DOI: 10. 19977/j.cnki.jfpnu.20220008

基于矩阵编码的秘密共享

余　湛[1]，吴红霞[1a]，薛醒思[2]

(1. 福建技术师范学院 a. 大数据与人工智能学院　b. 非遗数字化与多源信息融合工程研究中心，福建福清　350300；2. 福建工程学院，福建福州　350118)

摘　要：在分析各种信息隐藏算法优缺点的基础上，提出一种基于秘密共享的矩阵编码信息隐藏算法. 首先，发送方先通过矩阵编码将秘密信息或图像嵌入到负载图像中得到一幅共享图像，并将产生翻转的位置信息作为附加信息存储起来. 其次，利用相同的方法将附加信息嵌入到负载图像的副本中得到另外一幅共享图像；接收方在公共信道上接收到上述两幅共享图像后，先利用标记信息决定图像顺序，再通过校验矩阵进行校验就可以分别得到秘密信息和附加信息. 最后，通过附加信息就可以完全恢复原始的负载图像. 实验结果表明：该方法与现有的其他同类方法相比，在相同嵌入量的情况下得到的共享图像质量更优，并且该方法是完全可逆的.

关键词：秘密共享；(7，4) 汉明码；矩阵编码；可逆信息隐藏；高品质

中图分类号：TP309. 7　　文献标志码：A　　文章编号：1008-3421 (2022) 05-0477-12

随着互联网的普及，信息安全变得越来越重要，特别是在公共信道上传输数据的时候. 对比传统的数据保护技术，信息隐藏技术更加安全. 例如数据加密技术在传输的过程中可能会引起一些安全问题，因为加密数据是不可读取的，更容易引起攻击者的注意；而信息隐藏技术是将秘密信息隐藏在常见的数字媒体上，如文本、图像或音视频等，藏入前后的差别肉眼几乎无法区分，这使得它不容易被攻击者注意，从而增强了其在不安全信道上传输的安全性.

相关的信息隐藏技术有很多，常见的是利用数字图像作为载体，通过把秘密数据嵌入图像的方式有效地降低数据泄露的风险. 例如，最低有效位替换法就是一种被广泛使用的数据隐藏方法，它直接用秘密数据替换图像像素的最低有效位，并且可以根据数据量大小调整替换的位数，但是当需要替换更高位的时候会引起图像产生较为明显的失真，因此在使用中有一定的局限性. 后来有学者提出改进的方法，例如 EMD 法、矩阵编码法等. 1998 年 Crandall 最先提出矩阵编码方法[1]，首先依序在图像中选取 n 个像素，然后根据要嵌入的 k 位秘密数据，选取其中一个像素，使之加减 1 或者保持不变来实现信息隐藏. 由于该方法操作简单，并且可以取得令人满意的图像视觉效果，如今被广泛地应用于数据隐藏领域. 2016 年 Cao 等基于矩阵编码提出了一个提高数据嵌入量的数据隐藏方法[2]，它利用组合算法可以将 3 比特的秘密数据嵌入到像素组中，从而将嵌入率提高到接近 3bpp. 2019 年 Yu 等将上述方法进行改进，提出了一个基于矩阵编码的自适应位平面的数据隐藏方法[3]，该方法可以根据嵌入的数据量动态调整参与嵌入的像素组合，保证高

收稿日期：2021-11-28

基金项目：福建省自然科学基金面上项目 (2021J011237)，福建省中青年教师教育科研项目 (JAT201379).

作者简介：余　湛 (1981—)，男，福建邵武人，博士，讲师，主要研究方向为数据隐藏和图像处理.

吴红霞 (1980—)，女，湖北沙市人，讲师，主要研究方向为图像处理.

通信作者简介：薛醒思 (1981—)，男，福建福清人，博士，教授，主要研究方向为人工智能、数据科学和知识工程.

嵌入率的同时，实现最优的图像品质. 但是以上这些方法均不可逆，即提取秘密数据后，载体图像无法复原. 2019 年 Chen 提出一种基于(7，4) 汉明码和最高有效位预测的方案[4]，与现有方法相比，该方法可以实现更高的嵌入率、更好地标记图像质量和更少的数据嵌入执行时间. 因此，该方法适用于云端的实时应用. 2020 年 Wu 等提出一种通用的局部可逆的数据隐藏框架[5]，在数据传输阶段通过汉明码生成载体图像，在嵌入阶段将秘密信息隐藏到载体图像中形成标记图像，在数据提取和恢复阶段可以从标记图像中提取信息，并将标记图像恢复到载体图像.

秘密共享是 Shamir[6] 和 Blakley[7] 在 1979 年提出的一种视觉加密方法，它将秘密数据分成 22 个部分，每个部分由不同的参与者保存，将来只要 t 个参与共同合作就可以恢复出秘密数据. 受此启发，许多学者开始研究秘密共享，其中 Naor 和 Shamir 在 1995 年提出利用图像进行秘密共享[8]，此方法把秘密图像同载体图像通过公式计算得到的结果作为共享图像分发给 n 个参与者，将来 t 个参与者就可以解密图像. 许多秘密共享的方法在过去二十年里被相继提出，通常这些方法有两种方式创建共享图像：利用多项式计算或者利用参考矩阵查表得到共享图像. 2013 年 Abd El-Latif 等提出了一种结合了随机网格（RG）、误差扩散（ED）和混沌置换的算法[9]. 秘密图像首先基于混沌排列加密，然后由误差扩散生成的 n 个半色调阴影图像 RGs 共享，而恢复的秘密图像则从 k 个或更多阴影图像中恢复. 该方案计算简单，恢复时阴影图像的顺序可选，避免了复杂码本的设计，避免了像素扩展问题. 2014 年 Huynh 等提出了一种基于四向搜索算法的秘密共享方法[10]，它利用 Sudoku 矩阵作为参考矩阵，以一对像素为起始坐标，在其四个方向上搜索秘密数据的方式来创建共享图像和恢复秘密图像，该算法的时间复杂度较低，且能保证共享图像的品质和方法的安全性，因此十分适用于需要实时应用的场景. 2018 年 Cheng 等提出了一种基于 QR 码的秘密共享方案[11]，方案中共享的是有效的 QR 码，通过异或处理可以轻松地通过智能手机或其他 QR 扫描设备来恢复秘密信息. 2019 年 Liu 等基于 QR 码的识别模式和使用多项式秘密共享算法提出了一种保护隐私数据的方案[12]，QR 码被分为两级，其中公共信息可以被任何标准的 QR 阅读器解码，而隐私数据需要利用拉格朗日差值多项式进行解密. 2019 年 Li 等提出了一种基于多项式的秘密图像共享方案[13]，使物联网设备能够在云上无缝地共享图像. 该算法具有较高的嵌入容量，获得高质量的隐影图像，并能抵抗直方图分析. 还有一些方法在产生共享图像的过程中会利用算法在共享图像中藏入身份验证信息[14-15]，这样在恢复阶段可以通过提取这些身份信息，验证参与者的合法身份，以提高系统的安全性. 2019 年 He 等提出了一种加权的秘密图像共享方案[16]，根据云服务提供商的权重构造了一个扩展的 Mignotte 序列，并根据遥感图像的灰度值得到的哈希值生成图像隐影份额，然后将隐影分别存储在云上，最后利用中国剩余定理对遥感图像进行恢复. 2021 年 Yan 等提出基于中国剩余定理和错误检测码的秘密共享方案[17]，它可以在不增加共享大小的情况下实现纠错能力，对于某些噪声类型的攻击如最低有效位噪声、JPEG 压缩和椒盐噪声具有鲁棒性.

本文结合矩阵编码和秘密共享的优点，提出一种基于矩阵编码的秘密共享方法，该方法利用矩阵编码技术产生共享图像，并最终实现了完全可逆. 实验结果表明经过该方法嵌入秘密数据后得到的共享图像的品质很高，安全性和实时性都优于其他同类方法.

1 秘密共享

在 Shamir 提出的（t，n）门限机制中[6]，首先分享者从秘密信息 S 构造出 n 个共享信息 $\{y_i \mid i=1，2，\cdots，n\}$，并将它们分给事先确定好的参与者. 当参与者的人数大于或等于 t

时，他们共同合作就可以恢复秘密信息；当参与者的人数小于 t 时，将不能恢复秘密信息. 为了生成 n 个共享信息，分享者选择一个大的素数 p，并生成一个 $t-1$ 次多项式，如公式（1）所示:

$$F(x) = s_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \pmod{p} \quad (1)$$

其中，常数项 s_0 就是秘密信息 S，多项式系数（a_1，a_2，…，a_{t-1}）是属于 $[0, p-1]$ 取值范围的一组随机数列. 然后，分享者的共享信息为:

$$y_1 = F(1), y_2 = F(2), \cdots, y_n = F(n) \quad (2)$$

接着他把这些共享信息分发给 n 个参与者，其中只要任意 t 个参与者共同合作，就可以通过拉格朗日插值多项式重构多项式 $F(x)$ 获得秘密信息 S. 即

$$F(x) = \sum_{k=1}^{t} y_{ik} \prod_{j=1, j\neq k}^{t} \frac{x - i_j}{i_k - i_j} \quad (3)$$

下面通过一个例子解释 Shamir 的（2，3）秘密共享方案. 假设秘密信息 $S=83$，多项式 $F(x) = 83 + 7x \pmod{251}$，那么根据公式（2）可以分别得到: $F(1)=90$，$F(2)=97$ 和 $F(3)=104$，将这些结果分发给特定的参与者，因此得到（1，90），（2，97）和（3，104）三组数据. 将来这三名参与者当中任意两名共同合作就可以利用插值多项式计算多项式 $F(x)$，并由此得到秘密信息.

如图 1 所示，秘密图像 I 经过上述多项式计算后得到三张共享图像，这些共享图像上面的像素因为相对原图像素值都发生了变化，因此都是一些无意义的图像，即使被攻击者得到也无法知道原来的内容究竟是什么. 但是只要其中任意两名接收者共同合作，通过解码公式计算，就可以获得原始的秘密图像. 但就像之前讨论过的那样，无意义的图像在不安全的信道上传输容易引起攻击者的注意，因此，如果把这些共享图像利用信息隐藏技术嵌入到载体图像中去，那样系统的安全性将会显著提高.

2　矩阵编码

1950 年，由贝尔实验室 Richard Hamming 首先提出（7，4）汉明码技术[7]，即一个由四位原始数据和三位校验数据构成的二进制代码组合，可以在校验矩阵 H 的帮助下发现并校正任意一个位置发生的错误. 由于该方法操作简单，并且可以取得令人满意的图像视觉效果，如今被广泛地应用于数据隐藏领域[7].

2.1　汉明码的检测机制

（7，4）汉明码的具体说明如下，四位原始数据分别为 d_1，d_2，d_3，d_4，而三位奇偶校

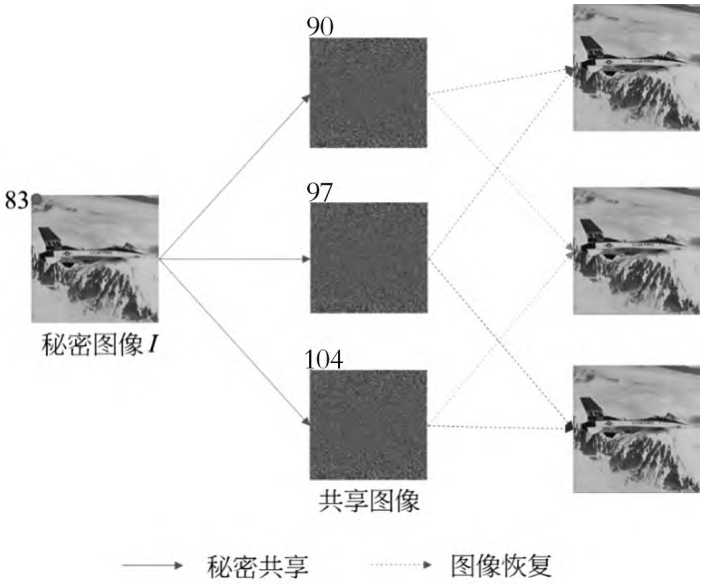

图 1　（2、3）秘密分享方法

验位 p_1，p_2，p_3 可以通过公式（4）获得，其中⊕表示异或操作符:

$$\begin{aligned} p_1 &= d_1 \oplus d_2 \oplus d_4, \\ p_2 &= d_1 \oplus d_3 \oplus d_4, \\ p_3 &= d_2 \oplus d_3 \oplus d_4. \end{aligned} \tag{4}$$

下面通过一个例子解释代码 C 的详细产生过程. 在图 2 中假设原始数据（d_1，d_2，d_3，d_4）=（1010）$_2$，那么根据公式（4）得到奇偶校验数据（p_1，p_2，p_3）=（101）$_2$，因此代码 C=（1011010）$_2$.

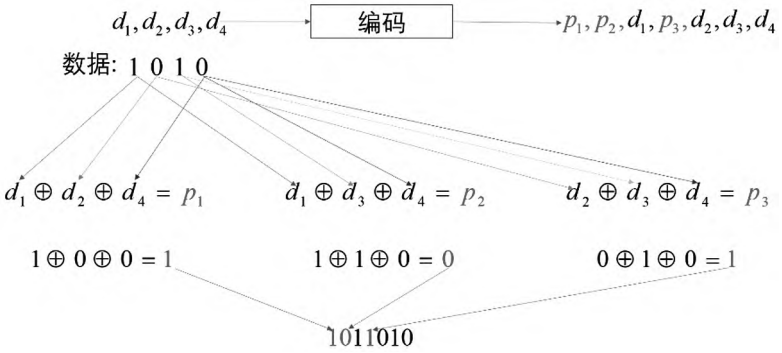

图2 数据的奇偶校验码

在解码端，接收者可以使用相同的奇偶校验矩阵 H 去侦测是否数据被篡改. 假设接收到的数据是 R，可以通过计算 z 来判断 R 是否被篡改，即

$$z = H \times R^{\mathrm{T}} \tag{5}$$

这里 z 被称为标志向量，具体来说，当 $z=0$ 表明数据 R 没有被篡改，即 $R=C$；否则，R 被篡改. 以 C=（0100101）$_2$ 为例，如果 C 的第 3 位被翻转，那么 R=（0110101）$_2$. 根据公式（5）可以计算出 z=（011）$_2$=（3）$_{10}$，$z\neq 0$ 意味着 1 比特错误发生在 R 的第 3 位，因此，原始数据可以通过翻转 R 的第 3 位来恢复，如图 3 所示，最后原始数据 C=（0100101）$_2$.

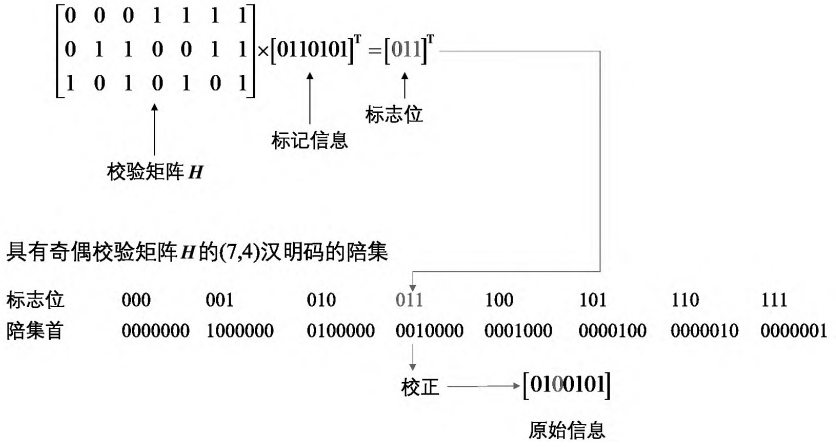

图3 基于(7,4) 汉明码的错误校验

2.2　矩阵编码算法

Crandall 在 1998 年提出基于（7，4）汉明码的图像隐藏方法即矩阵编码算法，在该方法中，只需要在原始图像中选择连续 7 个像素，通过修改其中一个的像素值，使之加减 1 或者保持不变来隐藏 3 比特的秘密信息.

首先依序从原始图像中提取 7 个像素的最末位组成一个 7 比特长的二进制序列. 其次利用随机数生成器产生一个八进制的一维数组 S 代表秘密信息，即 $S=\{s_j \mid j=1,2,\cdots,n\}$，这里 s_j 表示数组 S 的第 j 个元素，并且 $s_j \in \{0,1,\cdots,7\}$. 最后利用公式（6）计算标志位 z，若 $z=0$，原始序列 x 保持不变；若 $z\neq 0$，则将其转换成八进制数 z'，并翻转 x 的第 z' 位来产生新的二进制的标记序列 y，这里 x 和 y 分别代表原始序列和标记序列.

$$z=(\boldsymbol{H}\times \boldsymbol{x}^{\mathrm{T}})^{\mathrm{T}} \oplus s_j \tag{6}$$

在嵌入完成后，再用标记序列 y 的元素替换对应的原始像素最末位，以得到标记图像. 在接收端，接收者从标记图像中依序提取 7 个像素的最末位构成二进制序列 y，然后 s_j 的提取可以通过公式（7）进行:

$$s_j=\mathrm{conv}(\mathrm{mod}(\boldsymbol{H}\times \boldsymbol{y}^{\mathrm{T}},2))_{10} \tag{7}$$

这里上标 T 表示转置符，mod（·，2）表示模 2 操作，用来获得 3 比特秘密数据，conv（·）表示一个将二进制数转换为八进制数的函数. 矩阵编码可以取得令人满意的嵌入表现，因为对原始图像来说，每嵌入 3 比特的数据，图像最多改变了 1，因此图像的失真极小，得到的标记图像的品质非常高. 但是目前基于矩阵编码的可逆信息隐藏的研究还非常少.

3　矩阵编码的秘密共享

本小节将介绍基于矩阵编码的秘密共享方法，该方法可以分成两个部分：共享信息构建算法，以及秘密信息提取与原始图像恢复算法. 共享信息构建算法的流程图如图 4 所示，发送者将原始图像、秘密信息和校验矩阵一起输入到基于矩阵编码的秘密共享算法中，结果会输出两个藏有秘密信息的共享图像. 这些图像看起来和原始图像非常相似，只有特定的接收者通过解码算法才可以得到正确的秘密信息.

在 3.1 小节中，详细介绍共享信息构建算法，所有的步骤可以参照图 4 所示. 在共享信息被创建以后，发送者将把共享信息通过公共信道发送给特定的接收者. 为了得到秘密信息和恢复原始图像，接收者需要共同合作才能对共享信息进行解码，这些将在 3.2 小节中详细介绍.

3.1　共享图像构建算法

为了实现秘密信息的共享，秘密信息的发

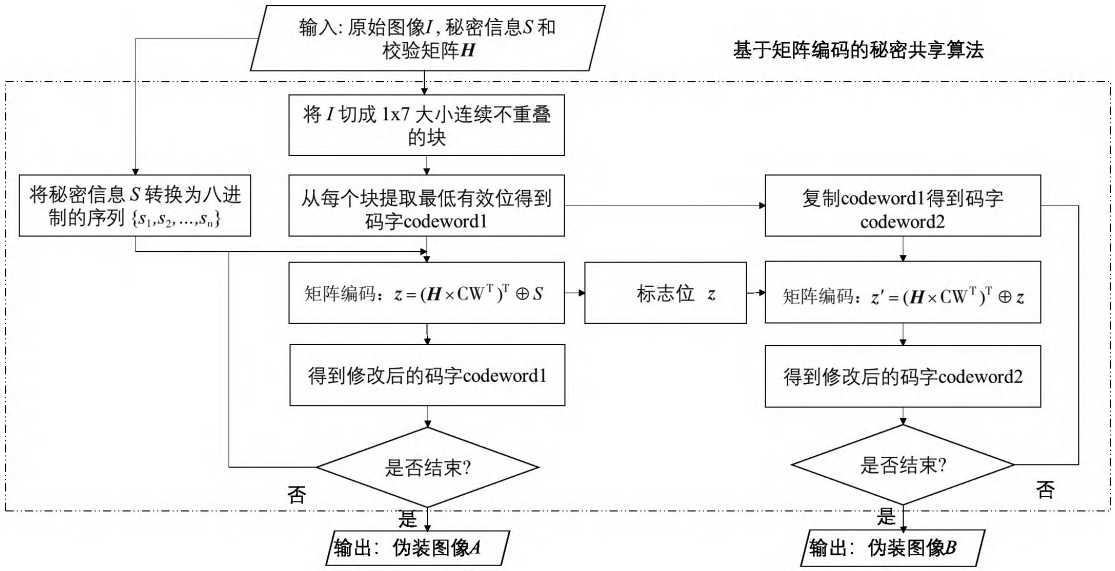

图 4　基于矩阵编码的秘密共享算法流程图

送者需要构建共享信息，并将共享信息发布给所有的参与者，因此输入信息包括秘密信息（也可以是秘密图像）、负载图片和奇偶校验矩阵. 详细的过程如下列伪代码所示.

a) 输入：秘密信息 $\{S_i \mid i=1，2，\cdots，n\}$ 且 $S_i \in [0，7]$，原始图像 I，奇偶校验矩阵 $\boldsymbol{H}$;

b) 输出：伪装图像 I_1 和 I_2.

第一步：按照光栅扫描的顺序（从左到右从上到下）把原始图像划分为一个个连续、不重叠的 1×7 大小的块 $\left\{C_i \,\middle|\, i=1，2，\cdots，\dfrac{\boldsymbol{H}\times\boldsymbol{W}}{7}\right\}$;

第二步：依次从每个块中取出每个像素的最低有效位组成一个二进制一维数组即码字 $\left\{\mathrm{CW}_i \,\middle|\, i=1，2，\cdots，\dfrac{\boldsymbol{H}\times\boldsymbol{W}}{7}\right\}$;

第三步：将这些码字 CW_i 和 S_i 分别通过矩阵编码运算，可以得到标记码字 MCW_{1i} 和标志位 z_{1i};

第四步：用标记码字 MCW_{1i} 依次替换对应块 C_i 的最低有效位，得到标记块 C_{1i};

第五步：重复第三、四步的操作，最后得到标记图像 I_1;

第六步：如果在第三步中，用相同的码字 CW_i 和标志位 z_i 进行矩阵编码运算，那么可以得到另一组标记码字和标志位，分别记作 MCW_{2i} 和 z_{2i};

第七步：用标记码字 MCW_{2i} 依次替换对应块 C_i 的最低有效位，得到标记块 C_{2i};

第八步：重复第六、七步的操作，最后得到伪装图像 I_2.

为进一步解释，以图 5 作为生成共享信息的示例. 以原始图像的第 i 块 C_i 的构建过程为例，假设秘密信息 $S_i=5$，图像块 $C_i=[7，10，9，6，3，5，17]$，首先取 C_i 每个元素的最低有效位组成码字 $\mathrm{CW}_i=[1，0，1，0，1，1，1]$；然后将 CW_i 和 S_i 进行矩阵编码运算，得到标记码字 $\mathrm{MCW}_{1i}=[1，0，0，0，1，1，1]$ 和标志位 $z_{1i}=3$；接着用标记码字替换 C_i 的最低有效位，得到标记图像块 $C_{1i}=[7，10，8，6，3，5，17]$；接着再将码字和标志位一起进行矩阵编码运算，得到标记码字 $\mathrm{MCW}_{2i}=[1，0，1，0，0，1，1]$ 和标志位 $z_{2i}=5$，替换原有图像的最低有效位，得到标记图像块 $C_{2i}=[7，10，9，6，2，5，17]$.

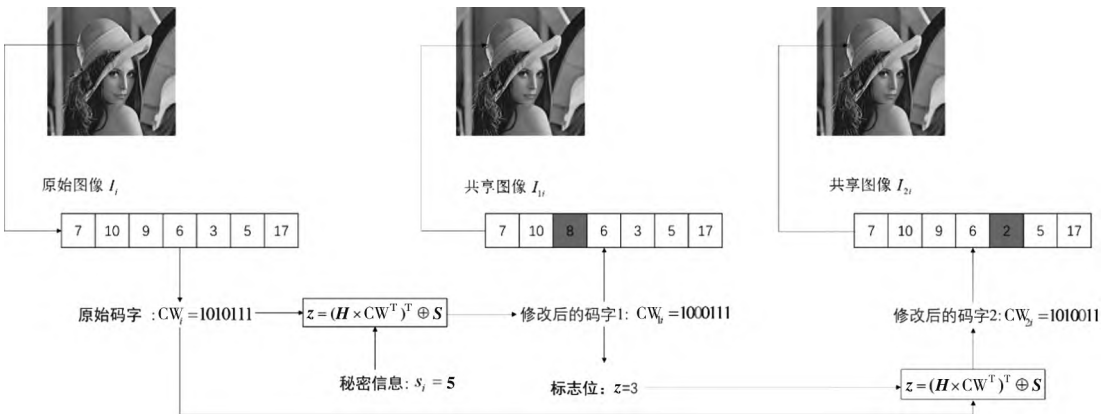

图5 共享图像构建算法

3.2 秘密图像提取和负载图像恢复

为了获取秘密信息，接收者必须共同合作，把各自的共享图像放到一起，然后利用秘密信息提取与原始图像恢复算法进行解码，才可以得到秘密信息和恢复原始图像. 详细的提取与恢复算法如下列伪代码所示.

a) 输入：标记图像 I_1 和 I_2，奇偶校验矩阵 $\boldsymbol{H}$;

b) 输出：秘密信息 $\{S_i \mid i=1，2，\cdots，n\}$ 且 $S_i \in [0，7]$，原始图像 I.

第一步：按照光栅扫描的顺序（从左到右从上到下）把标记图像 I_1 和 I_2 划分为一个个连续、不重叠的 1×7 大小的块 $\left\{C_{1i},C_{2i}\,\middle|\,i=1,2,\cdots,\frac{H\times W}{7}\right\}$；

第二步：依次从每个块中取出每个像素的最低有效位组成一个二进制一维数组即码字 $\left\{C_{1i},\ C_{2i}\,\middle|\,i=1,\ 2,\ \cdots,\ \frac{H\times W}{7}\right\}$；

第三步：将码字 CW_{1i} 和校验矩阵 H 通过公式（7），计算得到秘密信息 S_i；

第四步：重复步骤三，将得到的秘密信息 S_i 进行连接后得到秘密信息 S；

第五步：将码字 CW_{2i} 和校验矩阵 H 通过公式（7），计算得到标志位 z_{1i}；

第六步：若标志位 $z_{1i}=0$，则码字 CW_{1i} 保持不变；若标志位 $z_{1i}\neq 0$，则将码字 CW_{1i} 对应位置翻转，得到更新后的码字 CW_i；

第七步：用码字 CW_i 替换 C_{1i} 的最低有效位；

第八步：重复步骤六、七，最后得到原始图像 I.

下面通过一个例子解释秘密信息提取和图像恢复. 首先信息的接收者收集到伪装图像第 i 块的信息，即 $B_{1i}=$ [7，10，8，6，3，5，17] 和 $B_{2i}=$ [7，10，9，6，2，5，17]，分别提取最低有效位得到标记码字 $S_1=$ [1，0，0，0，1，1，1] 和 $S_2=$ [1，0，1，0，0，1，1]；然后分别将这两个码字与奇偶校矩阵进行解码运算，得到秘密信息 $S_i=101$ 和修改标志位 $\mathrm{Syndrome}=011$；接着利用标志位将标记码字 S_1 的第 3 位比特位进行翻转，得到原始码字 $S=$ [1，0，1，0，1，1，1]；最后用原始码字替换 B_{1i} 的最低有效位，得到原始图像块 $B_i=$ [7，10，9，6，3，5，17].

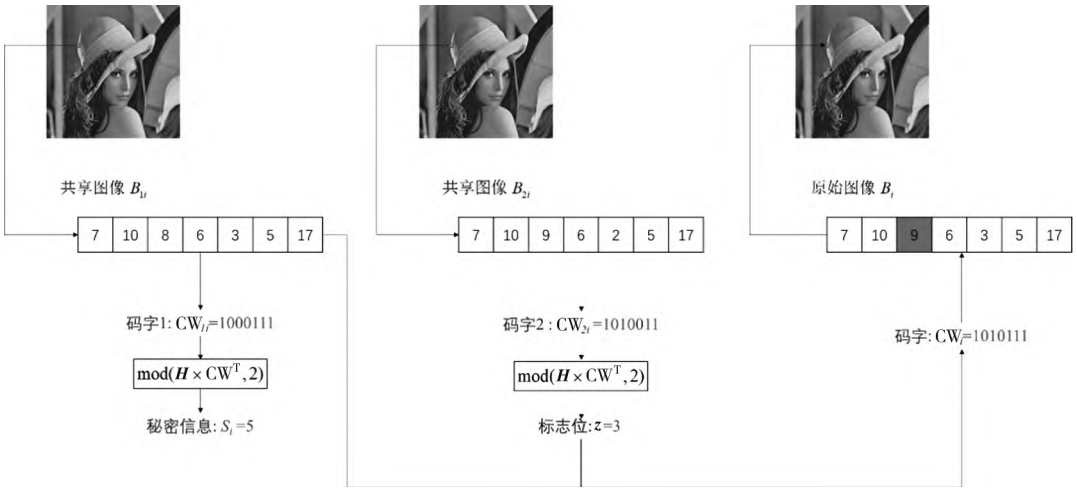

图6　秘密图像提取和负载图像恢复算法

4　实验结果和分析

本节为基于编码矩阵的秘密共享方案的实验结果展示和分析。实验软硬件平台分别选用 MATLAB R2017a 和一台双核 CPU，8 GB RAM 的计算机，实验图像选用 9 幅大小为 512×512 像素的灰度图像作为载体图像，测试图像如图 7 所示. 下面将分为 4 个小节分别从安全性、图像品质、时间复杂度和像素扩张这四个方面展示，并同其他同类方法的实验结果进行对比分析.

4.1　安全性

为了保证本方法的安全性和鲁棒性，嵌入秘密图像后得到的共享图像不能泄露任何关于秘密图像的信息，并且得到的共享图像都是有意义的图像，它们看上去就和普通的图像没有什么区别，这就很大程度上避免一些别有用心的人的怀疑，进一步提高了安全性. 如图 8 所示，通过对比原始图像和共享图像的直方图，可以发现嵌入前后的图像像素分布十分相似，

仅有一些细微的差别，因此像素分析对本方案无效. 另外如图 8 所示，两幅嵌入了秘密信息的共享图像同原始图像从视觉上几乎没有任何差别，因此本方案具有良好的视觉质量.

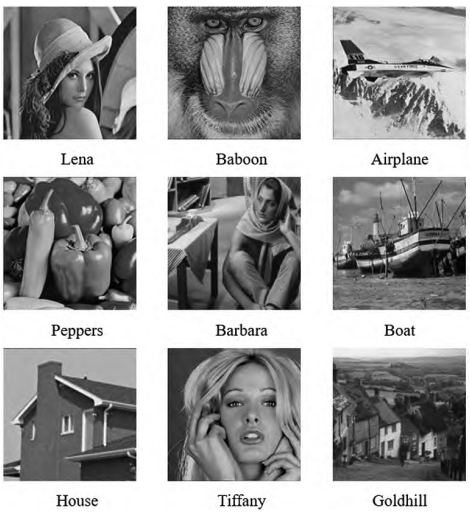

图7 测试图像

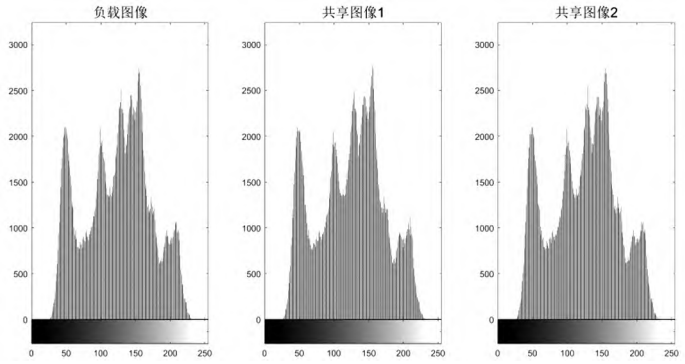

图8 共享图像像素分布图

实验还利用 RS 隐写分析技术来验证本方法的安全性，该分析方法常被用来检测最低有效位是否嵌入了隐藏信息. 经该函数计算得到 R_M、R_{-M}、S_M 和 S_{-M} 四个结果被用来判定检测图像中是否包含了隐藏的信息. 如果以上结果满足：$R_M \approx R_{-M} > S_M \approx S_{-M}$，则图像中没有包含隐藏信息；否则图像中包含隐藏信息. 实验对九幅测试图像进行了测试，并将测试结果记录在表 1 中. 从中可以发现 R_M 与 R_{-M} 的结果非常相似，共享图像 I_1 和 I_2 的平均差值分别为 0.016 8 和 0.017 6；而 S_M 与 S_{-M} 的结果也非常相似，共享图像 I_1 和 I_2 的平均差值分别为 0.009 3 和 0.011 5.

综上所述，实验从视觉和隐写分析两个角度测试了本方案的安全性，实验结果表明，方法整体安全性比较高.

表 1 分别对共享图像进行 RS 隐写分析的结果

图像	共享图像 1		共享图像 2	
	$\lvert R_M - R_{-M} \rvert$	$\lvert S_M - S_{-M} \rvert$	$\lvert R_M - R_{-M} \rvert$	$\lvert S_M - S_{-M} \rvert$
Lena	0.009 7	0.014 6	0.011 1	0.013 9
Baboon	0.006 6	0.009 9	0.002 1	0.009 2
Airplane	0.017 9	0.005 8	0.019 9	0.009 3
Peppers	0.007 2	0.000 2	0.015 2	0.011 9
Boats	0.031 7	0.017 8	0.022 3	0.014 2
House	0.005 8	0.013 5	0.005 0	0.014 9
Tiffany	0.016 6	0.004 8	0.017 2	0.004 7
Barbara	0.027 6	0.012 2	0.031 1	0.024 5
Goldhill	0.027 9	0.004 9	0.034 5	0.000 9
Average	0.016 8	0.009 3	0.017 6	0.011 5

4.2　图像品质

图像品质可以用均方误差（MSE）和峰值信噪比（PSNR）来表示，实际上当标记图像的 PSNR 值在 30 以上时，就会有一个比较好的质量. 具体的计算公式为:

$$\mathrm{MSE}=\frac{1}{W\times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I_{1,i,j}-I_{2,i,j}\right)^2 \quad (8)$$

$$\mathrm{PSNR}=10\times\log_{10}\frac{255^2}{\mathrm{MSE}} \quad (9)$$

这里 $W\times H$ 表示图像的宽和高，$I_{1,i,j}$ 和 $I_{2,i,j}$ 分别对应原始图像与标记图像在第 i 行和第 j 列的像素值. 当计算出的 PSNR 值越大，标记图像的质量越好，反之亦然.

表 2　对比不同得到的共享图像品质

峰值信噪比（dB）	文献［18］方案		文献［10］方案		本文方案	
原始图像	共享图像 1	共享图像 2	共享图像 1	共享图像 2	共享图像 1	共享图像 2
Lena	43.40	43.35	39.40	39.17	57.16	57.17
Baboon	43.44	43.36	39.34	39.16	57.16	57.17
Airplane	43.48	43.34	39.16	39.18	57.16	57.17
Peppers	43.28	43.36	39.16	39.13	57.16	57.17
Barbara	43.35	43.32	39.14	39.13	57.15	57.17
Boats	43.34	43.34	39.76	39.17	57.15	57.17
House	41.98	42.55	39.35	39.20	57.17	57.17
Tiffany	43.30	43.36	39.33	39.15	57.15	57.17
Goldhill	43.28	43.33	39.25	39.16	57.17	57.17

在测试图像品质的实验中，比较了同样采用秘密共享的文献［18］方案、文献［10］方案和本文方案在相同藏量的情况下得到的共享图像平均 PSNR 值，在秘密信息为 112 347 比特的情况下，具体实验结果如表 2 所示，文献［18］的方案 PSNR 平均值为 43.23，文献［10］的方案 PSNR 平均值为 39.24，而本文方案 PSNR 平均值为 57.16，得到的共享图像的 PSNR 平均值最高，分别比文献［18］和文献［10］方案的 PSNR 值高出 13.93 和 17.92. 另一方面，可以计算出文献［18］、文献［10］的方案和本文方案在 9 幅测试图像的 PSNR 值的均方差分别为: 0.368、0.155 和 0.007. 从以上分析可知，通过秘密共享的方法得到的共享图像的质量主要与算法本身关系比较密切，而与采用的测试图像无关.

图9　嵌入、提取和重构性能测试

如图 9 所示，在对本方案的性能测试实验中，分别选择 Airplane 和 Lena 作为秘密图像和负载图像进行测试. 首先，利用共享图像构建算法把秘密图像嵌入到负载图像并得到两幅共享图像，即图 9（c）和（d），这两幅图像看上去十分相似，用肉眼根本无法区分它们之间的差别，而它们的 PSNR 值也分别达到 57. 160 9 和 57. 167 0；其次，利用提取与恢复算法就可以正确地从这两幅共享图像中提取出秘密图像；最后，利用标志位信息就可以把共享图像恢复到原始的负载图像，准确率为 100%，即 PSNR = ∞. 因此，无论从图像的视觉效果还是 PSNR 值，本方案的实验结果都是高质量的，并且嵌入和恢复图像也完全可逆.

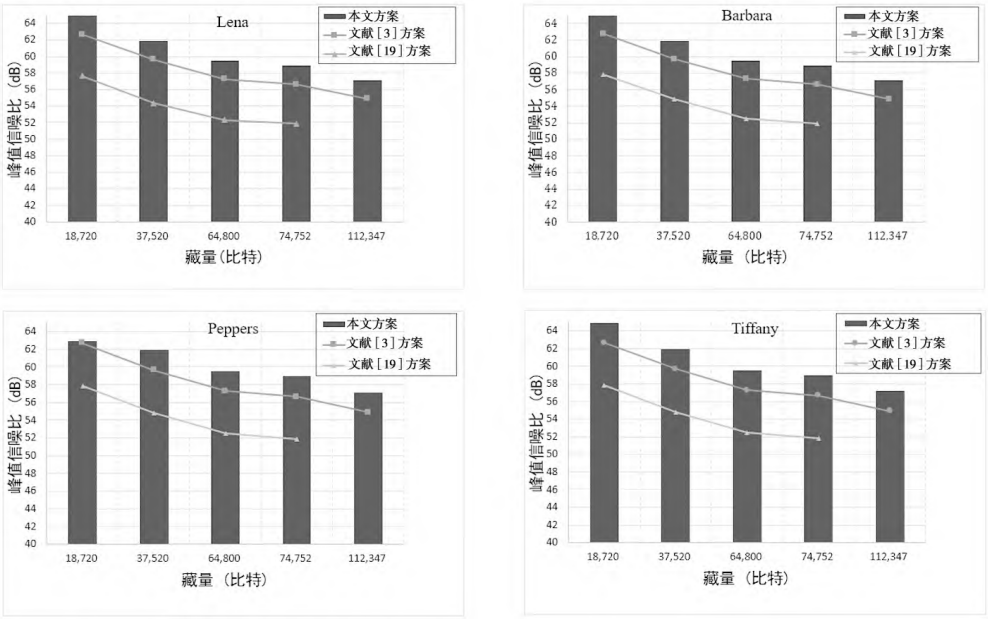

图10 相同藏量下不同方法在测试图(a) Lena,(b) Barbara,(c) Peppers和(d) Tiffany的PSNR对比

如图 10 所示，在固定藏量的实验中，选择了四幅测试图像，其中包括两幅纹理复杂的图像 Barbara、Peppers 和两幅纹理平滑的图像 Lena、Tiffany. 然后测试这些图像在藏量分别为 18 720、37 520、64 800、74 752 和 112 347 比特时得到的共享图像的峰值信噪比 PSNR 值，并用图表显示，其中橙色带方形节点的折线代表文献 [3] 的方案，绿色带三角形节点的折线代表文献 [19] 的方案[19]，蓝色的柱形图代表本文方案. 从图 10 中可以看出，本文方案的 PSNR 均优于文献 [3] 和文献 [19] 的方案，并且随着固定藏量的增加 PSNR 值下降得更加平缓，仍然保持在 57. 17 dB 以上，远远大于 30 dB 的标准，体现了本文方案在输出图像的品质上具备优势.

4. 3 计算复杂度

在秘密共享的方案中，如何在构建共享图像以及从共享图像中提取秘密信息的同时保持较低的计算复杂度非常重要，它将影响该方案的实际应用价值. 本文方案在创建共享图像阶段以及在提取秘密信息阶段的算法如 3. 1 和 3. 2 小节所述，算法的时间复杂度主要取决于矩阵编码运算，时间复杂度为 $O(n)$，即用极低的代价就可以实现秘密共享的效果. 表 3 展示了近年来提出的秘密共享方案同基于矩阵编码的共享方案计算复杂度的对比结果，从中可以看出本方案跟其他方案相比计算复杂度更低.

表 3　不同方法的计算时间复杂度比较

函数	文献[10]方案	文献[9]方案	文献[11]方案	文献[7]方案	本文方案
多项式	No	Yes	No	No	No
异或	Yes	No	Yes	No	Yes
差值扩张	Yes	No	Yes	No	No
搜索/聚类	Yes	No	Yes	Yes	No
乘法	Yes	Yes	Yes	No	No

4.4　像素扩张

在之前提到的秘密共享的方案中，通常在产生共享图像的过程中会出现像素扩张的问题，而在本文方案中，负载图像上连续 7 个像素的最低位通过矩阵编码的方式嵌入 3 个比特的秘密信息，最后产生 2 个共享图像，它们有着和负载图像相同的大小. 当然，可以通过使用更多的比特位来提高整体的嵌入率，虽然会导致得到的标记图像的图像品质变差，但不会引起像素扩张的问题.

5　结论

本文提出了一种新的基于矩阵编码的秘密共享方法，该方法包含能够产生高质量的共享图像的构建算法，也包含能够通过共享图像得到秘密图像的提取算法，更包含了可以将共享图像还原回原始图像的还原算法. 实验结果表明，本方案不仅满足隐藏秘密图像的需求，而且还提供了完全可逆的隐藏策略，即接收方不仅可以正确地提取秘密图像，还可以恢复负载图像，这一改进增强了本方案的实用性，并且算法的计算复杂度很低，可以满足一些特定场合下实时应用的需求.

参考文献:

[1] 陈鲁生，沈世镒.编码理论基础[M].北京: 高等教育出版社，2005.

[2] CAO Z，YIN Z，HU H，et al.High capacity data hiding scheme based on (7，4) Hamming code [J].Springer-Plus，2016，5(1)：175-187.

[3] YU Z，LIN C C，CHANG C C. ABMC-DH: An Adaptive Bit-Plane Data Hiding Method Based on Matrix Coding [J]. IEEE Access，2020，8: 27634-27648.

[4] CHEN K，CHANG C C.Real-time error-free reversible data hiding in encrypted images using (7，4) Hamming code and most significant bit prediction [J].Symmetry，2019，11(1)：51.

[5] WU X，YANG C N，LIU Y W.A general framework for partial reversible data hiding using Hamming code [J]. Signal Processing，2020，175: 107657.

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

[7] 庞辽军，王育民.基于 RSA 密码体制(t，n)门限秘密共享方案 [J].通信学报，2005，6: 70-73.

[8] NAOR M，SHAMIR A.Visual cryptography [J].Lecture Notes in Computer Science，1995，950: 1-12.

[9] ABD EL-LATIF A A，YAN X，LI L，et al.A new meaningful secret sharing scheme based on random grids，error diffusion and chaotic encryption [J]. Optics and Laser Technology，2013，54: 389-400.

[10] HUYNH N T，BHARANITHARAN K，CHANG C C. Quadri-directional searching algorithm for secret image sharing using meaningful shadows [J].Journal of Visual Communication and Image Representation，2015，28: 105-122.

[11] 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.

[12] LIU S，FU Z，YU B. A two-level QR code scheme based on polynomial secret sharing [J]. Multimedia Tools and Applications，2019，78(15)：21291-21308.

[13] LI L，HOSSAIN M S，ABD EL-LATIF A A，et al.Distortion less secret image sharing scheme for internet of things system [J]. Cluster Computing，2019，22(1)：2293-2307.

[14] WANG P, HE X, ZHANG Y, et al. A robust and secure image sharing scheme with personal identity information embedded [J]. Computers & Security, 2019, 85: 107-121.

[15] JIANG Y, YAN X, QI J, et al. Secret image sharing with dealer - participatory and non - dealer - participatory mutual shadow authentication capabilities [J]. Mathematics, 2020, 8(2): 234.

[16] HE Q, YU S, XU H, et al. A weighted threshold secret sharing scheme for remote sensing images based on Chinese remainder theorem [J]. Computers Materials & Continua, 2019, 58(2): 349-361.

[17] YAN X, LIU L, LI L, et al. Robust secret image sharing resistant to noise in shares [J]. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2021, 17(1): 1-22.

[18] LIN P Y, LEE J S, CHANG C C. Distortion - free secret image sharing mechanism using modulus operator [J]. Pattern Recognition, 2009, 42(5): 886-895.

[19] JANA B, GIRI D, KUMAR M. Dual image based reversible data hiding scheme using(7,4) hamming code [J]. Multimedia Tools and Applications, 2018, 77: 763-785.

[20] CHANG C C, LIN C C, LE T H N, et al. Self-verifying secret sharing using error diffusion and interpolation techniques [J]. Ieee transactions on Information Forensics and Security, 2009, 4(4): 790-801.

Secret Sharing Based on Matrix Encoding

YU Zhan[1], WU Hongxia[1a], XUE Xingsi[2]

(*1. Fujian Polytechnic Normal University a. school of Big Data and Artificial Intelligence b. Intangible Cultural Heritage Digitization and Multi-Source Information Fusion Engineering Research Center, Fuqing, Fujian 350300, China; 2. Fujian University of Technology, Fuzhou, Fujian 350118, China*)

Abstract: A secret sharing framework is proposed to provide separable reversible data hiding for gray image in this paper. A combination of secret sharing and matrix coding is used to enhance the hiding capacity and quality. In this scheme, the sender firstly obtains a shadow and syndrome of flipping position by embedding the secret images into cover image through matrix coding algorithm. Another shadow is obtained by embedding syndrome into a duplicate of cover image in the same way. The secret image revealing and cover image reconstructing include three steps. Firstly, the receiver determines the order of the images with the help of the marked information, and then the secret image and additional information are extracted through a parity check matrix. Finally, the additional information helps to completely reconstruct the cover image. Experimental results show that compared with other state-of-the-art schemes, the approach can attain high-quality shadows with the same embedding quantity, and it is completely reversible.

Key words: secret sharing; (7,4) Hamming code; matrix coding; reversible information hiding; high quality

(责任编辑: 赵少卡)