孟祥凤,王洪君,于唤理. 具有防欺骗能力的核心参与者视觉密码方案[J]. 智能计算机与应用,2024,14(11):67-73. DOI:10.20169/j.issn.2095-2163.24042401

具有防欺骗能力的核心参与者视觉密码方案

孟祥凤, 王洪君, 于唤理
(吉林师范大学 数学与计算机学院, 吉林 四平 136000)

摘 要: 针对分享份为无意义的随机二值图像问题,提出了一种分享为有意义的且具有核心参与者的视觉密码共享(2,4,3,6)方案。其中,参与恢复秘密图像的分享份中必须包含指定数量的核心分享份。与传统的具有核心参与者的视觉密码方案不同,该方案生成的分享图像不再是杂乱无章的噪声图像,而是包含特定的图像信息。方案主要利用构造基础矩阵的思想实现具有核心参与者的视觉密码共享(2,4,3,6)方案的构造。该方案对于提高视觉密码的安全性和可用性具有重要的意义,可以很好地满足实际应用的需要。实验结果验证了所提出方案的有效性。

关键词: 视觉密码; 核心参与者; 分享; 秘密图像; 掩盖图像
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 2095-2163(2024)11-0067-07

A visual cryptography scheme for essential participants with anti spoofing ability

MENG Xiangfeng, WANG Hongjun, YU Huanli
(College of Mathematics and Computer, Jilin Normal University, Siping 136000, Jilin, China)

Abstract: A visual cryptography sharing (2,4,3,6) scheme with meaningful shares and having essential participants is proposed for the problem of sharing random binary images. The shares involved in restoring secret images must include a specified number of essential shares. Different from traditional visual cryptography schemes with essential participants, the shared images generated by this scheme are no longer chaotic and noisy images, but contain specific image information. The scheme mainly realizes the construction of a visual cryptography sharing (2,4,3,6) scheme with essential participants by using the idea of constructing foundation matrix. The scheme is of great significance to improve the security and usability of visual cryptography. It can also meet the needs of practical applications. The experimental result verifies the effectiveness of the proposed scheme.

Key words: visual cryptography; essential parties; share; secret image; cover image

0 引 言

1994 年,Naor 和 Shamir[1]提出了一种名为视觉密码的图像分享技术,该技术将一个秘密分享给 n 个分享者, k 个(或者多于 k 个)分享者可以一起恢复秘密图像,而少于 k 个分享者不能获得秘密的任何信息。该技术主要对二值图像进行加密和解密处理,且解密过程不需要计算机做复杂的运算,仅需要人类的视觉系统就可以直接恢复秘密图像,具有很好的安全性,目前已经被广泛地应用于数据的安全存储与加密领域[2]。

Arumugam 等学者[3]在 2014 年首次提出了具有核心参与者的视觉密码方案,记为 $(1,k,n)$ - ENVCS (Essential and Non - essential Visual Cryptography Scheme)。为了提高核心参与者的重要性,Guo 等学者[4]在 Arumugam 等学者的基础上提出了具有 t 个核心参与者的视觉密码方案,记为 (t,k,n) - ENVCS。2014 年,Yan 等学者[5]在 (k,n) - VCS 的基础上,引入了核心和非核心的概念,提出了 (k_0,n_0,k,n) - ENVCS,其基本思想是将秘密图像分成 n 个分享份,其中 n_0 份是核心分享份, $n-n_0$ 份是非核心分享份,在解密阶段至少需要 k 张分享份, k 张分享份中至少包括 k_0 张核心分享份。Yang 等学者[6]在 2016 年利用基于概率型的视觉密码方案(Probabilistic Visual Cryptography Sharing, PVCS)设计出了一种无像素扩展的 $(t,k,$

作者简介: 孟祥凤(2001—),女,硕士研究生,主要研究方向:信息安全,密码学,视觉密码;于唤理(1999—),男,硕士研究生,主要研究方向:信息安全,密码学,视觉密码。
通信作者: 王洪君(1965—),男,博士,教授,硕士生导师,主要研究方向: 密码学,信息安全,网络体系结构。Email:jlnuwhj@sina.com。

收稿日期: 2024-04-24

n) - ENVCS。但是在文献[5]中却存在一个问题,即当收集到 $t+1$ 个不满足阈值条件的分享份时,也就是 $(t+1)<k$ 时,叠加收集到的分享份仍然可以恢复出秘密图像。为了解决以上问题,Liu 等学者在 2017 年提出了一种新的 (t,s,k,n) 核心和非核心视觉秘密方案,即 (t,s,k,n) - ENVCS。不仅满足了 2 个阈值的条件,而且在恢复秘密图像的过程中具有叠加的特性[7-9]。本文在文献[7]的基础上将分享份设计成有意义的图像,即设计为具有掩盖图像的视觉密码方案[10-13],在一定程度上减少了攻击者的注意,达到提高方案安全性的目的。

本文基于文献[14]的图像秘密共享方法,实现了分享份为有意义图像的(2,4,3,6)-ENVCS 方案,分享图像不再是杂乱无章的噪声图像,而是一幅有意义的图像,但是不会泄露秘密图像的任何信息,并且 2 个核心分享份和其他任意至少 1 个分享份叠加才可以恢复秘密图像。

1 具有核心参与者的视觉密码

1.1 视觉密码方案

Naor 和 Shamir 提出的 (k,n) 视觉密码方案是通过构造基础矩阵的方法实现的。构造的基础矩阵是一个 $n\times m$ 阶布尔矩阵,其中逻辑值"1"表示黑色像素点,逻辑值"0"表示白色像素点,n 表示参与秘密分享的参与者数量,m 表示秘密图像中的每一个像素在分享份中对应像素的数量,即像素扩展度[15-16]。(k,n) 视觉密码方案生成的分享份大多都是用户不友好的,解密时需要将这些分享份打印到透明胶片上,再让至少 k 个胶片叠加即可恢复秘密图像[17]。文献[18]对(3,4)-VCS 进行了研究,产生 4 个分享份,其中至少 3 个分享份叠加才能恢复秘密图像,对应的二维基础矩阵为:

$$\boldsymbol{M}_0=\begin{bmatrix}0&0&1&1&1&0\\0&0&1&1&0&1\\0&0&1&0&1&1\\0&0&0&1&1&1\end{bmatrix},\quad \boldsymbol{M}_1=\begin{bmatrix}1&1&0&0&0&1\\1&0&1&0&0&1\\1&0&0&1&0&1\\1&0&0&0&1&1\end{bmatrix}$$

可以看出该方案的像素扩展度为 6,即秘密图像中一个像素对应着分享份中的 6 个像素。其中,基础矩阵的两行相互叠加时,若秘密图像像素点为白色,其对应的 6 个子像素有 2 个"0";若秘密图像像素点为黑色,其对应的 6 个子像素也有 2 个"0",即 2 个分享份叠加不能得到秘密图像的任何信息。基础矩阵三行相互叠加时,若秘密图像像素点为白色,其对应的 6 个子像素有 2 个"0";若秘密图像像素点为黑色,其对应的 6 个子像素有 1 个"0",即叠加 3 张分享份可以恢复秘密图像,此时的对比度 $\alpha=1/6$。基础矩阵四行相互叠加时,若秘密图像像素点为白色,其对应的 6 个子像素有 2 个"0";若秘密图像像素点为黑色,其对应的 6 个子像素没有"0",此时的对比度 $\alpha=1/3$,即恢复的秘密图像更加清晰。

1.2 具有核心参与者的视觉密码

在具有核心参与者的 (t,s,k,n) 方案中包含 n 个参与者,其中 s 个表示核心参与者。(t,s,k,n) - ENVCS 方案具有阈值和必要性,也就意味着,秘密图像的恢复不仅需要至少 k 张分享份的叠加参与,还需要包含 t 个核心分享份[16-19]。基于以上思想将(3,4)-VCS 扩展为(2,4,3,6)-ENVCS 进行研究,即(3,4)-VCS 中的 4 个分享份作为(2,4,3,6)-ENVCS 方案的核心分享份,只需在此基础上增加 2 个非核心分享份即可,对应的二维基础矩阵为:

$$\boldsymbol{C}_0=\begin{bmatrix}0&1&1&1&0&0&0&1&1&1&1&0&0&1\\0&1&0&0&1&1&0&1&1&0&1&1&0&1\\0&0&0&1&1&0&1&1&1&1&0&1&0&1\\0&0&1&0&0&1&1&1&0&1&1&1&0&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1\end{bmatrix},\quad \boldsymbol{C}_1=\begin{bmatrix}1&1&1&1&1&0&0&0&1&1&1&0&0&0\\1&1&1&1&0&1&0&0&1&0&0&1&1&0\\1&1&1&1&0&0&1&0&0&0&1&1&0&1\\1&1&1&1&0&0&0&1&0&1&0&0&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0\\1&1&1&1&1&1&1&1&0&0&0&0&0&0\end{bmatrix}$$

不难看出,该方案的像素扩展度为 14,也就是分享份的尺寸是秘密图像的 14 倍。因为基础矩阵的第 5 行和第 6 行是方案中的非核心参与者,为了方便将第 5 行和第 6 行的像素值设置为相同的,所以下面在进行基础矩阵的 2 行相互叠加的时候分为前 5 行的任意 2 行叠加和后 2 行的相互叠加。

例如,基础矩阵前 5 行的任意 2 行叠加的结果是,不论秘密图像像素点是白色、还是黑色,其对应的 14 个子像素都有 3 个"0",也就是 2 个分享份叠加不能得到秘密图像的任何信息;基础矩阵的后 2 行相互叠加的结果是,不论秘密图像像素点是白色、

还是黑色，其对应的 14 个子像素点都有 6 个“0”，同样也是 2 个分享份叠加不能得到秘密图像的任何信息。当基础矩阵的 3 行叠加时，如果是前 4 行中的任意 3 行叠加，对比度 $\alpha = 1/14$；如果是前 4 行中的任意 2 行和后 2 行中的任意一行叠加，对比度 $\alpha = 1/14$；如果是前 4 行中的任意一行和后 2 行叠加，对比度 $\alpha = 0$，以上也就满足了(2,4,3,6)-ENVCS 的阈值性和必要性，即至少需要 3 个分享份、且 3 个分享份中至少包含 2 个核心分享份才能恢复秘密图像。基础矩阵 6 行叠加，对比度 $\alpha = 1/7$，也就是叠加出来的秘密图像更加清晰。

实验中所用的图像如图 1 所示，实验结果如图 2 所示。其中，分享份 1 和分享份 2 叠加得到叠加结果 1；分享份 1、5、6 叠加得到叠加结果 2；分享份 1、2、5 叠加得到叠加结果 3；分享份 1、2、3、5 叠加得到叠加结果 4；分享份 1、2、3、4、5 叠加得到叠加结果 5；分享份 1、2、3、4、5、6 叠加得到叠加结果 6，可以看到随着叠加的分享份逐渐增多，叠加结果也越来越清晰。

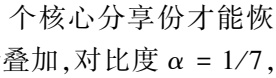


图 1　秘密图像

Fig. 1　The secret image

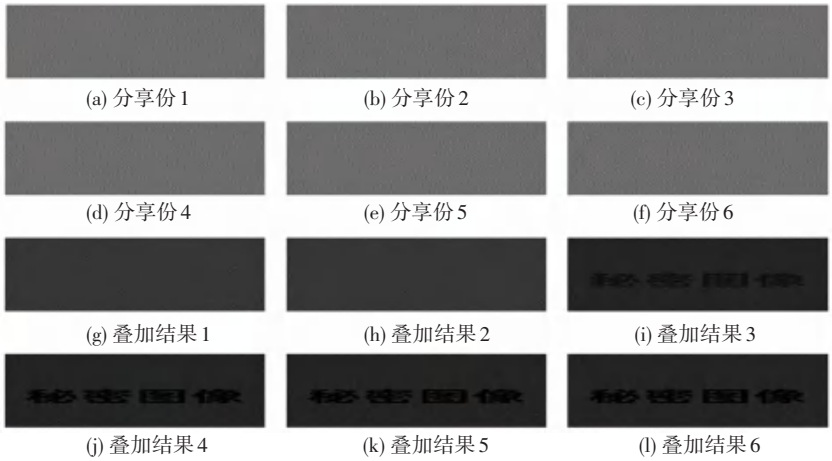


图 2　实验结果

Fig. 2　Experimental results

2　具有防欺骗功能的核心参与者视觉密码方案

2.1　方案构建方法

通过以上实验结果不难发现，(2,4,3,6)-ENVCS 产生的 6 个分享份都是黑白像素随机排列的，也就是都是无意义的图像，这样很容易引起攻击者的注意，所以在此基础上提出了分享份有意义的具有核心参与者的视觉密码方案。从 1.2 节中的基础矩阵可以看出矩阵每一行都包含 6 个“0”，为此考虑要使分享份是有意义的图像，对应基础矩阵的每一行里面“0”的数量应该存在差值。若掩盖图像像素点为白色，则对应基础矩阵的每一行应该至少有 7 个“0”；若掩盖图像像素点为黑色，则对应基础矩阵的每一行应该至少有 6 个“0”，即可满足掩盖图像中的白色像素点对应的子像素比黑色像素点对应的子像素含有更多的白色子像素，基础矩阵的任意 2 行叠加有相同数量的“0”，也就保证了任意 2 个分享份叠加不能得到秘密图像的任何信息，同时满足阈值性和必要性条件的分享份叠加的结果会产生对比度，任意不少于 4 个分享份叠加都能得到秘密图像信息。基于这样的思想构建的部分二维基础矩阵为：

$$C^{0}_{000000} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$C^0_{000001}=\begin{bmatrix}0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&1&1&1&0&1&1&1&1\\0&0&0&1&1&0&1&1&1&1&0&1&0&1&0&1&1&1&1&1&0&1&1&1\\0&0&1&0&0&1&1&1&0&1&1&1&0&1&1&0&1&1&1&1&1&0&1&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&0&1&1&1&1&1&0&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\end{bmatrix}$$

$$C^0_{000010}=\begin{bmatrix}0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&1&1&1&0&1&1&1&1\\0&0&0&1&1&0&1&1&1&1&0&1&0&1&0&1&1&1&1&1&0&1&1&1\\0&0&1&0&0&1&1&1&0&1&1&1&0&1&1&0&1&1&1&1&1&0&1&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&0&1&1&1&1&1&1&1\end{bmatrix}$$

$$C^0_{000100}=\begin{bmatrix}0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&1&1&1&0&1&1&1&1\\0&0&0&1&1&0&1&1&1&1&0&1&0&1&0&1&1&1&1&1&0&1&1&1\\0&0&1&0&0&1&1&1&0&1&1&1&0&1&1&1&1&1&1&1&1&1&1&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&0&1&1&1&1&1&0&1\\0&1&1&1&1&1&1&1&0&0&0&0&0&1&1&1&1&0&1&1&1&1&1&0\end{bmatrix}$$

$$C^1_{000000}=\begin{bmatrix}1&1&1&0&1&0&0&0&1&1&1&0&0&0&1&1&0&1&1&1&1&1&1&1\\1&0&1&1&0&1&0&0&1&0&0&1&1&0&1&1&1&0&1&1&1&1&1&1\\1&1&0&1&0&0&1&0&0&0&1&1&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&1&1&0&0&0&1&0&1&0&0&1&1&1&1&1&1&1&0&1&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&0&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&0&1&1&1&1&1&0&1\end{bmatrix}$$

$$C^1_{000001}=\begin{bmatrix}1&1&1&0&1&0&0&0&1&1&1&0&0&0&1&1&0&1&1&1&1&1&1&1\\1&0&1&1&0&1&0&0&1&0&0&1&1&0&1&1&1&0&1&1&1&1&1&1\\1&1&0&1&0&0&1&0&0&0&1&1&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&1&1&0&0&0&1&0&1&0&0&1&1&1&1&1&1&1&0&1&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&0&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1\end{bmatrix}$$

$$C^1_{000010}=\begin{bmatrix}1&1&1&0&1&0&0&0&1&1&1&0&0&0&1&1&0&1&1&1&1&1&1&1\\1&0&1&1&0&1&0&0&1&0&0&1&1&0&1&1&1&0&1&1&1&1&1&1\\1&1&0&1&0&0&1&0&0&0&1&1&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&1&1&0&0&0&1&0&1&0&0&1&1&1&1&1&1&1&0&1&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&0&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&0&1&1&1&1&1&0&1\end{bmatrix}$$

$$C^1_{000100}=\begin{bmatrix}1&1&1&0&1&0&0&0&1&1&1&0&0&0&1&1&0&1&1&1&1&1&1&1\\1&0&1&1&0&1&0&0&1&0&0&1&1&0&1&1&1&0&1&1&1&1&1&1\\1&1&0&1&0&0&1&0&0&0&1&1&0&1&1&1&1&1&0&1&1&1&1&1\\0&1&1&1&0&0&0&1&0&1&0&0&1&1&1&1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&0&1&1&1\\1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&0&1&1&1&1&0&1&1\end{bmatrix}$$

上标“0”表示秘密图像像素点为白色,上标“1”表示秘密图像像素点为黑色;下标中的“0”表示对白色像素点的分享,下标中的“1”表示对黑色像素点的分享;下标 6 位数字中的第 1 位表示基础矩阵的第一

行(分享份 1)，下标 6 位数字中的第 2 位表示基础矩阵的第 2 行(分享份 2)，下标 6 位数字中的第 3 位表示基础矩阵的第 3 行(分享份 3)，下标 6 位数字中的第 4 位表示基础矩阵的第 4 行(分享份 4)，下标 6 位数字中的第 5 位表示基础矩阵的第 5 行(分享份 5)，下标 6 位数字中的第 6 位表示基础矩阵的第 6 行(分享份 6)。基础矩阵 $\boldsymbol{C}^1_{000100}$ 表示对黑色像素点的分享方案，第 1、2、3、5、6 行表示掩盖图像像素点为白色，第 4 行表示掩盖图像像素点为黑色，6 行叠加没有“0” 即叠加结果为黑色像素点。

下面以 $\boldsymbol{C}^0_{000001}$ 和 $\boldsymbol{C}^1_{000001}$ 为例进行详细分析：对于基础矩阵 $\boldsymbol{C}^0_{000001}$ 和 $\boldsymbol{C}^1_{000001}$，如果掩盖图像对应的像素点是白色，那么基础矩阵的一行中包括 8 个“0”；如果掩盖图像对应的像素点是黑色，那么基础矩阵的一行中包括 6 个“0”，也就满足了分享份在进行叠加时掩盖图像中的白色像素点比黑色像素点有更多的白色子像素，其中对比度为 1/12。

当基础矩阵的 2 行相互叠加时，如果 2 张分享份中至少包含 1 张核心分享份，那么不论秘密图像像素点是白色、还是黑色，矩阵的 2 行叠加的结果都有 3 个“0”；如果 2 张分享份都是非核心分享份，那么不论秘密图像像素点是白色、还是黑色，矩阵的两行叠加的结果都有 6 个“0”，也就保证了 2 张分享份叠加得不到秘密图像的任何信息。

当基础矩阵的 3 行叠加时，如果 3 张分享份中至少包含 2 张核心分享份，那么若秘密图像像素点为白色，则矩阵 3 行相互叠加的结果有 2 个“0”；若秘密图像像素点为黑色，则矩阵 3 行相互叠加的结果有 1 个“0”，即对比度为 1/24，如果 3 张分享份中仅包含 1 张核心分享份，那么不论秘密图像像素点为白色、还是黑色，矩阵 3 行叠加的结果都有 3 个“0”，因为此时不满足(2,4,3,6)-ENVCS 方案的必要性条件，所以对比度为 0，即不能恢复秘密图像。

当基础矩阵的 4 行相互叠加时，如果 4 张分享份中至少包含 3 张核心分享份，那么若秘密图像像素点为白色，则矩阵 4 行相互叠加的结果有 2 个“0”；若秘密图像像素点为黑色，则矩阵 4 行相互叠加的结果没有“0”，即对比度为 1/12，如果 4 张分享份中仅包含 2 张核心分享份，那么若秘密图像像素点为白色，则矩阵 4 行相互叠加的结果有 2 个“0”；若秘密图像像素点为黑色，则矩阵 4 行相互叠加的结果有 1 个“0”，即对比度为 1/24。

当基础矩阵的 5 行或者 6 行叠加时，若秘密图像像素点为白色，则矩阵 5 行叠加的结果有 2 个“0”；若秘密图像像素点为黑色，则矩阵 5 行叠加的结果没有“0”，即对比度为 1/12。不难发现，随着叠加的分享份数量逐渐增多，对比度呈现非递减趋势。

如果秘密图像像素点为白色，分享由 $\boldsymbol{C}^0_{000000}$、$\boldsymbol{C}^0_{000001}$、$\boldsymbol{C}^0_{000010}$、$\boldsymbol{C}^0_{000100}$ 中的其中之一产生；如果秘密图像像素点为黑色，分享由 $\boldsymbol{C}^1_{000000}$、$\boldsymbol{C}^1_{000001}$、$\boldsymbol{C}^1_{000010}$、$\boldsymbol{C}^1_{000100}$ 中的其中之一产生。基础矩阵共有 128 个，其中对应白色秘密图像像素点的基础矩阵有 64 个，包括 $\boldsymbol{C}^0_{000000}$、$\boldsymbol{C}^0_{000001}$、$\boldsymbol{C}^0_{000010}$、$\boldsymbol{C}^0_{000100}$、$\boldsymbol{C}^0_{001000}$、$\boldsymbol{C}^0_{010000}$、$\boldsymbol{C}^0_{100000}$、$\boldsymbol{C}^0_{110000}$ 等；对应黑色秘密图像像素点的基础矩阵有 64 个，包括 $\boldsymbol{C}^1_{000000}$、$\boldsymbol{C}^1_{000001}$、$\boldsymbol{C}^1_{000010}$、$\boldsymbol{C}^1_{000100}$、$\boldsymbol{C}^1_{001000}$、$\boldsymbol{C}^1_{010000}$、$\boldsymbol{C}^1_{100000}$、$\boldsymbol{C}^1_{110000}$ 等，这里分别只给了 8 个，对给出的 16 个基础矩阵进行列变换即可得到剩余的 112 个基础矩阵。

2.2　实验分析

2.2.1　算法实现

输入　6 幅掩盖图像、1 幅秘密图像

输出　6 幅分享份

具体实验步骤：

(1)产生一个关于向量(1,2,3…,24)的随机置换 π。

(2)若秘密图像像素点 m 是白色像素，则对基础矩阵 $\boldsymbol{C}^0_{000000}$、$\boldsymbol{C}^0_{000001}$、$\boldsymbol{C}^0_{000010}$、$\boldsymbol{C}^0_{000100}$、$\boldsymbol{C}^0_{001000}$、$\boldsymbol{C}^0_{010000}$、$\boldsymbol{C}^0_{100000}$、$\boldsymbol{C}^0_{110000}$ 等之一进行列置换 π，得到变换后的矩阵 $\boldsymbol{T}$；若秘密图像像素点 m 是黑色像素，则对基础矩阵 $\boldsymbol{C}^1_{000000}$、$\boldsymbol{C}^1_{000001}$、$\boldsymbol{C}^1_{000010}$、$\boldsymbol{C}^1_{000100}$、$\boldsymbol{C}^1_{001000}$、$\boldsymbol{C}^1_{010000}$、$\boldsymbol{C}^1_{100000}$、$\boldsymbol{C}^1_{110000}$ 等之一进行列置换 π，得到变换后的矩阵 $\boldsymbol{T}$。

(3) 对 $1 \leqslant i \leqslant 6$，分配矩阵 $\boldsymbol{T}$ 的第 i 行给第 i 个参与者。

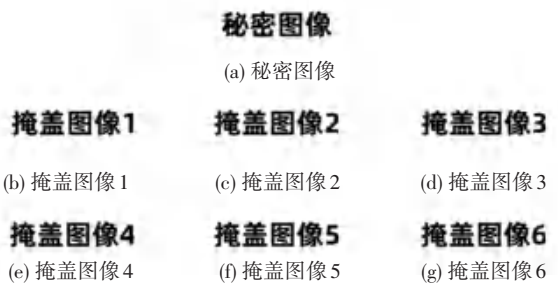
2.2.2　实验结果

实验中需要用到的图像如图 3 所示，实验结果如图 4 所示。其中，分享份 1 和分享份 2 叠加得到叠加结果 1；分享份 1、5、6 叠加得到叠加结果 2；分享份 1、2、5 叠加得到叠加结果 3；分享份 1、2、3、5 叠加得到叠加结果 4；分享份 1、2、3、4、5 叠加得到叠加结果 5；分享份 1、2、3、4、5、6 叠加得到叠加结果 6。

2.2.3　结果分析

从实验结果不难看出，6 个分享份都是有意义的图像，有别于传统的视觉密码方案，不易引起攻击者的注意。本方案与相关方案的性能比较结果见表 1。实验中产生的分享图像的像素扩展度为 24。本方案与其他文献相比像素扩展度增大了，但是随着参与恢复秘密图像的参与者数量的增多，本方案的

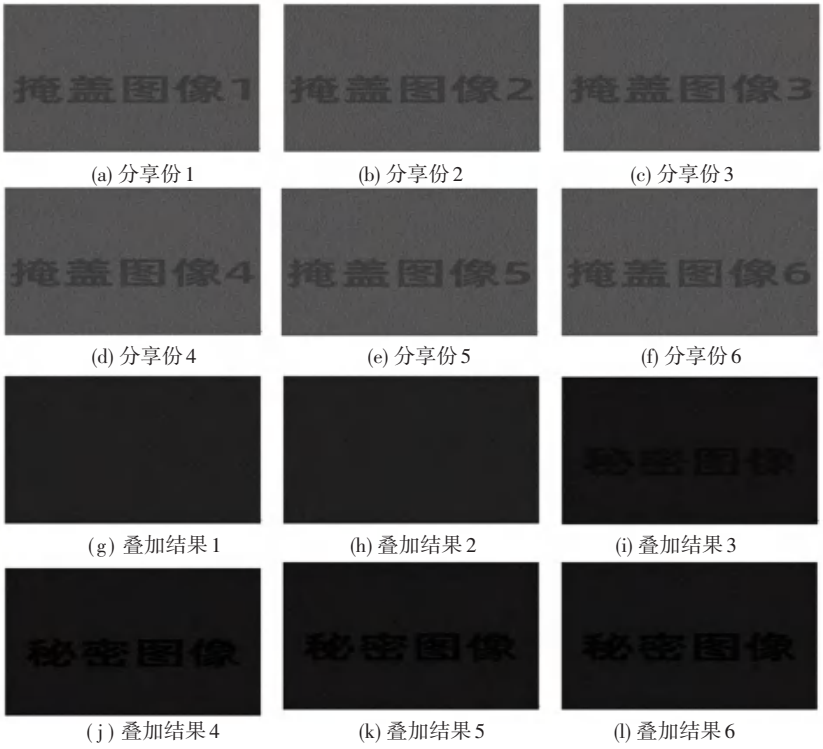
对比度是非递减的,而文献[20]中的对比度大小是一直不变的。并且本方案与其他文献中的方案相比,增加了掩盖图像,具备了验证功能,在一定程度上提高了方案的安全性。因为基础矩阵的任意 2 行相互叠加的结果都包含 3 个“0”,即没有对比度,所以任意 2 个分享份叠加不会泄露秘密图像的任何信息,2 张非核心分享份和任意 1 张核心分享份叠加产生的结果也是无意义的图像,同样不会泄露秘密图像的任何信息,保证了该方案的必要性,以上实验结果也证实了该方案是有效的。



(a) 秘密图像
(b) 掩盖图像 1 (c) 掩盖图像 2 (d) 掩盖图像 3
(e) 掩盖图像 4 (f) 掩盖图像 5 (g) 掩盖图像 6

图 3 秘密图像和掩盖图像

Fig. 3 The secret image and cover images



(a) 分享份 1 (b) 分享份 2 (c) 分享份 3
(d) 分享份 4 (e) 分享份 5 (f) 分享份 6
(g) 叠加结果 1 (h) 叠加结果 2 (i) 叠加结果 3
(j) 叠加结果 4 (k) 叠加结果 5 (l) 叠加结果 6

图 4 实验结果

Fig. 4 Experimental results

表 1 本方案与相关方案的性能比较

Table 1 Performance comparison between this scheme and related schemes

方案	文献[1]	文献[20]	文献[14]	本方案
像素扩展度	4	16	16	24
对比度 (l = 2)	12/48	–	–	–
对比度(l = 3)	–	3/48	3/48	2/48
对比度(l = 4)	–	3/48	9/48	2/48
对比度(l = 5)	–	3/48	18/48	4/48
对比度(l = 6)	–	3/48	18/48	4/48
掩盖图像	无	无	无	有
验证功能	无	无	无	有

3 结束语

本文给出了一种分享份有意义的(2,4,3,6)-ENVCS 方案,其中分享图像显示出掩盖图像。从实验结果来看该方案是有效的,分享份是有意义的图像。并且限于方案的阈值性,任意 2 个参与者叠加其对应的分享份都得不到秘密图像的任何信息,2 张非核心分享份和任意一张核心分享份叠加也不能得到秘密图像的任何信息,至少 3 张分享份并且 3 张分享份中至少包括 2 张核心分享份才能恢复出秘密图像,所给方案证实了以上想法。该方案适用于二值图像,接下来将对减少像素扩展度和改善恢复的秘密图像的质量等方面进行深入研究。

参考文献

[1] NAOR M, SHAMIR A. VisualCryptography[C]//Advances in Cryptology－EUROCRYPT´94：Workshop on the Theory and Application of Cryptographic Techniques. Cham：Springer，1995：1－12.

[2] 王洪君，牟晓丽，李静雪. 一种分享为有意义图像的(3，3)视觉密码方案[J]. 湖南师范大学自然科学学报，2014，37(6)：79－83.

[3] ARUMUGAM S，LAKSHMANAN R，Nagar A K. On $(k, n)^*$-visual cryptography scheme[J]. Designs，Codes and Cryptography，2014，71(1)：153－162.

[4] GUO Teng，LIU Feng，WU Chuankun，et al. On $(k, n)(k, n)$ visual cryptography scheme with t essential parties[C]// Proceedings of the 7th International Conference on Information Theoretic Security (ICITS 2013). Cham：Springer，2014：56－68.

[5] YAN Xuehu，WANG Shen，NIU Xiamu，et al. Essential Visual Cryptographic Scheme with Different Importance of Shares[C]// Proceedings of the 21st International Conference on Neural Information Processing(ICONIP 2014). Cham：Springer，2014：636－643.

[6] YANG C，SUN Lizhe，YAN Xuehu，et al. Design a new visual cryptography for human－verifiable authentication in accessing a database[J]. Journal of Real－Time Image Processing，2016，12：483－494.

[7] LI Peng，LIU Zuquan. A novel visual cryptography scheme with different importance of shadows[C]//Proceedings of the 16th International Workshop on Digital Forensics and Watermarking (IWDW 2017). Cham：Springer，2017：365－377.

[8] 甘明，甘志，陈克非. 具有掩盖图像的可视秘密共享方案[J]. 计算机应用与软件，2005，22(7)：1－2.

[9] ULUTAS M. Meaningful Share generation for increased number of secrets in visual secret－sharing scheme[EB/OL]. (2010－07－27). https://doi.org/10.1155/2010/593236.

[10] 付正欣，郁滨，房礼国. 具有伪装图案的操作式多秘密视觉密码[J]. 计算机科学，2011，38(6)：90－92.

[11] 王洪君，刘毅，苑卫鑫. 具有伪装图像的可视双秘密分享[J]. 吉林大学学报（理学版），2015，53(6)：1251－1256.

[12] KUMARI K，BHATIA S. Multi－pixelvisual cryptography for color images with meaningful shares[J]. International Journal of Engineering Science and Technology，2010，2(6)：2398－2407.

[13] WANG Daoshun，YI Feng，LI Xiaobo. On general construction for extended visual cryptography schemes[J]. Pattern Recognition，2009，42(11)：3071－3082.

[14] 刘祖权. 具有核心参与者的图像秘密共享方法研究[D]. 北京：华北电力大学，2018.

[15] FANG W. Friendly progressive visual secret sharing[J]. Pattern Recognition，2008，41(4)：1410－1414.

[16] CHIU P，LEE K. User－friendly threshold visual cryptography with complementary cover images[J]. Signal Processing，2015，108：476－488.

[17] WEIR J，YAN Weiqi. A Comprehensive Study of Visual Cryptography[M]//SHI Y Q. Transactions on Data Hiding and Multimedia Security V. Lecture Notes in Computer Science. Cham：Springer，2010：70－105.

[18] DROSTE S. New results on visual cryptography[C]// Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. Cham：Springer，1996：401－415.

[19] 尹丽萍. 具有核心参与者的视觉图像分享方案研究[D]. 北京：华北电力大学，2021.

[20] ATENIESE G，BLUNDO C，DE SANTIS A，et al. Visual cryptography for general access structures[J]. Information and Computation，1996，129(2)：86－106.