

灰度可视秘密共享方案分析与设计

刘健^{1,2}, 张益^{1,2}, 刘玉岭³, 胡浩⁴

- (1. 信息产业信息安全测评中心, 北京 100083;
2. 中国电子科技集团公司第十五研究所, 北京 100083;
3. 中国科学院信息工程研究所, 北京 100190;
4. 信息工程大学, 河南 郑州 450001)

摘要: 针对现有灰度可视秘密共享 (GVSS, gray visual secret sharing) 将原始图像转化为黑白二值图像进行处理时产生像素信息损失的问题, 提出了一种基于灰度叠加的 GVSS, 对于每一个灰度级像素, 分别设计相应的加密矩阵, 生成灰度共享图像, 在此基础上设计了 $(2, 2)$ 、 $(2, n)$ 、 (n, n) 方案。与现有方案相比, 所提方案有效降低了像素扩展度并实现了灰度密图的无损恢复。

关键词: 可视秘密共享; 灰度图像; 灰度叠加; 无损解密

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020049

Analysis and design of visual secret sharing scheme for gray image

LIU Jian^{1,2}, ZHANG Yi^{1,2}, LIU Yuling³, HU Hao⁴

1. Information Technology & Security Test and Evaluation Center, Beijing 100083, China
2. The 15th Research Institute of China Electronics Technology Group Corporation, Beijing 100083, China
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, China
4. Information Engineering University, Zhengzhou 450001, China

Abstract: Existing gray visual secret sharing (GVSS) convert the original image into black-white binary image for processing, which causes the pixel information loss problem. For this purpose, a kind of GVSS based on gray superposition was proposed. For each gray-scale pixel, the corresponding encoding matrix was designed to generate gray share image. On this basis, the schemes for $(2, 2)$, $(2, n)$, (n, n) threshold structures were designed. Compared with the existing schemes, the proposed scheme effectively reduces pixel expansion and achieves the perfect reconstruction of gray secret images.

Key words: visual secret sharing, gray image shares, grayscale superposition, lossless decoding

收稿日期: 2020-02-28; 修回日期: 2020-06-05

通信作者: 刘健, liuj@itsec.org.cn

基金项目: 国家重点研发计划基金 (2016YFF0204003)

Foundation Item: The National Key R&D Program of China (2016YFF0204003)

论文引用格式: 刘健, 张益, 刘玉岭, 等. 灰度可视秘密共享方案分析与设计[J]. 网络与信息安全学报, 2020, 6(4): 140-147.
LIU J, ZHANG Y, LIU Y L, et al. Analysis and design of visual secret sharing scheme for gray image[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 140-147.

1 引言

可视秘密共享 (VSS, visual secret sharing) 作为一种新兴图像秘密分享技术, 通过将秘密图像加密成若干杂乱无章的共享份, 解密时利用人眼直接识别秘密信息, 引起了学者们的广泛关注^[1-7]。

传统 VSS 方案只能处理黑白二值图像^[8], 限制了 VSS 的应用范围^[9], 近年来, 有学者提出灰度可视秘密共享 (GVSS, gray visual secret sharing)^[10], 目前该方向研究处于起步阶段, 按设计方法, 主要分为半色调 GVSS 和矩阵拼接式 GVSS 两类。

对于半色调 GVSS, Lin 等^[10]首先提出运用半色调技术来实现秘密共享, 通过误差扩散方法将原秘密图像转化为尺寸相同的二值图像, 恢复图像不会产生额外的像素扩展度, 简化了设计思路, 继承了可视秘密共享恢复简单的特点, 并有效降低了像素扩展。然而, 由于使用了半色调技术, 在半色调处理过程中会产生信息熵损失, 秘密分享生成的共享份是黑白二值图像, 最终恢复的也是黑白二值图像, 产生像素色度信息损失。随后, 有学者提出矩阵拼接式 GVSS 方案^[11], 核心思想是将黑白二值 VSS 方案的加密矩阵拼接成一个新的加密矩阵作为相应灰度级像素的加密矩阵, 并为每一级灰度级设计了相应的加密矩阵, 分享过程中根据灰度级的不同来加密对应像素点, 实现秘密图像的完全恢复。Blundo 等^[11]首次提出 GVSS, 并给出加密矩阵的构造方法; MacPherson^[12]在 Blundo 等的基础上提出了 $L=4$ 级灰度下 (n, n) 门限的最优加密矩阵构造方法, 并证明了矩阵拼接式方案最优参数界限, 像素扩展度 $m=3 \cdot 2^{n-1}$, 相对差 $\alpha = \frac{1}{m}$ 。此类方法的优点是保留了秘密图像的全部信息, 可以无损恢复秘密图像; 不足是像素扩展度太大, 对于同一存取结构, 像素扩展度是二值方案的 $L-1$ 倍, 产生较大的系统开销。为了将灰度图像拓展到彩色图像, 近年来, De Prisco 和 De Santis 提出了系列 (k, n) 彩色黑白可视密码方案 (CBW-VSS), 该方案采用共享份图像中的彩色像素点来共享黑白秘密图

像, k 个或更多的参与者可以通过叠加共享份图像来重建秘密图像, Yang 等^[15]将现有 CBW-VSS 扩展到 CBW-EVSS, 并理论证明了方案成立的安全性、相对差和伪装图像条件。为了克服恢复图像扩展大的问题, 同时提供灵活的共享策略, Wu 等^[16]定义了彩色像素的异或运算, 提出了一种基于通用访问结构的随机栅格方案 (RG-CBW-VSS, random grids based CBW-VSS), 首次将随机栅格的概念引入彩色像素域, 实现了复杂应用场景下的共享策略, 理论和实验证明了方法的安全性和对比条件, 并给出了相对差的计算方法。Dutta 等^[17]提出了一种实现基于强访问存取结构的彩色方案, 给出了在同一颜色模型中分享彩色图像的通用构造方法, 优化了相对差, 丰富了现有方案的构造思路, 但该方法以牺牲像素扩展度为代价, 存在共享份开销大的问题。在实际应用方面, Das 等^[18]提出了一种基于彩色 VSS 和神经网络的安全图像传输方案。为了增强共享单车服务安全认证, Feng 等^[19]提出了一种新的基于彩色 VSS 和 QR 码的身份认证方案, 将基于纠错机制的彩色 QR 码与 VSS 相结合进行开锁认证。由于彩色图像实际上是 RGB3 个不同通道的灰色图像的叠加, 研究灰度图像的可视秘密共享方法是研究彩色 VSS 的基础, 因此本文重点围绕灰色图像展开研究。

本文主要贡献: 深入分析了灰度图像与加密矩阵构造之间的关系; 提出一种基于灰度叠加的 GVSS 方案; 在实现解密图像无损恢复的前提下, 显著降低了像素扩展度。

2 基本概念

VSS 解密依据人眼视觉系统特性, 即人类的视觉系统在观察物体时, 利用像素块的平均色度效果来区分不同区域。

定义 1^[3] C_0 和 C_1 是两个 $n \times m$ 的布尔矩阵集合, 设参与者数目为 n , 恢复门限值 k , 若从 C_0 和 C_1 中任意选出两个 $n \times m$ 加密矩阵 S_0 和 S_1 满足下列两个条件, 则称 (k, n) -VSS 是一个可视秘密共享方案。

1) 对 $\forall S_1 \in C_1$, 设 $i_1, i_2, \dots, i_k$ 为 S_1 中的任意 k 行, $V = i_1 + i_2 + \dots + i_k$, “+” 表示或运算, 则 $H(V) \geq d$ (其中 $H(V)$ 表示向量 V 的汉明重量),

对 $\forall S_0 \in C_0$, 则有 $H(V) \leq d - \alpha \cdot m$ 。

2) 对于任意子集 $\{i_1, i_2, \dots, i_q\} \subseteq \{1, 2, \dots, n\}$ ($q < k$), 在集合 $C_t (t \in \{0, 1\})$ 中任取 $i_1, i_2, \dots, i_q$ 行, 得到以 $q \times m$ 矩阵为元素的集合 D_t 。其中, D_0, D_1 包含同一矩阵元素的概率相同, 即它们是不可区分的。

在定义 1 中, 条件 1) 和条件 2) 分别表示方案的对比性和安全性条件, 参数如下。

1) 门限值 d , 解密后图像中像素被人眼解析为黑色与白色的灰度临界值, 当解密后图像中像素的灰度值大于或等于 d 时该像素被人眼解析为黑色, 相应地, 当像素的灰度值小于 $d - \alpha \cdot m$ 时被解析为白色。

2) 像素扩展度 m , 一个像素分享后得到的像素块包含子像素的个数, 即尺寸失真的倍数。

3) 相对差 α , 表征解密后图像的黑白差异, 等于恢复图像中代表黑像素的向量汉明重量最小值 l 与代表白像素的向量汉明重量最大值 h 之差与像素扩展度 m 之比

定义 2 (k, n) -GVSS 的参与者集合为 $P = \{1, 2, \dots, n\}$, 生成的共享份为 $A_0, A_1, \dots, A_{n-1}$, 当且仅当共享份 $A_0, A_1, \dots, A_{n-1}$ 满足以下条件时成立。

1) 任意 k 张共享份 $A_0, A_1, \dots, A_{k-1}$ 通过灰度图像叠加原理可以恢复秘密图像, 即 $S_k' = A_0 A_1 \dots A_{k-1}$, $T(S_k'[S_k(g_i)]) - T(S_k'[S_k(g_j)]) > 0$, 其中, “ $\cdot$ ” 表示灰度叠加运算。

2) 从任意 $k-1$ 张共享份中无法得到秘密图像的信息, 即 $S_{k-1}' = A_0 A_1 \dots A_{k-2}$, $T(S_{k-1}'[S_k(g_i)]) - T(S_{k-1}'[S_k(g_j)]) = 0$ 。

关于定义 2 的几点补充说明。

(1) 条件 1) 是对比性条件, 当 k 个共享份进行叠加时, 利用灰度叠加原理可以解密秘密信息。条件 2) 是安全性条件, 表示小于 k 个共享份叠加时, 叠加图像中每个像素点显示各灰度级的概率相同, 人眼无法区分。

(2) 像素扩展度 m : 原始图像中的单个像素点在叠加恢复图像中对应一个包含 m 个像素点的像素块, 反映了原始图像在外形、比例和面积上失真情况, m 越大, 表示失真越严重, 存储和传输开销越大, $m=1$ 是一种最优情况, 表示恢复图

像不存在像素扩展。

(3) 相对差 α 的计算公式如下。

$$\alpha = \frac{T(S_k'[S_k(g_i)]) - T(S_k'[S_k(g_j)])}{m}$$

解密后图像黑白差异的表征量, 表示原始图像中不同灰度值像素在恢复图像中的灰度值的差值与像素扩展度 m 的比值, $\alpha \in [0, 1]$, 当 $\alpha=0$ 时代表黑白像素的灰度值相等, 秘密图像完全不能辨识, 是最差情况; 当 $\alpha=1$ 时代表秘密图像中黑白像素能够完全恢复; 当 $m=1, \alpha=1$ 时, 是最理想的情况, 秘密图像实现了无损恢复。

3 基于灰度叠加的 GVSS 方案

本节首先研究了灰度叠加原理, 然后在此基础上依次设计了 $(2, 2)$ 、 $(2, n)$ 和 (n, n) 方案。通过新设计加密矩阵, 实现灰度图像的无损叠加恢复, 克服半色调产生的信息损失问题。

3.1 灰度叠加原理

灰度图像叠加原理是指不同灰度值的像素叠加会生成一个颜色更深的灰度像素, 符合人眼视觉特性。设灰度级 L , 两个叠加的像素灰度值分别为 g_1 与 g_2 , 叠加后像素值为 $\text{add}(g_1, g_2) = L - \text{int} \frac{(L - g_1) \cdot (L - g_2)}{L}$, 其中, $\text{int}()$ 表示向下取整函数。例如, $L=16$ 时, $\text{add}(3, 4) = 16 - \text{int}((16-3) \cdot \frac{16-4}{16}) = 16 - \text{int}(9.75) = 16 - 9 = 7$ 。和黑白二值像素叠加类似, 这种叠加规则是依赖人眼成像原理, 不需要额外加入复杂运算, 满足恢复简单的特性。

3.2 $(2, 2)$ -GVSS

若秘密图像包含的灰度级为 L , 由于不同的灰度级对应的加密矩阵不同, 秘密图像像素取值集合为 $\{0, 1, 2, \dots, L-1\}$, 共享份的像素取值集合为秘密图像像素取值集合的子集, 为减小像素扩展度, 加密矩阵中可以选择几个不同的灰度级来显示整个秘密图像的灰度级, 需要满足以下 2 个条件。

1) 共享份像素取值集合中灰度级经过灰度叠加规则运算可以覆盖整个秘密图像的取值集合。

2) 共享份像素取值集合应当尽可能小。

其中, 条件 1) 是实现秘密图像无损恢复的关

键; 条件 2) 有利于控制加密矩阵规模。方案核心是构造加密矩阵, 本文采用一列有效、其余列抵消的构造思路。即灰度叠加后, 只有其中一列显示出原秘密图像真正的灰度值, 其余列被遮盖元素抵消掉 (GVSS 中黑像素被当作遮盖元素, 因为任何灰度级与黑像素叠加会得到黑像素)。在此基础上为每一个灰度级设计一个加密矩阵, 以 (2, 2)-GVSS 为例, 加密矩阵需满足的安全性和有效性条件如下。

1) 安全性条件: 不同灰度级加密矩阵的任意行向量中包含不同灰度值元素的个数相同。

2) 对比性条件: 加密矩阵中的两行叠加后能够显示原始秘密图像对应的灰度值。

下面以 16 级灰度为例, 给出 (2, 2)-GVSS 的加密矩阵构造流程。

算法 1 (2, 2)-GVSS 的加密矩阵构造算法

输入 灰度级 $L=16$

输出 加密矩阵 $S_0, S_1, \dots, S_{15}$

Step 1 初始化秘密图像像素取值集合 $\{0, 1, 2, \dots, 15\}$ 。

Step 2 生成共享份像素取值集合 $\{0, 1, 3, 5, 7, 12, 15\}$ 。

Step 3 利用共享份像素取值集合中的元素, 按照一列有效、其余列抵消的构造思路, 为每一个灰度级设计相应的加密矩阵。

Step 4 输出加密矩阵。

$$S_0 = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 0 & 15 & 15 & 15 & 15 & 15 & 1 & 3 & 5 & 7 & 12 \end{pmatrix}$$

$$S_1 = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 1 & 15 & 15 & 15 & 15 & 15 & 0 & 3 & 5 & 7 & 12 \end{pmatrix}$$

$$S_2 = \begin{pmatrix} 1 & 0 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 1 & 15 & 15 & 15 & 15 & 15 & 0 & 3 & 5 & 7 & 12 \end{pmatrix}$$

$$S_3 = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 3 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 5 & 7 & 12 \end{pmatrix}$$

$$S_4 = \begin{pmatrix} 1 & 0 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 3 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 5 & 7 & 12 \end{pmatrix}$$

$$S_5 = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 5 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 7 & 12 \end{pmatrix}$$

$$S_6 = \begin{pmatrix} 3 & 0 & 1 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 3 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 5 & 7 & 12 \end{pmatrix}$$

$$S_7 = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 7 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 12 \end{pmatrix}$$

$$S_8 = \begin{pmatrix} 1 & 0 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 7 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 12 \end{pmatrix}$$

$$S_9 = \begin{pmatrix} 5 & 0 & 1 & 3 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 5 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 7 & 12 \end{pmatrix}$$

$$S_{10} = \begin{pmatrix} 5 & 0 & 1 & 3 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 7 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 12 \end{pmatrix}$$

$$S_{11} = \begin{pmatrix} 7 & 0 & 1 & 3 & 5 & 12 & 15 & 15 & 15 & 15 & 15 \\ 7 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 12 \end{pmatrix}$$

$$S_{12} = \begin{pmatrix} 0 & 1 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 12 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 7 \end{pmatrix}$$

$$S_{13} = \begin{pmatrix} 1 & 0 & 3 & 5 & 7 & 12 & 15 & 15 & 15 & 15 & 15 \\ 12 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 7 \end{pmatrix}$$

$$S_{14} = \begin{pmatrix} 7 & 0 & 1 & 3 & 5 & 12 & 15 & 15 & 15 & 15 & 15 \\ 12 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 7 \end{pmatrix}$$

$$S_{15} = \begin{pmatrix} 12 & 0 & 1 & 3 & 5 & 7 & 15 & 15 & 15 & 15 & 15 \\ 12 & 15 & 15 & 15 & 15 & 15 & 0 & 1 & 3 & 5 & 7 \end{pmatrix}$$

在上述算法中, 加密矩阵构造采取其余列抵消的构造思路, 16 个加密矩阵 $S_0, S_1, \dots, S_{15}$ 的大小都是 2×11 , 且任意矩阵 S_i 的任意行向量包含的 11 个元素完全相同, 因此单个共享份不会泄露秘密图像的任何信息, 满足安全性条件; 当两个行向量灰度叠加运算时, 对于原始灰度级 i 的像素加密矩阵 S_i , 第 1 列对应位置两个元素叠加值为 i , 其余列对应位置元素叠加的结果不小于 15, 因此, 在恢复图像时, 扩展像素块中仅第一个子像素的颜色呈现原始图像的颜色, 其余子像素点颜色全黑, 作用相互抵消, 满足秘密恢复的有效性条件。由于篇幅限制, 本文不再列举 256 级灰度图像的加密矩阵, 构造方法类似。

3.3 (2, n)-GVSS

(2, n)-GVSS 构造以 (2, 2)-GVSS 为基础, 主要设计思想为: 采用一列有效、其余列抵消的构造思路, 利用 (2, n)-VSS 的加密矩阵, 将 (2, 2)-GVSS 中的行替换 (2, n)-VSS 加密矩阵中的 0 和 1, 构造本文方案加密矩阵。

具体步骤如下, 首先生成 (2, n)-VSS 的黑像素加密矩阵 ϕ_i , 如 Step 1 所示; 每个灰度级的加密矩阵构造都是以 ϕ_i 为基础的。在构造灰度级为

g_i 的加密矩阵时, 用 $(2, n)$ -VSS 中相应的 g_i 加密矩阵中的一行替换 φ_1 中的“1”, 用另一行替换 φ_1 中的“0”, 对应 Step 3, 生成的新矩阵即为 $(2, n)$ -GVSS 中灰度级 g_i 的加密矩阵。

在对不同灰度级图像进行加密时, 需要为每个灰度级像素分别构造一个加密矩阵, $(2, n)$ -GVSS 加密矩阵生成流程如下, 对于不同灰度级图像分享, 若算法输入的灰度级 L 不同, 则输出的加密矩阵不同, 算法具有通用性。

例如, $(2, 3)$ 方案基矩阵生成流程如下。

Step1 生成黑白二值 $(2, 3)$ -VSS 的黑像素加

$$\text{密矩阵 } \varphi_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

Step2 生成 $(2, 2)$ -GVSS 的加密矩阵 $\{S_0, S_1, \dots, S_{15}\}$, 记 S_0 中第一行为 v_0^1 , 第二行为 v_0^2 , 其余加密矩阵依次类推;

Step3 输出 $(2, 3)$ -GVSS 加密矩阵。

$$S_0^{(2,3)} = \begin{pmatrix} v_0^1 & v_0^2 & v_0^2 \\ v_0^2 & v_0^1 & v_0^2 \\ v_0^2 & v_0^2 & v_0^1 \end{pmatrix}$$

$$S_1^{(2,3)} = \begin{pmatrix} v_1^1 & v_1^2 & v_1^2 \\ v_1^2 & v_1^1 & v_1^2 \\ v_1^2 & v_1^2 & v_1^1 \end{pmatrix}$$

...

$$S_{15}^{(2,3)} = \begin{pmatrix} v_{15}^1 & v_{15}^2 & v_{15}^2 \\ v_{15}^2 & v_{15}^1 & v_{15}^2 \\ v_{15}^2 & v_{15}^2 & v_{15}^1 \end{pmatrix}$$

3.4 (n, n) -GVSS

(n, n) 方案设计的约束条件更加复杂, 要求 n 张共享份叠加时能恢复出秘密图像, 但任意少于 n 张共享份进行叠加时不会泄露秘密信息。加密矩阵构造仍采用“一行有效、其余列抵消”的设计原则。不同之处是设计加密矩阵时, 重新选择共享份的取值集合, 因为参与叠加的为 n 列。分别考虑任意 2 行叠加、3 行叠加、 $n-1$ 行叠加的情况, 使叠加结果不随加密矩阵的不同而发生变化, 通

过在矩阵中加入多余列, 使可能的结果出现在禁止集合的叠加结果中, 并使禁止集合的叠加结果完全一致, 从而任意 k 个共享份无法恢复秘密信息。

4 方案有效性分析

本节从相对差和安全性两个方面对方案有效性进行分析。

4.1 相对差分析

在 3.2 节 $(2, 2)$ -GVSS 加密矩阵中, 由于采用了“一行有效, 其余列抵消”的思路, 叠加后其中第一列的叠加结果为秘密图像真正的灰度值, 其余列被遮盖像素抵消, 相对差 $\alpha = \frac{T(S'_k[S_k(g_i)]) - T(S'_k[S_k(g_j)])}{m}$ 。 $(2, n)$ -GVSS 加密

矩阵是将 $(2, n)$ -VSS 与 $(2, 2)$ -GVSS 的矩阵结合得到, 相对差 $\alpha = \frac{2 \cdot T(S'_k[S_k(g_i)]) - T(S'_k[S_k(g_j)])}{m'}$,

其中, m' 为 $(2, n)$ -GVSS 加密矩阵的扩展度, (n, n) 方案的相对差与 $(2, 2)$ 方案类似, 因此方案的相对差 α 与灰度级 L 以及方案的扩展度 m 有关, 确保了恢复效果。

4.2 安全性分析

在 $(2, 2)$ -GVSS 加密矩阵中, 任意行向量的元素组成都相同, 因此单独的共享份不会泄露任何秘密信息。 $(2, n)$ -GVSS 的加密矩阵由 $(2, n)$ -VSS 与 $(2, 2)$ -GVSS 结合得到, 其安全性依赖后两者的安全性, 单个共享份同样不会泄露秘密信息, 类似地, 对于 (n, n) -GVSS 的加密矩阵, 任意 $k < n$ 行叠加后的汉明重量相等, 不会泄露任何秘密信息。

5 实验分析

以 $(2, 2)$ 、 $(2, 3)$ 和 $(3, 3)$ 门限方案为例, 与文献 [5, 6, 16] 进行综合比较, 结果如图 1~图 3 所示。

由图 1~图 3 可以看出, 本文方案单个共享份不会泄露秘密图像的任何信息, 对于 $(2, 2)$ 和 $(2, 3)$ 门限结构, 本文两个共享份叠加可以显示秘密图像 (图 1(d)、图 2(e)); 对于 $(3, 3)$ 门限结构, 两个共享份叠加后的图像是杂乱无意的 (图 3(e)), 无法得到秘密图像的任何信息, 3 个

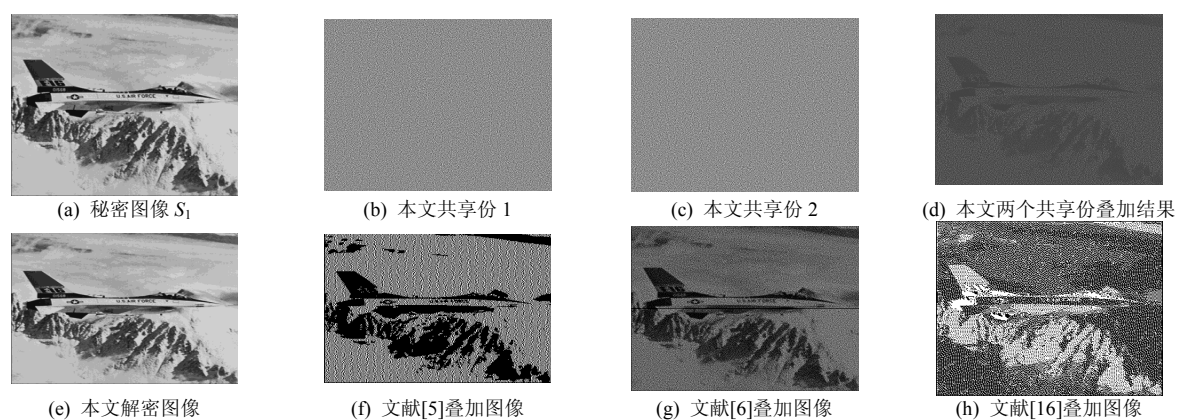


图 1 (2, 2)-GVSS 实验比较
Figure 1 (2, 2)-GVSS experiment comparisons

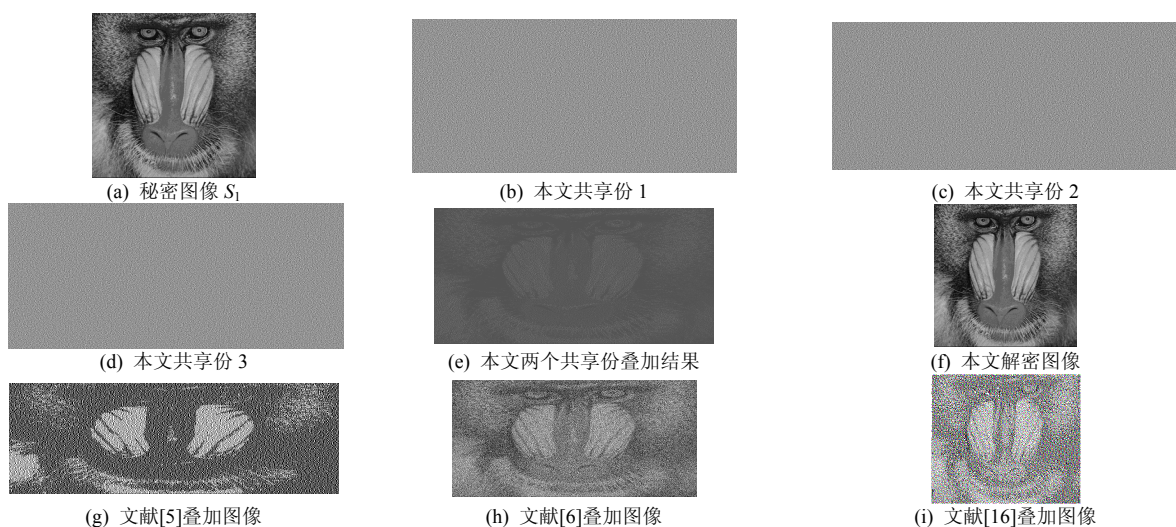


图 2 (2, 3)-GVSS 实验比较
Figure2 (2, 3)-GVSS experiment comparisons

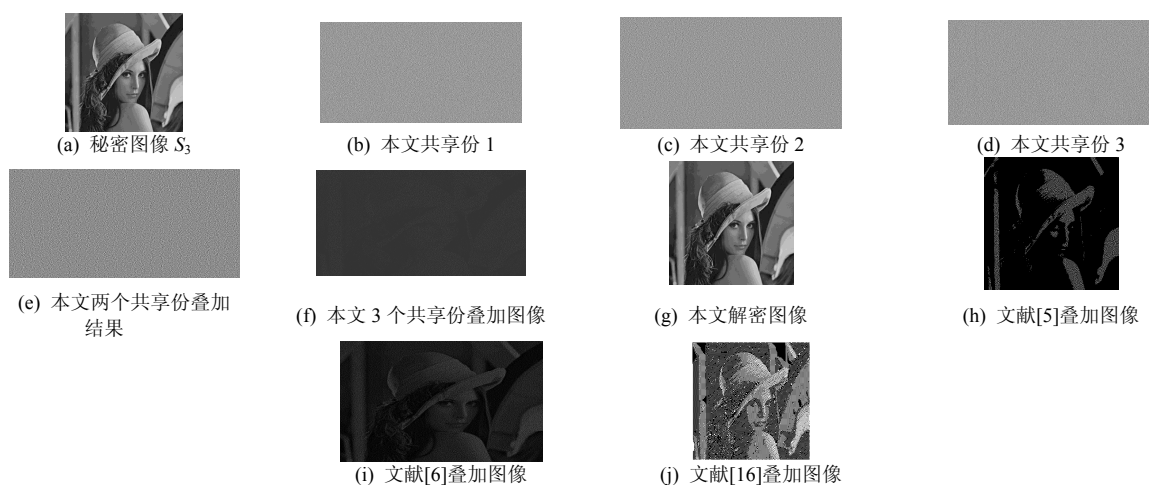


图 3 (3, 3)-GVSS 实验比较
Figure 3 (3, 3)-GVSS experiment comparisons

共享份进行叠加时可以显示秘密图像 (图 3(f)), 从本文叠加图像中提取解密图像如图 1(e)、

图 2(f)、图 3(g)所示, 可以实现原始图像的无损恢复。文献[5]在分享前对原始图像进行了半色调

预处理, 将其转化为黑白二值图像, 得到的解密图像也是二值图像 (图 1(f)、图 2(g)、图 3(h)), 相比原始灰度图像, 恢复图像产生信息损失。文献[16]利用随机栅格法对秘密图像进行分享, 共享份是大小与原图像相等的光栅, 将它们叠加在一起, 利用黑白区域的光通量不同来显示秘密信息, 优点是分享过程不依赖加密矩阵, 仅依靠随机函数来完成秘密分享, 基础原理是通过提高黑像素恢复的随机概率大于白像素, 来区分黑白区域, 然而随机函数的引入易产生像素信息损失, 恢复图像产生明显噪声, 如图 3(i)所示。本文通过为每个灰度级像素点设计相应的加密矩阵, 利用灰色叠加原理, 在无损恢复的前提下实现了像素扩展度的压缩, 因此恢复图像的像素扩展度比文献[6]小, 有效降低了共享份的传输和存储开销。

方案综合性能比较如表 1 所示, 对于 (2, 2) 方案, 由相对差计算公式, 文献[5, 6]相对差分别为 $\frac{1}{2}$ 和 $\frac{1}{3}$; 对于 (2, 3) 方案, 文献[5, 6]相对差分别为 $\frac{1}{3}$ 和 $\frac{1}{45}$; 对于 (3, 3) 方案, 文献[5, 6]相对差分别为 $\frac{1}{4}$ 和 $\frac{1}{60}$; 由于文献[5]在分享前对原始图像进行了半色调预处理, 将其转化为黑白二值图像, 得到的解密图像也是二值图像, 相比原始灰度图像, 虽然像素扩展度小, 但恢复图像存在信息损失, 无法恢复图像中的一些细节信息, 限制了其实际应用。而本文方案实现了恢复图像的无损恢复 (图 1(e)、图 2(f)、图 3(g)), 提取的解密图像相对差 $\alpha=1$, 因此恢复效果更佳。与文献[6]相比, 本文的像素扩展度更小, 对于 (2, 2)、(2, 3)、(3, 3) 这 3 种门限结构, 本文方案的像素扩展度分别约为文献[6]的 36.7%、73.3%、53.3%, 通过将灰度叠加融入可视秘密共享, 依据灰度图像的特点设计了相应的加密矩阵, 降低了共享份的存储和传输开销。除了像素扩展度和相对差之外, 方案恢复运算的计算复杂度也是重要的性能指标, 文献[5, 16]将原始灰度图像转化为黑白二值图像进行分享, 在秘密恢复时, 利用了布尔 OR 运算 (0 和 1 叠加), 因此恢复运算的计算复杂度为 $O(1)$; 对于灰度级 L 的秘密图像, 文献[6]和本

文对灰度像素进行叠加, 运算复杂度为 $O(L)$, 上述方法的计算都满足常数阶的复杂度, 符合可视密码解密简单的特点。

综上, 现有的 GVSS 方案中, 半色调方法是以牺牲部分秘密图像信息为代价来获得较小的像素扩展度, 矩阵拼接式方案实现了信息无损恢复, 但像素扩展度太大。本文引入灰度图像叠加原理, 生成灰度共享份, 充分利用了灰度图像的特性, 在保证恢复图像信息无损的前提下, 显著降低了像素扩展度, 减少了系统开销。

表 1 方案性能综合比较
Table 1 Performance comparisons among different schemes

存取结构	方法	共享份	像素扩展度	解密图像	秘密恢复复杂度
(2, 2)	本文	灰度	11	无损	$O(L)$
	文献[5]	黑白二值	2	有损	$O(1)$
	文献[6]	灰度	30	无损	$O(L)$
	文献[16]	灰度	1	有损	$O(1)$
(2, n)	本文	灰度	33	无损	$O(L)$
	文献[5]	黑白二值	3	有损	$O(1)$
	文献[6]	灰度	45	无损	$O(L)$
	文献[16]	灰度	1	有损	$O(1)$
(n, n)	本文	灰度	32	无损	$O(L)$
	文献[5]	黑白二值	4	有损	$O(1)$
	文献[6]	灰度	60	无损	$O(L)$
	文献[16]	灰度	1	有损	$O(1)$

6 结束语

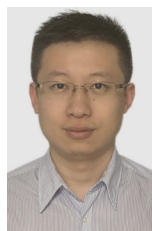
本文针对灰度图像无损共享问题展开研究, 采用“一列有效、其余列抵消”的设计思路, 选取合适的共享份灰度取值集合, 对每个灰度级分别构造加密矩阵, 在此基础上设计了 (2, 2)、(2, n)、(n, n)-GVSS 方案, 为 GVSS 研究提供了新思路。如何设计任意 (k, n) 门限下的无损恢复方案, 并进一步优化加密矩阵构造, 降低矩阵规模, 减小存储开销和传输带宽是后续研究的重点。

参考文献:

- [1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612-613.
- [2] NAOR M, SHAMIR A. Visual cryptography[C]//Advances in Cryptology-Eurocrypt 94, Lecture Notes in Computer Science.

- 1995: 1.
- [3] DROSTE. New results on visual cryptography[C]//Advances in Cryptology - CRYPTO '96, LNCS 1109. 1996: 401-415.
- [4] NARAYANA V L, GOPIL A P. Visual cryptography for gray scale images with enhanced security mechanisms[J]. *Traitement du Signal*, 2017, 34(3-4): 197.
- [5] ALEX N S, ANBARASI L J. Enhanced image secret sharing via error diffusion in halftone visual cryptography[C]//The 3rd International Conference on Electronics Computer Technology. 2011: 393-397.
- [6] PATEL T, SRIVASTAVA R. Hierarchical visual cryptography for grayscale image[C]//International Conference on Green Engineering and Technologies (IC-GET). 2016: 1-4.
- [7] 胡浩, 沈刚, 郁滨, 等. 基于随机栅格的异或区域递增式可视密码方案[J]. *计算机研究与发展*, 2016, 53(8): 1857-1866.
- HU H, SHEN G, YU B, et al. XOR-based region incrementing visual cryptography scheme by random grids[J]. *Journal of Computer Research and Development*, 2016, 53(8): 1857-1866.
- [8] 谭亦夫, 李子臣. 基于 Shamir 门限秘密分享的图像可视加密算法[J]. *网络与信息安全学报*, 2018, 32(4): 73-80.
- TAN Y F, LI Z C. Image visualization encryption algorithm based on Shamir threshold secret key sharing[J]. *Chinese Journal of Network and Information Security*, 2018, 32(4): 73-80.
- [9] HU H, SHEN G, LIU Y, et al. Improved schemes for visual secret sharing based on random grids[J]. *Multimedia Tools and Applications*, 2019, 78(9): 12055-12082.
- [10] LIN C C, TSAI W H. Visual cryptography for gray-level images by dithering techniques[J]. *Pattern Recognition Letters* 24, 2003: 349-358.
- [11] BLUNDO C, DE SANTIS A, NAOR M. Visual cryptography for grey level images[J]. *Information Processing Letters*, 2000, 75(6): 255-259.
- [12] Macpherson L. Grey level visual cryptography for general access structures[D]. Brussels University of Waterloo, 2002.
- [13] 何文才, 刘畅, 韩妍妍, 等. 一种无损恢复的多级别的可视密码方案[J]. *计算机应用研究*, 2017, 34(5): 1540-1543.
- HE W C, LIU C, HAN Y Y, et al. Multi-level visual cryptography scheme with lossless recovery[J]. *Application Research of Computers*, 2017, 34(5): 1540-1543.
- [14] 郁滨, 付正欣. 无损分享可视密码研究[J]. *通信学报*, 2013, 34(3): 165-170.
- YU B, FU Z X. Lossless sharing visual cryptography[J]. *Journal on Communications*, 2013, 34(3): 165-170.
- [15] YANG C N, SUN L Z, CAI S R. Extended color visual cryptography for black and white secret image[J]. *Theoretical Computer Science*, 2016, 609: 143-161.
- [16] WU X, LAI Z R. Random grid based color visual cryptography scheme for black and white secret images with general access structures[J]. *Signal Processing: Image Communication*, 2019, 75: 100-110.
- [17] DUTTA S, AVISHEK A, SUSHMITA R. Maximal contrast color visual secret sharing schemes[J]. *Designs, Codes and Cryptography*. 2019, 87(7): 1699-1711.
- [18] DAS S S, SHARMA K D, CHANDRA J K, et al. Secure image transmission based on visual cryptography scheme and artificial neural network-particle swarm optimization-guided adaptive vector quantization[J]. *Journal of Electronic Imaging*, 2019, 28(3): 1-11.
- [19] FENG X, CHANG C C. Aesthetic QR code authentication based on directed periodic texture pattern[C]//Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018). 2019: 251.

[作者简介]



刘健(1983—), 男, 浙江文成人, 信息产业信息安全检测中心高级工程师, 主要研究方向为图像信息隐藏、安全测评、网络与信息安全。



张益(1983—), 男, 湖南常德人, 信息产业信息安全检测中心高级工程师, 主要研究方向为网络与信息安全、信息内容安全、安全性分析与测试。



刘玉岭(1982—), 男, 山东济阳人, 博士, 中国科学院信息工程研究所副研究员, 主要研究方向为安全态势感知、网络行为分析。



胡浩(1989—), 男, 安徽池州人, 博士, 信息工程大学讲师, 主要研究方向为可视秘密共享与网络安全。