容量由补齐比特的长度决定,计算公式为 $l=8\times R-\sum_{j=1}^{p}(M_j+I_j+D_j)-T$,其中补齐比特的长度取决于公共信息的长度. 因此,公共信息越少,可嵌入的秘密信息长度越多. 假设公共信息 bit 长度为 p,其中 p 小于二维码数据区域长度,则本方案的可嵌入长度范围为(56,23624)-p bits.

以(2,3)门限 4-H 二维码方案为例,对现有的方案进行比较. 其中,根据 ISO/IEC 18004 查阅,Chuang 方案[12]的实际嵌入容量为 272 bits. Lin 的方案[15]中,实际嵌入容量为 32 bits. 在 Chow 等[13]和 Cheng 等[14]的方案中,因为通过牺牲纠错冗余实现信息的嵌入,而 4-H 二维码的纠错冗余是 256 bits,所以他们方案中的嵌入容量是 256 bits. 而我们的方案中,嵌入容量由公共信息决定,最大的可嵌入容量为 272 bits. 显然,我们方案的嵌入容量高于其他现有方案,并且不会像[13-15]中的方案牺牲二维码的纠错冗余从而导致二维码的纠错功能被破坏,也不会像[12]中的方案一样将无意义的份额作为隐写二维码的公共信息而引起攻击者的注意导致被攻击.

3.3 验证能力

为了防止不诚实参与者伪造二维码来重构秘密信息,需要在秘密重构前采取措施来验证参与重构二维码的真实性. 在这一部分中,详细阐述了本方案的验证能力,并与其他方案[12-15]进行了比较,表 4 展示了相关方案在验证能力方面的详细比较. 在文献[12-14]中,由于载体二维码中没有被嵌入任何的验证信息,因此这些方案不具备验证能力. 在 Lin 的方案[15]中,验证信息不是基于份额生成的,而是基于参与者密钥生成,换句话说,如果攻击者提供了一个假密钥,验证过程很容易被破坏. 因此,Lin 方案中的验证能力不能够抵御不诚实参与者的攻击[16]. 在我们提出的方案中,根据份额生成与剩余位相同长度的验证信息. 因此,验证信息的长度就是二维码中剩余位的长度. 根据 ISO/IEC 18004 标准,不同版本二维码的剩余位长度范围为(1,7)bits,因此二维码中验证信息的最大可嵌入为 7 bits. 以 4-H 载体二维码为例,由于 4-H 二维码的剩余位长度为 7,所以我们方案中的验证信息的长度为 7 位. 值得注意的是,我们方案中的验证信息是嵌入在二维码剩余位中,因此不会影响二维码的纠错冗余,即使二维码被部分损坏,也依然可以正常使用.

表 4 验证能力比较

Table 4 The comparison of authentication capacity

方案	验证信息长度/bit	4-H QR 下(2,3)方案的验证信息长度
[12]	0	0
[13]	0	0
[14]	0	0
[15]	0	0
本文	**(1,7)**	**7 bits**

为了更直观地展示本方案的优势,本文将验证能力使用指标 AR(authentication ratio)进行量化,AR 的计算公式如下

$$\mathrm{AR}=1-\left(\frac{1}{2}\right)^{l_U}, \tag{19}$$

式中,l_U 代表验证信息的长度.

在我们的方案中,对于一个隐写二维码,共有 7 bits 的验证信息被嵌入,所以 $\mathrm{AR}=1-\left(\frac{1}{2}\right)^{7}\approx 0.992$,也就是说能够成功探测隐写二维码中信息被篡改的概率是 99.2%. 因此,可以说本方案能够准确地检测隐写二维码的真实性.

3.4　纠错能力

众所周知,二维码在实际应用中常以纸质形式出现,例如商家的收款码等. 由于直接暴露在日常生活中,二维码难免会沾染细微污渍,如果污渍遮挡了隐写二维码的秘密信息区域,秘密信息将无法重构. 此外,若有不诚实的参与者或攻击者对隐写二维码的某些位进行篡改,秘密信息同样会丢失. 因此,对隐写二维码的误码进行校正是一个至关重要的功能. 然而,在之前的方案中,研究者并未充分考虑载体的纠错能力[12-15]. 例如,在[12]的方案中,若载体遭受篡改,载体二维码中的误码无法被正确纠正,但由于秘密信息以公共信息的形式嵌入,秘密信息本身依赖二维码的纠错功能仍可被恢复. 然而,这种嵌入方式使载体二维码的公共信息失去实际意义,容易引起攻击者的怀疑. 在[13-15]的方案中,秘密信息被嵌入到二维码的纠错冗余中,一旦二维码遭受攻击,不仅会破坏纠错功能导致二维码无法正常扫描解析,而且秘密信息也将无法恢复.

图 8 展示了我们方案中纠错能力的实验结果. 图 8(a)为原始隐写二维码;随后对该二维码中每个数据码元的某一位进行随机篡改,篡改后的结果如图 8(b)所示;图 8(c)对比了原始二维码与篡改后二维码的差异,其中红色模块表示被篡改的部分,黑色区域表示未被篡改的部分;接着,利用(8,4)扩展汉明码理论,我们成功恢复了原始隐写二维码,如图 8(d)所示,其与图 8(a)完全一致;最终,基于纠正后的隐写二维码,成功重构出图 8(e)所示的秘密信息. 然而,通过图 8(f-h)可以看出,[13-15]中的方案在载体二维码遭受篡改后,未能成功重构出秘密信息.



(a) 原始隐写二维码　(b) 被篡改的隐写二维码　(c) 被篡改的区域　(d) 恢复后的隐写二维码

(e) 本方案重构的秘密信息　(f) 方案[13]重构的秘密信息　(g) 方案[14]重构的秘密信息　(h) 方案[15]重构的秘密信息

图 8　隐写二维码纠错能力对比实验

Fig. 8　The comparison experiment of error correction capability of stego-QR Codes

3.5　鲁棒性

由于二维码通常以纸质形式发布或以图像形式在公共信道中传输,载有秘密信息的二维码容易受到各种常见攻击,如高斯噪声、均匀噪声、高斯模糊、压缩和旋转等. 因此,本节实验针对这些常见攻击进行了测试,表 5 展示了本方案中隐写二维码的鲁棒性. 与传统图像不同,二维码图像遭受攻击后不会扭曲其像素,因为其像素以黑白模块表示(0 为黑色,1 为白色),因此只要攻击不改变模块颜色,秘密信息仍可正常恢复. 在噪声实验中,对隐写二维码分别添加了 50%与 70%的高斯噪声和均匀噪声. 此外,为了提高存储容量,通常会对数据进行压缩,本文采用 JPEG 2000 压缩技术(质量系数分别为 70%和 100%)对隐写二维码进行处理. 由于二维码通常通过移动设备读取,旋转攻击也被纳入测试范围. 实验结果表明,如表 5 所示,隐写二维码在遭受上述攻击后,黑白模块未受影响,因此秘密信息仍能成功恢复,展现了较强的鲁棒性. 需要注意的是,二维码的解码结果会受到不同灯光、移动设备、扫描仪的影响[20].

表 5　隐写二维码的鲁棒性实验

Table 5　The robustness experiment of stego-QR Codes

常见图像攻击	高斯噪声:50%	高斯噪声:70%	均匀噪声:50%	均匀噪声:70%
被攻击后的 QR Code				
常见图像攻击	高斯模糊:2 pixels	高斯模糊:3 pixels	JPEG 2000:70%	JPEG 2000:100%
被攻击后的 QR Code				
常见图像攻击	旋转:45°	旋转:90°	旋转:135°	旋转:270°
被攻击后的 QR Code				

4　结论

在现有的二维码秘密分享方案中,如果验证能力只能单纯地检测被篡改的区域,而无法实现误码的纠正,那该方案的实用性会大大降低. 事实上,由于二维码纸质化的特殊性,比特误差会经常出现在二维码上. 如果这些误码能够得到纠正,二维码秘密分享方案的实用性将会大大提高. 因此,我们提出了一种(k,n)门限的基于扩展汉明码的二维码秘密分享方案(QR Secret Sharing with Extended Hamming Code,QRSS-EHC). 我们提出的方案不仅能抵抗二维码中码元存在单比特误码的情形,而且能够无损地纠正这些误码. 实验结果表明,本文所提出的算法具有较好的纠错能力和较高的嵌入容量.

如今,随着数字化进程的加速推进,个人信息的安全防护已经迫在眉睫,信息安全已然从行业的奢侈品变为必需品. 在今后的工作中,我们将把我们的安全方案推广到神经网络的梯度安全上,从而保证神经网络的安全;其次我们将寻找更好的纠错方法,以实现更优秀的纠错能力.

[参考文献]

[1] XIONG L,ZHONG X,YANG C. Transform domain-based invertible and lossless secret image sharing with authentication[J]. IEEE transactions on information forensics,2021,16:2912-2925.

[2] MASHHADI S,SAEEDI Z. A (t,n)-secret image sharing with steganography based on rook polynomial and LWE problem[J]. Multimedia tools and applications,2023,82(25):39077-39097.

[3] WU X,AN N,XU Z. Sharing multiple secrets in XOR-based visual cryptography by non-monotonic threshold property[J]. IEEE transactions on circuits and systems for video technology,2022,33(1):88-103.

[4] SHAMIR A. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613.

[5] BLAKLEY G R. Safeguarding cryptographic keys[C]//Managing Requirements Knowledge,International Workshop On. New York,USA:IEEE Computer Society,1979:313.

[6] XIONG L,HAN X,ZHONG X,et al. RSIS:a secure and reliable secret image sharing system based on Extended Hamming Codes in industrial internet of things[J]. IEEE internet of things journal,2021,10(3):1933-1945.

(下转第 138 页)

[37] CARSTENSEN S,CHUN-WEI LIN J. TKU-PSO:an efficient particle swarm optimization model for top-k high-utility itemset mining[J]. International journal of interative multimedia and artificial intelligence,2024:1-12.
[38] SONG W, LI J, HUANG C. Artificial fish swarm algorithm for mining high utility itemsets[C]//Advances in Swarm Intelligence:12th International Conference. Qingdao,China:Springer International Publishing,2021:407-419.
[39] GAO Z, HAN M, LIU S, et al. High utility itemsets mining based on hybrid harris hawk optimization and beluga whale optimization algorithms[J]. Journal of intelligent & fuzzy systems,2024,46(4):7567-7602.
[40] SONG W, HUANG C. Discovering high utility itemsets based on the artificial bee colony algorithm[C]//Advances in Knowledge Discovery and Data Mining: 22nd Pacific-Asia Conference. Melbourne, VIC, Australia: Springer International Publishing,2018:3-14.
[41] SUKANYA N S, THANGAIAH P R J. Enhanced differential evolution and particle swarm optimization approaches for discovering high utility itemsets[J]. International journal of computational intelligence and applications, 2023, 22(1): 2341005.
[42] ARUNKUMAR M S, SURESH P, GUNAVATHI C. High utility infrequent itemset mining using a customized ant colony algorithm[J]. International journal of parallel programming,2020,48:833-849

[责任编辑:杜忆忱]

(上接第 123 页)

[7] XIONG L,ZHONG X,XIONG N N,et al. QR-3S:a high payload QR code secret sharing system for industrial Internet of Things in 6G networks[J]. IEEE transactions on industrial informatics,2020,17(10):7213-7222.
[8] LI L L,HUANG P C,XIE R. QR Code secret sharing algorithm based on CRC[C]//2022 International Conference on Image Processing and Computer Vision. Okinawa,Japan:IEEE,2023:134-139.
[9] Information Technology:Automatic Identification and Data Capture Techniques:QR Code Bar Code Symbology Specification[M]. ISO/IEC 18004:2015. Geneva,Switzerland:ISO,2015.
[10] ZHANG L,SUN J,ZHANG X,et al. Two-level QR Code scheme based on region matrix image secret sharing algorithm[J]. Mathematical biosciences and engineering,2023,20(9):16678-16704.
[11] RAWAT A S, DESHMUKH M, SINGH M. QR shares based secret sharing scheme using DWT, random permutation and arithmetic modulo operation for QR secret[C]//2023 10th International Conference on Signal Processing and Integrated Networks. Noida,India:IEEE,2023:772-777.
[12] CHUANG J C, HU Y C, KO H J. A novel secret sharing technique using QR Code[J]. International journal of image processing,2010,4(5):468-475.
[13] CHOW Y W,SUSILO W,YANG G,et al. Exploiting the error correction mechanism in QR Codes for secret sharing[C]// Information Security and Privacy:21st Australasian Conference. Melbourne,VIC,Australia:Springer International Publishing, 2016:409-425.
[14] 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.
[15] LIN P Y. Distributed secret sharing approach with cheater prevention based on QR Code[J]. IEEE transactions on industrial informatics,2016,12(1):384-392.
[16] HUANG P C,CHANG C C,LI Y H. Sudoku-based secret sharing approach with cheater prevention using QR Code[J]. Multimedia tools and applications,2018,77:25275-25294.
[17] COX R. QArt codes[R/OL]. [2012-04-12]. http://research.swtch.com/qart.
[18] SAEIDI Z,YAZDI A,MASHHADI S,et al. High performance image steganography integrating IWT and Hamming Code within secret sharing[J]. IET image processing,2024,18(1):129-139.
[19] GOTTIMUKKALA A R, KUMAR N, DASH J K, et al. Image watermarking based on remainder value differencing and extended Hamming Code[J]. Journal of electronic imaging,2024,33(1):011003.
[20] MUNOZ-MEJIAS D, GONZALEZ-DIAZ I, DIAZ-DE-MARIA F. A low-complexity pre-processing system for restoring low-quality QR Code images[J]. IEEE transactions on consumer electronics,2011,57(3):1320-1328.

[责任编辑:杜忆忱]