计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(5):269−276 [doi: 10.15888/j.cnki.csa.008429]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 CRT 的无损高效门限彩色图像秘密共享信息隐藏算法①

陈维启[1], 张珍珍[2], 李祯祯[2], 丁海洋[2], 李子臣[2]

[1](北京印刷学院 信息工程学院, 北京 102600)
[2](北京印刷学院 数字版权保护技术研究中心, 北京 102600)
通信作者: 陈维启, E-mail: 550898639@qq.com

摘　要: 目前对秘密图像共享的研究主要集中在灰度图像上, 而日常生活中使用的图像大多是彩色的, 因此, 研究彩色图像的秘密共享具有重要的意义和应用价值. 该方案将基于中国剩余定理 (CRT) 的秘密共享与 DCT 信息隐藏技术进行结合, 保障了传输彩色秘密图像的安全性. 在生成端, 利用 DCT 信息隐藏算法将彩色秘密图像通过 CRT 生成的彩色秘密影子图像, 嵌入至用户提供的彩色载体图像中, 并分发. 在恢复端提取出影子图像, 使用 CRT 恢复彩色秘密图像. 该过程满足 (*t*, *n*) 门限. 实验结果验证, 该算法可实现无损恢复, 并用相关参数对该方案进行评估, 优于其他方案.

关键词: 秘密共享; 彩色图像; CRT; 门限; 信息隐藏; 无损; 可验证; 隐藏算法

引用格式: 陈维启,张珍珍,李祯祯,丁海洋,李子臣.基于 CRT 的无损高效门限彩色图像秘密共享信息隐藏算法.计算机系统应用,2022,31(5):269–276. http://www.c-s-a.org.cn/1003-3254/8429.html

Lossless and Efficient Threshold Color Image Secret Sharing and Information Hiding Algorithm Based on CRT

CHEN Wei-Qi[1], ZHANG Zhen-Zhen[2], LI Zhen-Zhen[2], DING Hai-Yang[2], LI Zi-Chen[2]

[1](Information and Engineering Academy, Beijing Institute of Gtaphic Communication, Beijing 102600, China)
[2](Digital Copyright Protection Technology Research Center, Beijing Institute of Gtaphic Communication, Beijing 102600, China)

Abstract: At present, the research on secret image sharing mainly focuses on gray-scale images. However, most images used in daily life are color images. Therefore, it is of great significance and application value to study the secret sharing of color images. The scheme combines the secret sharing based on the Chinese remainder theorem (CRT) with DCT information hiding technology to ensure the security of color secret image transmission. At the generation end, the color secret shadow image generated by CRT is embedded into the color carrier image of users and distributed by DCT information hiding algorithm. The shadow image is extracted at the recovery end, and the color secret image is recovered by CRT. The process satisfies the (*t*, *n*) threshold. The experimental results show that the algorithm can achieve lossless recovery, and the evaluation with relevant parameters reveals that the scheme outperforms other ones.

Key words: secret sharing; color image; Chinese remainder theorem (CRT); threshold; information hiding; lossless; verifiable; hiding algorithm

1　引言

随着计算机网络技术的进步和信息时代的到来, 几乎每个人都有一部智能手机, 我们在日常生活中经常用它来拍照, 记录一些图像信息, 并在互联网上共享

① 基金项目: 国家自然科学基金 (61370188); 北京市教委科研计划 (KM202010015009, KM202110015004); 北京印刷学院科研创新团队项目 (Eb202101); 北京印刷学院博士启动金项目 (27170120003/020)
收稿时间: 2021-07-07; 修改时间: 2021-08-04; 采用时间: 2021-08-12; csa 在线出版时间: 2022-04-11

和传输数字图像. 虽然电脑和智能手机使我们能够方便地传输图像信息, 但通过互联网传输重要或秘密的图像, 如商业企业或军方使用的图像, 可能会带来一定的危险. 攻击者或间谍可以通过监视互联网来检测和捕获有价值的图像, 因此在考量如何保证秘密图像传输的安全性时, 需要采用相应的图像保护机制.

加密[1,2] 和信息隐藏[3,4] 是目前最常见的图像保护技术. 加密后的图像是类噪声的, 使攻击者看不到任何秘密信息, 但类噪声图像很容易被攻击者怀疑含有秘密信息, 从而破坏甚至破解原始的秘密图像, 造成原秘密图像的破坏和泄露. 信息隐藏可以弥补加密的不足. 它能将秘密图像嵌入到可理解的载体图像中, 使攻击者不会怀疑秘密信息的存在, 从而有效地规避攻击. 但仅用信息隐藏算法太过单一. 如果是重要的秘密图像, 无法达到军事等领域需要的权限分享, 多方协作要求. 所以结合信息隐藏的秘密共享方案可以解决这个问题.

Shamir[5] 首先提出了基于多项式的秘密共享 (SS) 方案, 通过构造一个 t–1 次多项式来产生 n 个秘密共享从而对秘密信息进行加密. 当收集 t 个或多个共享时, 可以通过拉格朗日插值重构多项式来解密. 受到 Shamir 工作的启发, Thien 等人[6] 把多项式应用在图像领域进行秘密共享. 但在灰度图像中, 每个像素具有 256 个可能值, 并且 256 不是质数, 因此他们采用小于 256 的最大质数 251 作为 p. 所有大于 250 的像素值将被模块 251 截断, 从而导致有损恢复. 另外, 为了消除相邻像素之间的相关性, 他们的方案需要在共享前对原始图像的像素进行置乱, 导致了影响效率的辅助加密.

由于模块化方法仅需 O(k) 运算[7] 即可恢复每个秘密像素, 因此基于中国剩余定理 (CRT) 的图像秘密共享具有计算量小的优点, 这在考虑大量图像像素时非常重要. Asmuth 等人[7] 以及 Mignotte[8] 分别于 1983 年提出了基于 CRT 的 (t, n) 门限秘密共享. 基于 CRT[9,10] 的秘密图像共享方法也有很多, 但是这些研究主要集中在灰度图像上, 而我们日常生活中使用的图像大多是彩色的. 为了具有实用价值, 我们需要将秘密共享方案有效地应用到彩色图像中.

彩色图像秘密共享是通过处理彩色图像, 实现共享的方案. 传统的彩色图像秘密共享方案是分别共享和恢复 R、G 和 B 色平面[11–13]. 闫伟齐等人[14] 首先将 CRT 引入图像秘密共享, 它可能会有少量的信息泄漏和恢复损失. Ulutas 等人[15] 提出了一种基于文献 [7] 方案的 CRT 图像秘密共享, 将像素值分成两部分间隔. 但他们没有给出精确的参数限制, 当随机数太小时, 可能达不到 (t, n) 阈值. Hu 等人[16] 提出了一种基于混沌映射的 CRT 图像秘密共享, 涉及辅助加密. Chuang 等人[17] 对 Ulutas 等人[15] 提出的基于 CRT 的图像秘密共享进行了扩展, 设计了一个 (t, n) 门限图像秘密共享, 只共享最重要的 7 位, 以满足 CRT 的限制. 它们独立地存储和传输秘密图像像素的最低有效位 (LSB), 或者直接丢弃它们. 因此, 它们的缺点是恢复的秘密图像有损且传输成本高. 近期的彩色图像秘密共享方案中, Wu 等人[18] 解决了像素扩展问题, 但恢复的图像是二值秘密图像与彩色影子图像的叠加图像, 对于各种应用场景不具有普适性, 且需要多次重建, 并不能做到直接恢复出无损的秘密图像. Wang 等人[19] 运用的秘密图像是彩色图像. 但恢复的还是彩色秘密图像与彩色影子图像的叠加图像, 且 PSNR 值低. Prasetyo 等人[20] 的彩色影子图像有轮廓, 即影子图像有相关性, 像素并非均匀分布. 且若要无损恢复彩色秘密图像需要多次异或叠加, 复杂度较高. Mhala 等人[21] 恢复的彩色秘密图像是类噪声的, 并非无损恢复. Blesswin 等人[22] 没有显示彩色影子图像, 且 RGB 三通道的灰度影子图像较黑, 说明像素值较低, 模数较低, 并非均匀分布, 无法保证安全性, 不能满足基于 CRT 的秘密共享对于模数的控制.

本文在 CRT 的基础上, 提出了一种 (t, n) 门限的无损高效彩色图像秘密共享信息隐藏算法, 该方案将基于中国剩余定理 (CRT) 的秘密共享与 DCT 信息隐藏技术进行结合, 保障了传输彩色秘密图像的安全性. 在生成端, 利用 DCT 信息隐藏算法将彩色秘密图像通过 CRT 生成的彩色秘密影子图像, 嵌入至用户提供的彩色载体图像中, 并分发. 在恢复端提取出影子图像, 使用 CRT 恢复彩色秘密图像. 实验结果表明, 本文提出的算法能无损恢复秘密图像, 影子图像像素值近似均匀分布, 也不产生像素扩展, 与其它方案相比本文方案具有较高效率.

2 预备知识

2.1 秘密共享

在密码学中, 秘密共享是将秘密信息分成众多子秘密, 形成共享份, 使用达到阈值的子秘密共享份就可以还原该秘密信息. 秘密共享技术具体形式如下:

绝大多数涉密需要保护的通信系统, 它的安全性

皆是由主密钥决定的. 如若出现主密钥被破坏或在传输过程中丢失的情况, 该系统将不再安全.

密码学中提出了一种解决办法: 秘密共享技术. 该技术可以达到减小风险, 分散权力, 容许攻击的目的. 通过将一个主密钥 s 分割成 n 份 $s_1, s_2, \cdots, s_n$, 获取满足门限值 t 的份额通过秘密共享算法即可恢复秘密 s, 而获取不满足门限值 t 的份额时, 无法恢复秘密 s.

2.2 基于中国剩余定理的秘密共享方案

本方案基于中国剩余定理 (CRT), 提出了一个 (t, n) 秘密共享方案, 由秘密 s 通过 CRT 相关公式计算得到 y. 再与 n 个递增的模数 $m_1, m_2, \cdots, m_n$ 通过取模运算得到 (m_i, y_i) 即是共享份, 在实际方案中只需要保存 y_i.

2.2.1 参数选取

参数的选择满足以下要求.

(1) $q > s$.

(2) $\gcd(m_1, m_j) = 1, \forall i, j, i \neq j$.

(3) $\gcd(q, m_i) = 1, i = 1, 2, \cdots, n$.

(4) $N = \prod_{i=1}^{t} m_i > q \prod_{i=1}^{t-1} m_{n-j+1}$.

2.2.2 秘密共享与恢复

参数 A 经由随机选取, 范围是 $0 \leqslant A \leqslant \lfloor N/q \rfloor - 1$. 根据公式 $y = s + Aq$, 求得用于计算共享份的参数 y, 该参数满足 $y < q + Aq = (A+1)q \leqslant \lfloor N/q \rfloor \cdot q \leqslant N$. 由 $y_i \equiv y \bmod m_i (i = 1, 2, \cdots, n)$. (m_i, y_i) 是共享份额, 因为模数公开, 所以将其中的 y_i 作为子共享, 分发给用户. 达到门限值的 t 个用户 $i_1, i_2, \cdots, i_t$ 提供自己的子共享, 根据 $\{(m_{i_j}, y_{i_j}) | i = 1, 2, \cdots, t\}$ 建立方程组.

$$\begin{cases} y_{i_1} \equiv y \bmod m_{i_1} \\ y_{i_2} \equiv y \bmod m_{i_2} \\ \quad \vdots \\ y_{i_t} \equiv y \bmod m_{i_t} \end{cases} \tag{1}$$

可以求得:

$$y \equiv y' \bmod N' \tag{2}$$

其中, $y' \equiv \sum_{j=1}^{t} y_{i_j} M_{i_j} M_{i_j}^{-1}$, $M_i = M/m_i$. 同时 $M_i M_i^{-1} \equiv 1 (\bmod m_i)$. M_i^{-1} 是 M_i 的逆元. 本文使用基于费马小定理的逆元求解法. 只需进行模幂运算就可以快速求解, 即 $M_i^{-1} \equiv M_i^{m_i - 2} (\bmod m_i)$.

最后根据 $N' \equiv \sum_{j=1}^{t} m_{i_j} \geqslant N$, 得到 $y \equiv y' \bmod N'$, 由 $y \bmod q$ 解得秘密 s.

2.2.3 (t, n) 门限确定依据

因为由 t 个成员的共享计算得到的模满足条件 $y < N \leqslant N'$, 所以 $y = y'$ 是唯一的. 再由 $y' - Aq$ 即得秘密 s.

若仅有 t–1 个参与者提供自己的共享份 (m_i, y_i), 则只能求得 $y'' \equiv y \bmod N''$. 其中 $N'' = \prod_{j=1}^{t-1} m_{i_j}$, 得 $N'' < N/q$, $N/N'' > q$. 令 $y = y'' + \alpha N''$, 其中 $0 \leqslant \alpha < y/N'' < N/N''$. 由于 $N/N'' > q$, $(N'', q) = 1$, 当 α 在 $[0, q-1]$ 变化时, $y'' + \alpha N'' < N$, 都是 y 的可能取值. 因此 t–1 个参与者无法确定 y.

2.3 DCT 信息隐藏算法嵌入参数选择

本文方案中待嵌入的数据是彩色秘密共享的 RGB 三通道灰度图与超过 255 像素边界值产生的倍数与余数图像. 将以上的图像进行分块处理, 分为 4 × 4 的像素块. 以 Zigzag 的顺序[23], 如图 1 所示, 在二维 DCT 变换操作后, 进行像素扫描. 从低频到高频, 对 DCT 系数进行排列, 将系数间存在的相关性作为信息隐藏的依据. 本方案在恢复端将无损恢复彩色秘密图像, 非中高频范围的选取会导致无法无损恢复的情况.

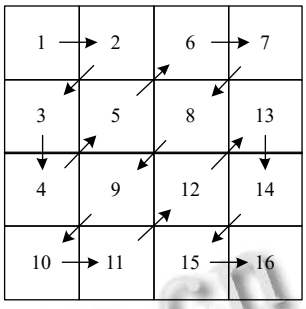


图 1 Zigzag 扫描顺序图

2.4 DCT 信息隐藏算法

本文选择第 12 个系数, 即中高频系数进行嵌入, 所以, 规则如下:

$$\begin{cases} K12_i \geqslant 0, & W_i = 1 \\ K12_i < 0, & W_i = 0 \end{cases} \tag{3}$$

根据 $W_i = 0$ 取值, 有如下两种情况, 其中, k 是水印嵌入强度.

$W_i = 0$ 时, 满足 $K12_i \leqslant -k$:

$$K12_i = \begin{cases} -K12_i, & K12_i > k \\ -k, & k \geqslant K12_i \geqslant -k \\ K12_i, & K12_i < -k \end{cases} \tag{4}$$

$W_i = 1$ 时, 满足 $K12_i \geqslant k$:

$$K12_i = \begin{cases} K12_i, & K12_i > k \\ k, & k \geqslant K12_i \geqslant -k \\ K12_i, & K12_i < -k \end{cases} \tag{5}$$

按照 $K12_i$ 的正负, 将 W_i 提取:

$$W_i=\begin{cases}1, & K12_i\geqslant 0\\ 0, & K12_i<0\end{cases} \tag{6}$$

3 无损 (*t*, *n*) 门限彩色图像秘密共享信息隐藏算法

本文设计的方案, 包括以下几个重要的过程: 首先, 生成彩色共享影子图像, 再运用 DCT 信息隐藏算法生成含彩色影子图像的彩色载体图像. 最后, 不少于门限值 *t* 个用户提取彩色影子图像, 并通过 CRT 恢复彩色秘密图像. 流程图如图 2.

3.1 参数测试

公布互素、递增的模数$A\in[0,\lfloor N/q\rfloor-1]$. 素数 q 满足$A\in[0,\lfloor N/q\rfloor-1]$且与模数互素. 本方案中的秘密图像是 64×64 的彩色秘密图像. 彩色秘密图像中的每个像素值域为 [0, 255], 所以选取$A\in[0,\lfloor N/q\rfloor-1]$满足算法要求, 即大于 255. 随机取$A\in[0,\lfloor N/q\rfloor-1]$. 由公式$y=s+Aq$得 y, 带入公式$y_i\equiv y \bmod m_i$. 只要分别保存 RGB 三通道生成的 5 个 64×64 的y_i. 即 5 份可视灰度秘密共享影子图像, 影子图像大小与原图一致, 不会出现部分多项式秘密共享出现的像素扩展现象. 再将 RGB 三通道分别生成的 5 份可视的灰度秘密共享影子图像通过 *cat* 函数组合成彩色秘密共享影子图像. 由于选取的模数$m_i>255$, 且选取的素数 $q>255$, 所以生成的y_i可能会超过灰度图像能够保存的最大像素值 255. 根据像素 (pixel)、倍数 (multiple) 和余数 (remainder) 的英文首字母列出以下公式: $p=255\times m+r$, 因此本文将超过 255 像素值的倍数与余数分别保存成图像.

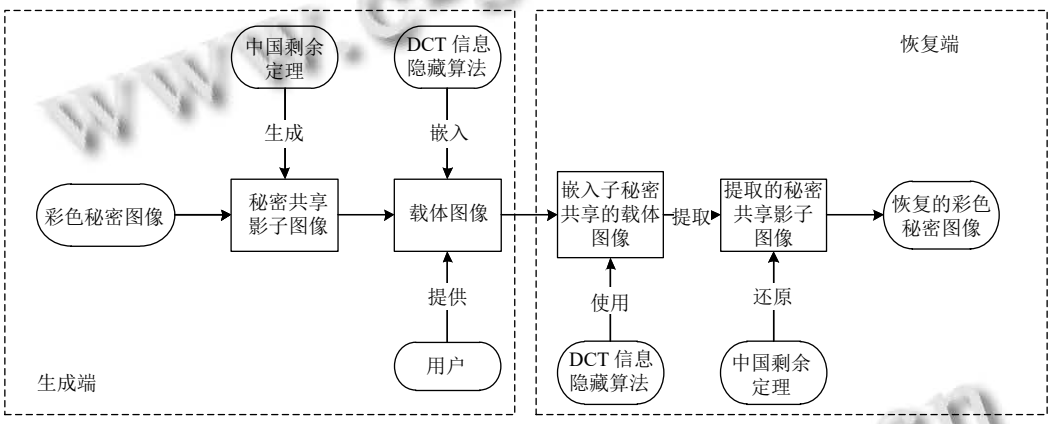


图 2 方案流程图

3.2 生成含彩色影子图像的彩色载体图像

将 n 份彩色秘密共享影子图像中含有的 RGB 三通道灰度秘密共享影子图像与伴随它们存在的 3 份倍数图像、余数图像运用 DCT 信息隐藏算法, 将它们的像素连在一起存成一个大字符串进行 DCT 嵌入. 嵌入 n 张用户提供的载体图像中.

3.3 不少于门限值 *t* 个用户提取彩色影子图像

提取时不需要获得整个字符串, 只需要知道字符串的长度, 便可以实现秘密信息的盲提取. 根据 (*t*, *n*) 门限, 需要进行 t 次提取, 可完整提取出嵌入的字符串, 再将它们分割, 分别存成 RGB 三通道灰度影子图像、倍数图像、余数图像. 并将 RGB 三通道灰度影子图像通过 *cat* 函数还原成 t 份 RGB 彩色影子图像.

3.4 恢复彩色秘密图像

在恢复端读取整型的 RGB 三通道灰度影子图像与伴随它们存在的 3 份倍数和余数图像通过公式 $p=255\times m+r$ 对应相加, 并将 p 存成双精度型的矩阵进行秘密共享恢复操作. t 个用户拿出自己的秘密共享份额, 根据 CRT 建立方程组, 对 RGB 三通道运算, 分别解得 s, 存成矩阵, 并利用 *cat* 函数还原彩色秘密图像. 在本文的实验结果部分将给出参数论证例子及效果展示.

3.5 算法实现创新工作

算法实现创新工作在于: 解决了基于 CRT 的秘密共享算法在彩色图像应用实现上出现的像素溢出问题, 将超过 255 像素值的共享数据根据上文分别存成倍数图像与余数图像, 并开创性的结合信息隐藏算法, 将共享影子图像、倍数图像、余数图像全都嵌入到彩色图像中, 从而使该算法全部在彩色图像上进行操作, 实现了彩色秘密图像的无损恢复.

4 实验结果及分析

为了更好的展示基于 CRT 的彩色高效无损门限秘密图像信息隐藏算法, 对基于 (3, 5) 门限的方案进行验证. 最后, 综合学界相关论文的诸多参数与其他方案进行比较.

4.1 参数测试

本方案选取互素模数$m_1 = 283$, $m_2 = 293$, $m_3 = 307$, $m_4 = 311$, $m_5 = 313$. 素数$q = 257$.

$$N = \prod_1^3 m_i = 25456133 > q \times m_4 \times m_5 = 257 \times 311 \times 313 = 25017151 \tag{7}$$

$A \in \left[0, \left\lfloor N/q \right\rfloor - 1\right]$, 代入即 [0, 99050] 内, 取 A=22548. 彩色秘密图像的第 64 × 64 个像素中红色通道的像素值作为证明对象. 选取红色通道的最后一个像素 255 为秘密. 由:

$$y = s + Aq = 255 + 22548 \times 257 = 361467 \tag{8}$$

代入公式$y_i \equiv y \bmod m_i$, 得出y_i. 如式 (9) 所示:

$$\begin{cases} y_1 \equiv y \bmod m_1 \equiv 5795051 \bmod 283 \equiv 100 \\ y_2 \equiv y \bmod m_2 \equiv 5795051 \bmod 293 \equiv 137 \\ y_3 \equiv y \bmod m_3 \equiv 5795051 \bmod 307 \equiv 159 \\ y_4 \equiv y \bmod m_4 \equiv 5795051 \bmod 311 \equiv 228 \\ y_5 \equiv y \bmod m_5 \equiv 5795051 \bmod 313 \equiv 209 \end{cases} \tag{9}$$

遍历彩色图片红绿蓝三通道所有像素, 计算得到y_i. 在恢复端, 取 (283, 100)、(307, 159)、(311, 228). 参数$M = m_1 \times m_3 \times m_4 = 27019991$. 计算$M_i = M/m_i$. 还需计算$m_i^{-1}$, m_i^{-1}是m_i的逆元, 公式表示为:

$$M_i M_i^{-1} \equiv 1 \ (\bmod m_i) \tag{10}$$

综合求得参数:

$$y \equiv \left(\sum_1^t y_i M_i M_i^{-1}\right) \bmod M \equiv (100 \times 95477 \times 275 + 159 \times 88013 \times 291 + 228 \times 86881 \times 25) \bmod 27019991 \equiv 5795091 \tag{11}$$

最后一步得:

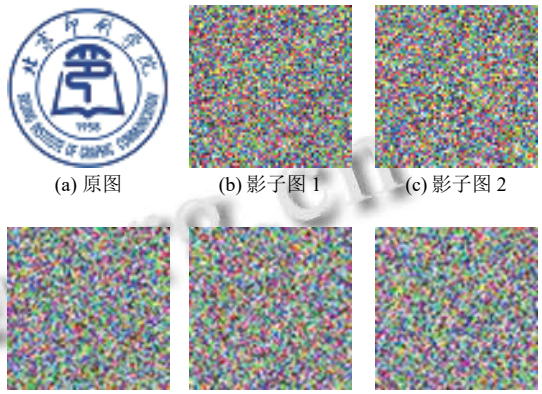
$$s \equiv y \bmod q \equiv 5795091 \bmod 257 \equiv 255 \tag{12}$$

证明彩色图像红色信道的秘密共享生成与恢复过程正确. 恢复彩色秘密图像需要遍历计算红色信道的每一个像素值. 同理计算绿色与蓝色信道的每一个像素值. 最后用 *cat* 函数生成彩色图片即可得到子秘密彩色图像.

4.2 (3, 5) 门限无损高效彩色图像秘密共享信息隐藏方案实验结果

首先运行算法程序, 由彩色秘密图像共享生成彩色秘密共享影子图像, 如图 3 所示.

彩色秘密共享影子图像是类噪声的无意义图像, 无法获得任何秘密信息. 下文将讨论影子图像的无相关性并用直方图进行分析.



(a) 原图 (b) 影子图 1 (c) 影子图 2

(d) 影子图 3 (e) 影子图 4 (f) 影子图 5

图 3 原始图像与生成的秘密影子图像

通过 DCT 信息隐藏算法, 将彩色秘密共享图像中的 RGB 三通道灰度图与其相应的余数图像嵌到用户提供的彩色载体图像中, 本实验使 2048×2048 的 Lena 图与其直方图展示效果, 如图 4 所示.

(a) 原图 (b) 嵌入载体图 1 (c) 嵌入载体图 2

(d) 原图直方图 (e) 载体 1 直方图 (f) 载体 2 直方图

(g) 嵌入载体图 3 (h) 嵌入载体图 4 (i) 嵌入载体图 5

(j) 载体 3 直方图 (k) 载体 4 直方图 (l) 载体 5 直方图

图 4 载体图像与其对应的直方图

通过图 4 中直方图可以看出嵌入信息的载体图像在像素值分布上与原图基本一致, 从而认证从视觉角度看, 嵌入秘密共享影子图像与余数图像的载体图像与原载体图像没有区别. 同时当 PSNR 值大于 33 时[24], 肉眼无法识别不同之处并获取秘密图像信息. 由表 1 体现本方案中信息隐藏的效果优于其他方案, 说明嵌入的秘密信息安全. 峰值信噪比, 即 PSNR 值越大, 嵌入的秘密信息越不容易被识别, 隐藏性越好. 平均结构相似性, 即 MSSIM 值越接近 1, 嵌入秘密的载体图像与原载体图像越相似, 隐藏程度越好. 见表 1.

表 1 Lena 图片上其他嵌入秘密共享方案 PSNR、MSSIM 值与本方案对比

参数	文献[25]	文献[26]	本文
PSNR	55.46	60.44	61.22
MSSIM	0.999 3	0.999 9	0.999 9

从嵌入秘密的载体图像中提取出 5 份彩色秘密共享影子图像的 RGB 三通道图片与之相应的余数图片, 并组合存成双精度浮点型矩阵, 再利用 CRT 进行还原. 最后无损恢复原彩色秘密图像.

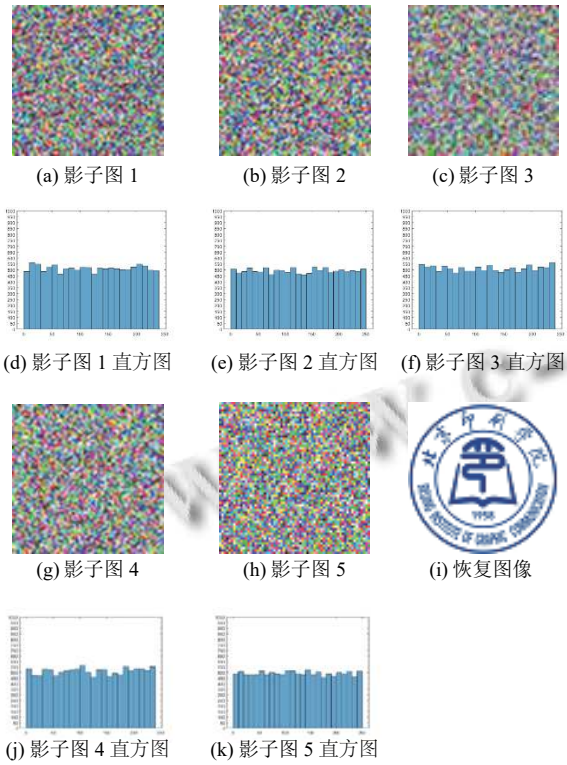


图 5 提取的秘密共享图像与还原的秘密图像及其直方图

通过比较图 5 中提取的秘密共享影子图像的直方图可以看出像素值均匀分布, 证明影子图像是类噪声的, 没有轮廓, 无法获得任何信息, 安全性好.

将嵌入的图像像素首尾相连存为一个字符串, 再转成二进制, 通过 BER (误比特率) 函数, 比较原图像与回复后图像的比特流, 若值为 0, 说明无误比特, 即证明本方案无损恢复秘密图像. 见表 2.

表 2 恢复前后图像 BER 值

原图片	恢复的图片	BER值
彩色秘密图	恢复后的彩色秘密图	0
彩色影子图1	提取后的彩色影子图1	0
彩色影子图2	提取后的彩色影子图2	0
彩色影子图3	提取后的彩色影子图3	0
彩色影子图4	提取后的彩色影子图4	0
彩色影子图5	提取后的彩色影子图5	0

如表 2 所示, 通过 BER 函数比较恢复前后秘密图像完全一致, 本文方案无损的恢复了秘密图像.

4.3 与相关成果的对比分析

本方案在同等 512×512 的图像下做多次实验, 取平均值, 并与现今一些方案进行了效率对比, 体现出本方案效率的提升.

从表 3 中可以看出本方案比文献 [27] 的传统算法效率高.

表 3 秘密共享生成与恢复总时 (s)

门限值	文献[27]	本文
(2, 3)	8.45	7.75
(3, 4)	14.12	13.65
(4, 5)	24.10	21.26

同时由图 6 中可以体现出基于中国剩余定理的秘密共享方案在像素值越大, 门限要求越高的大计算量条件下优于基于多项式的秘密共享算法.

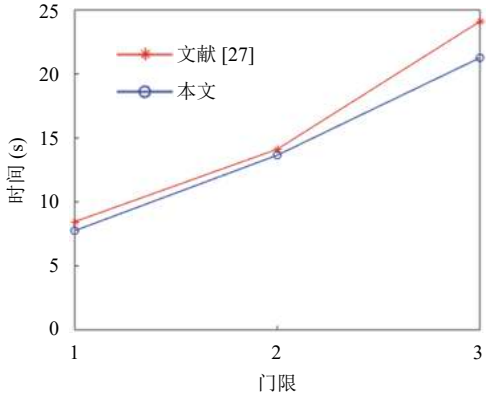


图 6 与文献 [27] 计算速度对比折线图

表 4 与其他方案的重要参数对比

方案	辅助加密	无损恢复	(t, n) 门限	高效
文献[15]	不需要	可以 (有条件)	满足 (有条件)	不满足
文献[16]	需要	可以	满足	不满足
文献[17]	不需要	不可以	满足	不满足
文献[28]	需要	可以	满足	不满足
文献[29]	不需要	可以	满足	不满足
本文	不需要	可以	满足	满足

由表 4 可以看出与其他方案对比, 本文提出的方案满足以下条件: 不需要辅助加密, 可以无损恢复秘密图像, 具有 (t, n) 门限以及高效性.

5 结束语

本文利用基于中国剩余定理 (CRT) 的门限秘密共享技术, 设计了一个基于 CRT 的无损高效门限彩色图像秘密共享信息隐藏算法. 以 (3, 5) 门限彩色图像秘密共享信息隐藏算法为例论证. 实验结果表明本文设计的秘密共享信息隐藏算法在全彩色图像操作环境上, 能无损恢复秘密图像, 从而达到在系统中安全传输秘密图像, 实现权力共享的机制. 诸多指标优于学界其他方案. 下一步将探究更多的秘密共享算法并进行改进, 在彩色图像上进行实验, 进一步提升性能.

参考文献

1 Li L, Abd El-Latif AA, Shi ZF, *et al*. A new loss-tolerant image encryption scheme based on secret sharing and two chaotic systems. Research Journal of Applied Sciences, Engineering and Technology, 2012, 4(8): 877–883.

2 Abd El-Latif AA, Li L, Wang N, *et al*. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Processing, 2013, 93(11): 2986–3000. [doi: 10.1016/j.sigpro.2013.03.031]

3 Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. International Journal of Theoretical Physics, 2016, 55(1): 107–123. [doi: 10.1007/s10773-015-2640-0]

4 Yeung Y, Lu W, Xue YJ, *et al*. Secure binary image steganography based on LTP distortion minimization. Multimedia Tools and Applications, 2019, 78(17): 25079–25100. [doi: 10.1007/s11042-019-7731-0]

5 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612–613. [doi: 10.1145/359168.359176]

6 Thien CC, Lin JC. Secret image sharing. Computers & Graphics, 2002, 26(5): 765–770.

7 Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Transactions on Information Theory, 1983, 29(2): 208–210. [doi: 10.1109/TIT.1983.1056651]

8 Mignotte M. How to share a secret. Proceedings of the Workshop on Cryptography. Burg Feuerstein: Springer, 1983. 371–375.

9 Tan LD, Lu YL, Yan XH, *et al*. Weighted secret image sharing for a (k, n) threshold based on the Chinese remainder theorem. IEEE Access, 2019, 7: 59278–59286. [doi: 10.1109/ACCESS.2019.2914515]

10 Li LL, Lu YL, Yan XH, *et al*. Lossless (k, n)-threshold image secret sharing based on the Chinese remainder theorem without auxiliary encryption. IEEE Access, 2019, 7: 75113–75121. [doi: 10.1109/ACCESS.2019.2921612]

11 Lin CC, Tsai WH. Secret image sharing with steganography and authentication. Journal of Systems and Software, 2004, 73(3): 405–414. [doi: 10.1016/S0164-1212(03)00239-5]

12 Chang CC, Lin CC, Lin CH, *et al*. A novel secret image sharing scheme in color images using small shadow images. Information Sciences, 2008, 178(11): 2433–2447. [doi: 10.1016/j.ins.2007.12.016]

13 Yan XH, Liu X, Yang CN. An enhanced threshold visual secret sharing based on random grids. Journal of Real-Time Image Processing, 2018, 14(1): 61–73. [doi: 10.1007/s11554-015-0540-4]

14 闫伟齐, 丁玮, 齐东旭. 基于中国剩余定理的图像分存方法. 北方工业大学学报, 2000, 12(1): 6–9.

15 Ulutas M, Nabiyev VV, Ulutas G. A new secret image sharing technique based on Asmuth Bloom's scheme. Proceedings of the International Conference on Application of Information and Communication Technologies (AICT). Baku: IEEE, 2009. 1–5.

16 Hu CQ, Liao XF, Xiao D. Secret image sharing based on chaotic map and Chinese remainder theorem. International Journal of Wavelets, Multiresolution and Information Processing, 2012, 10(3): 1250023. [doi: 10.1142/S0219691312500233]

17 Chuang TW, Chen CC, Chien B. Image sharing and recovering based on Chinese remainder theorem. Proceedings of the International Symposium on Computer, Consumer and Control. Xi'an: IEEE, 2016. 817–820.

18 Wu XT, Yang CN. Probabilistic color visual cryptography schemes for black and white secret images. Journal of Visual Communication and Image Representation, 2020, 70: 102793. [doi: 10.1016/j.jvcir.2020.102793]

19 Wang L, Yan B, Yang HM, *et al*. Flip extended visual

cryptography for gray-scale and color cover images. Symmetry, 2021, 13(1): 65.

20 Prasetyo H, Hsia CH. Lossless progressive secret sharing for grayscale and color images. Multimedia Tools and Applications, 2019, 78(17): 24837–24862. [doi: 10.1007/s11042-019-7710-5]

21 Mhala NC, Pais AR. Contrast enhancement of Progressive Visual Secret Sharing (PVSS) scheme for gray-scale and color images using super-resolution. Signal Processing, 2019, 162: 253–267. [doi: 10.1016/j.sigpro.2019.04.023]

22 Blesswin AJ, Raj C, Sukumaran R, *et al*. Enhanced semantic visual secret sharing scheme for the secure image communication. Multimedia Tools and Applications, 2020, 79(23–24): 17057–17079.

23 Deng YN, Kenney C, Moore MS, *et al*. Peer group filtering and perceptual color image quantization. IEEE International Symposium on Circuits and Systems. Orlando: IEEE, 1999. 21–24.

24 唐明伟. 图像信息隐藏与隐藏分析算法研究 [博士学位论文]. 成都: 电子科技大学, 2012.

25 Yuan HD. Secret sharing with multi-cover adaptive steganography. Information Sciences, 2014, 254: 197–212. [doi: 10.1016/j.ins.2013.08.012]

26 Singh P, Raman B. Reversible data hiding based on Shamir's secret sharing for color images over cloud. Information Sciences, 2018, 422: 77–97. [doi: 10.1016/j.ins.2017.08.077]

27 Gong QH, Wang YJ, Yan XH, *et al*. Efficient and lossless polynomial-based secret image sharing for color images. IEEE Access, 2019, 7: 113216–113222. [doi: 10.1109/ACCESS.2019.2934999]

28 Shyu SJ, Chen YR. Threshold secret image sharing by Chinese remainder theorem. Proceedings of the IEEE Asia-Pacific Services Computing Conference. Yilan: IEEE, 2008. 1332–1337.

29 Yan XH, Lu YL, Liu LT, *et al*. Chinese remainder theorem-based two-in-one image secret sharing with three decoding options. Digital Signal Processing, 2018, 82: 80–90. [doi: 10.1016/j.dsp.2018.07.015]