基于异或的外形比例不失真(k,n)视觉密码方案

董 晨[1] 张皓宇[2] 季姝廷[2] 李 磊[2]

[1](天津理工大学计算机科学与工程学院天津市智能计算及软件新技术重点实验室 天津 300384)

[2](天津市大数据管理中心 天津 300221)

摘 要 通过设计基于奇偶列的加密矩阵构造方法,结合多行扫描和多点加密的像素不扩展技术,提出一种基于"异或"运算的(k,n)视觉密码方案,并证明方案的安全性和有效性。实验结果表明,该方案能够实现秘密图像的外形比例不失真恢复,同时提高相对差,有效改善图像的恢复效果。

关键词 视觉密码 异或 门限结构 外形比例不失真

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.09.044

ASPECT RATIO INVARIANT(K,N) VISUAL CRYPTOGRAPHY SCHEME BASED ON XOR

Dong Chen[1] Zhang Haoyu[2] Ji Shuting[2] Li Lei[2]

[1](*Tianjin Key Laboratory of Intelligence Computer and Novel Software Technology, School of Computer Science and Engineering, Tianjin University of Technology, Tianjin 300384, China*)

[2](*Big Data Management Center, Tianjin 300221, China*)

Abstract By designing the construction method for encryption matrix based on odd-even columns, and combining the pixel unexpanded technology with multi-lines scanning and multi-pixel encryption, this paper proposes a(k,n) visual cryptography scheme based on "XOR" operation. Meanwhile, the security and effectiveness of our scheme is proved. The experimental results indicate that our scheme can achieve the undistorted restoration of the aspect ratio of the secret image. The relative difference is increased, and the restoration effect of the image is effectively improved.

Keywords Visual cryptography XOR Threshold structure Aspect ratio invariant

0 引 言

作为一种秘密共享技术,视觉密码[1](Visual Cryptography,VC)具有理论安全和恢复简单的特点。它将秘密分享为若干杂乱无章的共享份,恢复时将足够数量的共享份叠加,自提出以来,便引起众多学者的重视和研究兴趣[2-4]。

在视觉密码的早期研究中,方案主要采用透明胶片为介质,因而其恢复操作只能是叠加,亦即布尔二元运算中的"或"运算。无论是 Naor 等[1]最早给出视觉密码的(n,n)方案,还是 Droste 等[5]通过设计加密矩阵给出相对差为 $1/m$(m 为加密矩阵列数)的(k,n)方案,都存在像素扩展度较大、外形比例失真和相对差较小的问题,需要进一步对视觉密码方案参数进行优化。为此,Hou 等[6]提出了一种多点加密技术,对秘密图像逐行进行扫描,每分享 m 个黑(白)像素就使用了加密矩阵的所有列,实现了秘密图像的不扩展分享与恢复,虽然恢复图像的外形比例不失真,但该方案的相对差没有得到实质性提高。

另一种实现像素不扩展的方法是随机栅格法,文献[7]设计了基于随机栅格(Random Grid,RG)的视觉密码(RG-based VC,RGVC),共享份是与原始图像尺寸相同的光栅,通过将共享份进行"或"叠加,通过黑白区域的光通量不同来显现秘密信息。由于 RGVC 只借助随机函数来实现秘密共享[8],因此共享过程不依

收稿日期:2019-06-21。国家级大学生创新创业训练计划项目(201810060008)。**董晨**,讲师,主研领域:视觉密码,数据挖掘。**张皓宇**,工程师。**季姝廷**,工程师。**李磊**,工程师。

赖加密矩阵是 RGVC 的优势,可以有效减小加密矩阵的存储开销。依据该思路,Shyu[9] 基于二元运算的 3 种函数f_{equ}、f_{ran}和f_{com}设计了一种$(2,2)$方案的秘密分享算法。此后,Chen 等[10]、Guo 等[11]和 Hu 等[12]相继设计了存取结构为$(2,n)$、(n,n)和(k,n)的 RGVC 改进方案。Shen 等[13]分析了 RGVC 方案到加密矩阵方案的变换,指出随机栅格是加密矩阵的算法表示。事实上,RGVC 方案是加密矩阵方案的一个特例,同样存在恢复效果不佳的问题,因此设计更优的加密矩阵方案成为当前主流的研究思路。

综上所述,尽管现有方案在像素扩展度方面得到了优化,但始终存在恢复图像相对差低的问题。本质上,该类方案用"或"运算执行像素叠加,从代数结构上讲,其操作都属于半群结构,使得像素无法实现完全恢复,特别地,对于表示白像素的 0 而言,其代数结构不存在逆元,是限制恢复效果进一步改善的根本原因。为了突破基于透明胶片叠加的运算介质对方案的影响,Biham 等[14]提出了基于偏振光的视觉密码,恢复像素的颜色不再是共享份对应像素"或"运算的结果,而是由共享份偏振方向的平行"或"正交来决定,该操作可以表示为"异或"(XOR)运算,具有像素扩展度小和相对差大的特点,但方案依赖特定的光学设备,恢复过程较为复杂。随着现代科学技术的发展,具有计算能力的智能终端在现实应用中日益普及,为实现"异或"操作提供了简便途径,Tuyls 等[15]首次给出基于 XOR 视觉密码的定义,并实现了(n,n)方案的完全恢复,但该方案的分享算法不适用于一般的(k,n)存取结构。郁滨等[16]结合(n,n)"异或"方案的加密矩阵,提出了共享份分块构造的设计思路,可以实现相对差的无失真恢复,但叠加图像的外形比例存在失真。

针对以上问题,本文设计基于奇偶列的加密矩阵构造方法,在图像分享时,通过改进多行扫描、多点加密技术,构造出一种基于"异或"的(k,n)秘密分享算法,在实现恢复图像外形比例不失真的前提下,提高了相对差,最后,通过理论和实验验证方案安全性和对比性。

1　基本概念

设共享集合为$K=\{i_1,i_2,\cdots,i_n\}$,定义授权集合为$Q(Q\subseteq K$ 且$|Q|\geqslant k)$,禁止集合为$P(P\subseteq K$ 且$|P|<k)$,对于任意参与者集合$X\subseteq K=\{i_1,i_2,\cdots,i_p\}$,记$\boldsymbol{V}(X,\boldsymbol{S},\oplus)$表示矩阵$\boldsymbol{S}$中$X$的分量所在行"异或"得到的行向量,$H(\boldsymbol{V})$表示$\boldsymbol{V}$的汉明重量。

定义 1　称两个$n\times m$布尔矩阵为元素的集合C_0和C_1构成一个(k,n)"异或"视觉密码方案,其中C_0表示分享白像素的映射空间,C_1表示分享黑像素的映射空间,在分享白(黑)像素时从C_0(C_1)中随机选取一个矩阵$\boldsymbol{S}_0$($\boldsymbol{S}_1$),对应n个共享份各自的m个子像素,则矩阵$\boldsymbol{S}_0$、$\boldsymbol{S}_1$满足下列两个条件:

1)安全性条件:当$X\subseteq P$时,$H(\boldsymbol{V}(X,\boldsymbol{S}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{S}_1,\oplus))$。

2)对比性条件:当$X\subseteq Q$时,$H(\boldsymbol{V}(X,\boldsymbol{S}_1,\oplus))-H(\boldsymbol{V}(X,\boldsymbol{S}_0,\oplus))>0$。

安全性条件表明当参与者人数小于k时,禁止集合P中的参与者无法获得秘密图像的任何信息。对比性条件表明当参与者人数等于k时,授权集合Q中的参与者通过共享份"异或"运算可以实现秘密恢复。评价视觉密码方案有两个重要参数:像素扩展度m和相对差α。

定义 2　设(k,n)-VCS 加密矩阵为$\boldsymbol{S}_0$和$\boldsymbol{S}_1$,任取$\boldsymbol{S}_0$(或$\boldsymbol{S}_1$)中k行,当$\boldsymbol{S}_0$中此k行的任意列向量$\boldsymbol{l}$中含有奇数个"1"(或$\boldsymbol{S}_1$中k行的任意列向量$\boldsymbol{l}'$中含有偶数个"1")时,则称向量$\boldsymbol{l}(\boldsymbol{l}')$为矩阵$\boldsymbol{S}_0$(或$\boldsymbol{S}_1$)的多余列。将$\boldsymbol{l}(\boldsymbol{l}')$的$k$行中所含有"1"的个数记为$r$。

关于上述定义的三点补充说明:

1)m表示原始图像中的一个像素在分享图像中扩大的子像素的个数,也就是原始图像经过扩展后在面积上失真的倍数。像素扩展度越大所需的存储空间就越大,即代表其在面积上的失真也会越大。

2)α是恢复图像中代表黑像素的向量汉明重量最小值$\boldsymbol{l}$与代表白像素的向量汉明重量最大值$\boldsymbol{h}$之差与像素扩展度m之比,即:$\alpha=(\boldsymbol{l}-\boldsymbol{h})/m$,其中$\alpha\in[0,1]$,当$\alpha=0$时代表黑白像素的灰度值相等,完全不能辨别出原图像,即无法识别秘密信息;当$\alpha=1$时代表恢复图像中黑白像素完美恢复,是最理想的情况。

3)定义 2 给出多余列的概念,用于后续算法 2 中加密矩阵的构成。

2　方案设计

本节构造一种外形比例不失真的(k,n)"异或"视觉密码方案的秘密分享和恢复流程,并对方案的有效性进行证明。

2.1　秘密分享流程

为进一步优化视觉密码相关参数,本文通过添加奇偶列的方法构造加密矩阵,通过融合多行扫描和多点加密技术,构造(k,n)方案的秘密图像分享流程如

图 1 所示,通过该流程生成的共享份不存在像素扩展。

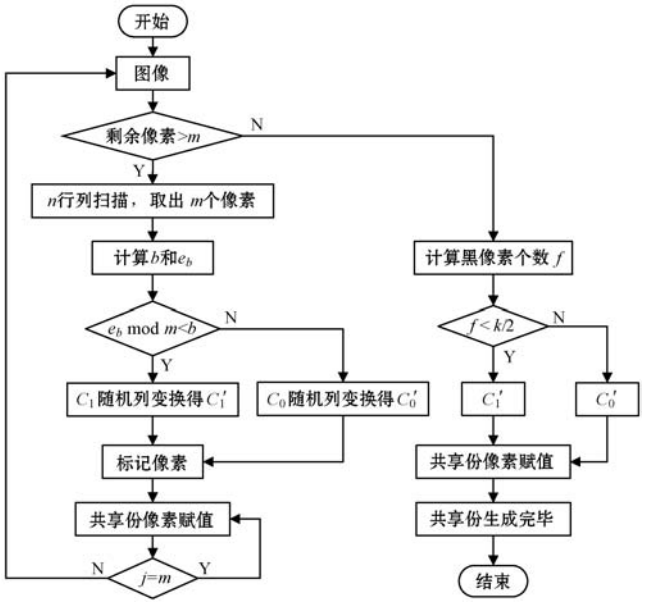


图 1 (k,n)视觉密码方案秘密分享流程

算法 1 秘密图像分享算法

输入:秘密图像 S。

输出:共享份 $SI_1,SI_2,\cdots,SI_n$。

Step 1 读取原始秘密图像 S 中的各像素信息。

Step 2 取 $n=\lceil\sqrt{m}\rceil$,对图像像素依次按 n 行进行行列扫描,扫描选取出连续的 m 个像素。

Step 3 计算这 m 个像素中黑像素的个数,记为 b,用 e_b 代表已经完成扫描的像素中含有 b 个黑像素的扫描序列的个数,其中 $b=(0,1,\cdots,m)$,初始时定义 $e_b=0$。

Step 4 判断 $e_b \bmod m<b$ 是否成立,若是,则对此向量采用加密矩阵 $\boldsymbol{C}_1$ 随机列变换后得到的 $\boldsymbol{C}_1'$ 矩阵进行加密,否则用加密矩阵 $\boldsymbol{C}_0$ 随机列变换后得到的 $\boldsymbol{C}_0'$ 矩阵进行加密。

Step 5 将这 m 个像素按扫描顺序依次标记为向量 $\boldsymbol{P}_{lj}=(V_{l1},V_{l2},\cdots,V_{lm})$,$(l=1,2,\cdots,m)$,用 l 标记完成扫描序列的个数,j 表示当前扫描到的像素在 $\boldsymbol{P}_{lj}$ 标记向量中的位置,初始化 $l=1,j=1$。

Step 6 针对扫描序列中的单个像素,若此像素位于第 l 标记的第 j 个位置,若加密矩阵 $\boldsymbol{C}'_x(x=0$ 或 $1)$中,第 i 行第 j 列元素为 1,则对第 i 个共享份中需要加密的 m 个像素的第 j 个像素设置为 1(黑);若加密矩阵 $\boldsymbol{C}'_x(x=0$ 或 $1)$中,第 i 行第 j 列元素为 0,则设置为 0(白)。

Step 7 判断是否 $j=m$。若是,则返回 Step 2,重新扫描;若不是,则令 $j=j+1$,进行下一个像素的处理。

Step 8 若最后剩余的像素有 k 个,不及 m 个,则判断其中黑像素所占个数 f;若 $f<k/2$,用 $\boldsymbol{C}_0'$ 加密,否则用 $\boldsymbol{C}_1'$ 加密。具体单个像素的处理同 Step 5 – Step 6;所有像素处理完毕。

Step 9 输出生成的共享份 $SI_1,SI_2,\cdots,SI_n$,算法结束。

关于算法 1 的三点补充说明:

1) Step 2 – Step 4 实现秘密图像的多行扫描,按行列顺序依次将秘密图像以 m 个像素为单位进行划分,并计算各 m 个像素中黑像素个数;

2) Step 5 – Step 6 利用多点加密法实现对 1)中 m 个像素的分享,$n\times m$ 矩阵 $\boldsymbol{C}'_x$ 各向量分别赋值给 n 个共享份上对应位置上的 m 个像素值;

3) Step 4 中加密矩阵设计是算法的核心环节,本文提出一种基于奇偶列的加密矩阵构造方法,具体如算法 2 所示。

加密矩阵的构造流程如图 2 所示。

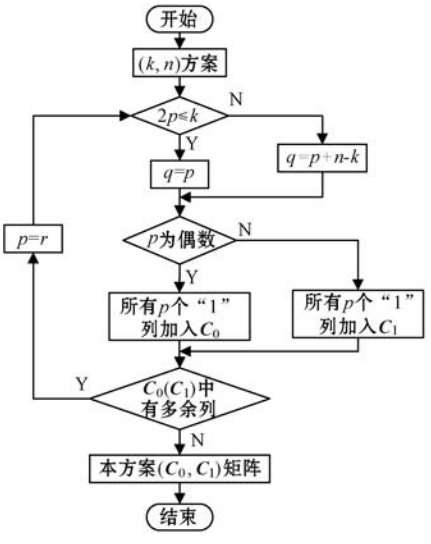


图 2 加密矩阵构造流程

算法 2 加密矩阵构造算法

输入:门限结构(k,n),$n\geqslant k\geqslant 2$。

输出:加密矩阵$(\boldsymbol{C}_0,\boldsymbol{C}_1)$。

Step 1 对于所有偶数 $p(0\leqslant p\leqslant k)$,若 $2p\leqslant k$,则令 $q=p$;否则,令 $q=n+p-k$,将所有含 q 个“1”的 n 维列向量的组合添加到矩阵 $\boldsymbol{C}_0$ 中。

Step 2 对于所有奇数 $p(0\leqslant p\leqslant k)$,若 $2p\leqslant k$,则令 $q=p$;否则,令 $q=n+p-k$,将所有含 q 个“1”的 n 维列向量的组合添加到矩阵 $\boldsymbol{C}_1$ 中。

Step 3 依据定义 2,在 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$ 中添加多余列:1) 将 $\boldsymbol{C}_1$ 中的多余列用 Step 1 和 Step 2 的方法添加到 $\boldsymbol{C}_0$ 中,生成新的 $\boldsymbol{C}_0$;2) 将 $\boldsymbol{C}_0$ 中的多余列添加到 $\boldsymbol{C}_1$ 中,生成新的 $\boldsymbol{C}_1$。

Step 4 判断 $\boldsymbol{C}_0$、$\boldsymbol{C}_1$ 中的多余列是否相等,若相等,则该步骤结束,否则转到 Step 1。

Step 5 生成和输出加密矩阵 $\boldsymbol{C}_0$、$\boldsymbol{C}_1$,算法结束。

2.2 秘密恢复流程

秘密恢复如图 3 所示,依据(k,n)门限原理,从生成的 n 个共享份 $SI_i(i=1,2,\cdots,n)$中任取 k 个,采用“异或”操作进行叠加,即可恢复出原秘密图像。

图 3 秘密恢复流程

3　方案有效性证明

依据定义 1,本节分别从安全性和对比性两个方面对方案的有效性进行形式化证明。

引理 1[1]:在(k,k)-VCS 中,加密矩阵 $\boldsymbol{C}_{0(k\times k)}$ 中任意一列 1 的个数为偶数,$\boldsymbol{C}_{1(k\times k)}$ 中任意一列 1 的个数为奇数。

定理 2(安全性)　当 $X\subseteq P$ 时,$H(\boldsymbol{V}(X,\boldsymbol{C}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{C}_1,\oplus))$。

证明:根据(k,n)方案的加密矩阵构造方法,$\boldsymbol{C}_0$($\boldsymbol{C}_1$)中任取 k 行产生的多余列将以同样数目添加到 $\boldsymbol{C}_1$($\boldsymbol{C}_0$)中去,将 $\boldsymbol{C}_0$($\boldsymbol{C}_1$)中任取 k 行产生的所有多余列和从 $\boldsymbol{C}_1$($\boldsymbol{C}_0$)添加过来的所有多余列合并在一起生成加密矩阵 $\boldsymbol{C}_0$($\boldsymbol{C}_1$)的相同列,通过添加多余列来保证加密矩阵 $\boldsymbol{C}_0$($\boldsymbol{C}_1$)的任意 k 行由引理 1 中的矩阵 $\boldsymbol{C}_{0(k\times k)}$($\boldsymbol{C}_{1(k\times k)}$)相同列构成。故 $\boldsymbol{C}_0$、$\boldsymbol{C}_1$ 任意 k 行中相同列所包含的列向量相同,由于相同列具有相同的汉明重量,在只考虑任意 k 行时可以忽略。对于 $\boldsymbol{C}_0$($\boldsymbol{C}_1$)取 k 行剩余的偶数(奇数)列,满足 $\boldsymbol{C}_{0(k\times k)}$($\boldsymbol{C}_{1(k\times k)}$)矩阵的特性。任取 $p(p<k)$行,令:

$$SUM1=\binom{k-p}{1}+\binom{k-p}{3}+\cdots+\binom{k-p}{t}(t\text{ 为奇数})$$

$$SUM2=\binom{k-p}{0}+\binom{k-p}{2}+\cdots+\binom{k-p}{t}(t\text{ 为偶数})$$

则在指定扩展位置,对于奇数列 p 有 $SUM1$ 或 $SUM2$ 种将 $\boldsymbol{C}_{0(p\times p)}$($\boldsymbol{C}_{1(p\times p)}$)扩展为基本 $\boldsymbol{C}_{0(k\times k)}$($\boldsymbol{C}_{1(k\times k)}$)矩阵的组合方式,利用组合数学可以证明 $SUM1=SUM2$[5],此处不再赘述。

同样反过来,可以推导出 $\boldsymbol{C}_0$、$\boldsymbol{C}_1$ 中任意 $p(p<k)$行所包含的列相同(随机列交换等价),由此可以得出当 $X\subseteq P$ 时,$H(\boldsymbol{V}(X,\boldsymbol{C}_0,\oplus))=H(\boldsymbol{V}(X,\boldsymbol{C}_1,\oplus))$,即当参与者个数小于 k 时,无法得到秘密图像任何信息,满足定义 1 中的安全性条件。

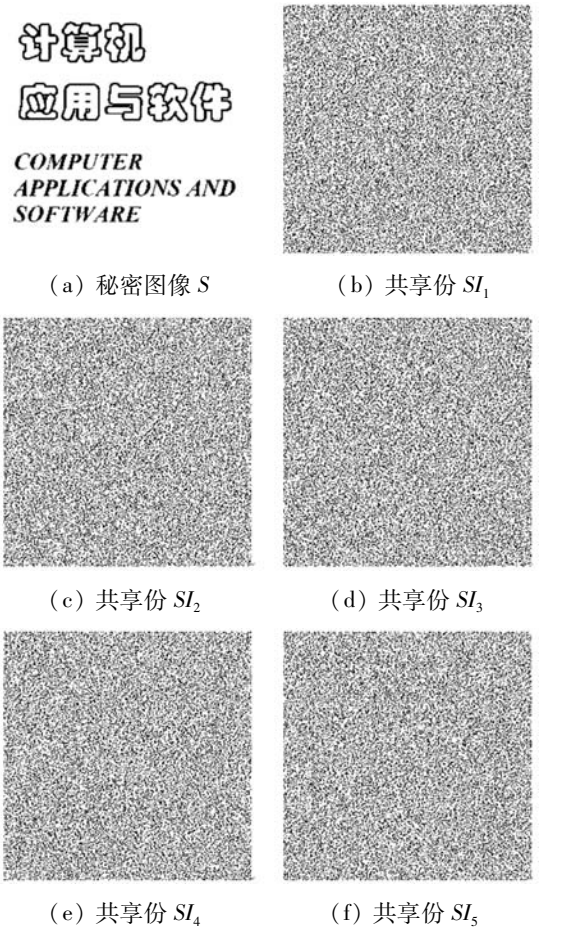
定理 3(对比性)　当 $X\subseteq Q$ 时,$H(\boldsymbol{V}(X,\boldsymbol{S}_1,\oplus))-H(\boldsymbol{V}(X,\boldsymbol{S}_0,\oplus))>0$。

证明:如果 $X\subseteq Q$,则存在参与者个数大于等于门限值 k。当参与者个数等于 k 时,($\boldsymbol{C}_0$,$\boldsymbol{C}_1$)中任意 k 行包含($\boldsymbol{C}_{0(k\times k)}$,$\boldsymbol{C}_{1(k\times k)}$)及相同列,由于相同列无论是“异或”还是“或”叠加所得到的汉明重量相等,不影响汉明重量差。则对于 $\boldsymbol{C}_{0(k\times k)}$($\boldsymbol{C}_{1(k\times k)}$)中的偶数(奇数)列,$H(\boldsymbol{V}(X,\boldsymbol{C}_{1(k\times k)},\oplus))-H(\boldsymbol{V}(X,\boldsymbol{C}_{0(k\times k)},\oplus))=2^{k-1}>0$,即参与者个数为 k 时秘密图像可恢复。当参与者个数大于 k 时,任取其中 k 个共享份“异或”叠加即可恢复图像,满足定义 1 中的对比性条件。

4　实验分析

下面以图 4 黑白秘密图像 S 为例,采用(4,5)门限结构对方案有效性进行实验验证。首先利用 2.1 节算法 2 构造(4,5)方案的加密矩阵如下:

$$\boldsymbol{C}_0=\begin{bmatrix}111100000000011\\100011100000011\\010010011000011\\001001010100011\\000100101100011\end{bmatrix}\quad \boldsymbol{C}_1=\begin{bmatrix}100001000011110\\010000100011101\\001000010011011\\000100001010111\\000010000101111\end{bmatrix}$$



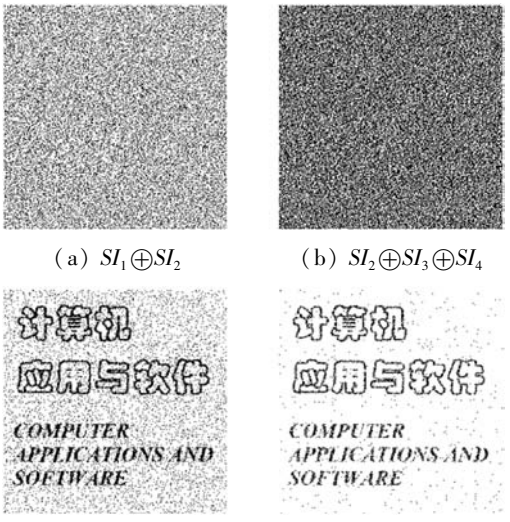
(a) 秘密图像 S　(b) 共享份 SI_1

(c) 共享份 SI_2　(d) 共享份 SI_3

(e) 共享份 SI_4　(f) 共享份 SI_5

图 4　秘密图像与共享份

利用 2.1 节算法 1 生成共享份 SI_1、SI_2、SI_3、SI_4、SI_5,如图 4 所示,基于 2.2 节恢复流程得到叠加图像如图 5 所示,依据第 1 节相对差计算公式得到方案参数如表 1 所示。可以看出,共享份图像完全杂乱无章,不会泄露原秘密图像 S 的任何信息,当少于 4 个共享份进行叠加时,也无法恢复秘密信息,验证方案的安全性。当不少于 4 个共享份进行“异或”运算时,可以显示秘密信息,验证方案的对比性,即必须满足(k,n)门限条件时才可完成秘密恢复。



(a) $SI_1 \oplus SI_2$ (b) $SI_2 \oplus SI_3 \oplus SI_4$

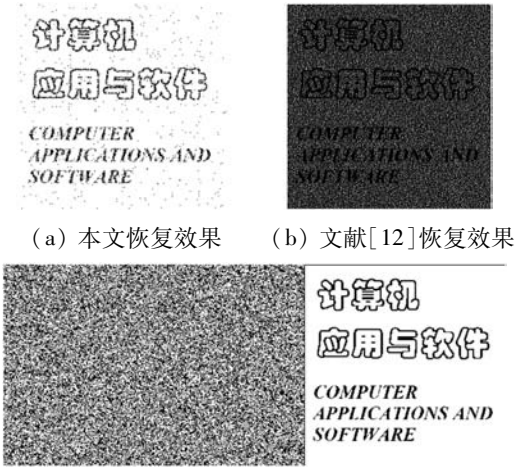
(c) $SI_1 \oplus SI_2 \oplus SI_3 \oplus SI_4$ (d) $SI_1 \oplus SI_2 \oplus SI_3 \oplus SI_4 \oplus SI_5$

图 5 不同数量共享份叠加效果

表 1 方案参数比较

类型	像素扩展度 m	相对差
本文	1	8/15
文献[12]	1	1/8
文献[16]	2.5	1

将本文与文献[12,16]进行对比,恢复效果比较如图 6 所示。可以看出,文献[12]的恢复图像虽然不存在像素扩展但恢复效果不佳,由于文献[12]设计受限于"或"运算,导致恢复图像的相对差为 1/8,而本文中 4 个共享份进行恢复时的相对差为 8/15,恢复效果明显优于文献[12];文献[16]基于"异或"运算设计,虽然能实现秘密区域的完美恢复,但恢复图像较原始图像 S 在外形尺寸上存在较大失真,像素扩展为 2.5,特别地,当 k、n 值逐渐增大时,像素扩展度 m 迅速增加,不便于共享份图像的传输和存储。综上,本文方案在实现外形比例不失真的前提下,明显提高相对差,折中考虑像素扩展度和相对差,使方案关键参数得到优化。



(a) 本文恢复效果 (b) 文献[12]恢复效果

(c) 文献[16]恢复效果

图 6 方案恢复效果比较

5 结 语

本文提出的(k,n)"异或"视觉密码方案,通过添加奇偶列的方法构造加密矩阵,在秘密分享时利用多行扫描、多点加密逐像素点进行加密,恢复图像实现外形比例不失真,且增大相对差,优化共享份图像的存储和传输开销,并改善秘密图像的恢复效果。但本文方法无法实现秘密图像的完美恢复,与原始图像相比,恢复图像相对差仍存在一定的失真,如何进一步优化是后续研究重点。

参 考 文 献

[1] Naor M, Shamir A. Visual cryptography[C]//Workshop on the Theory and Application of of Cryptographic Techniques, 1994.

[2] Hu H, Shen G, Fu Z, et al. General construction for XOR-based visual cryptography and its extended capability[J]. Multimedia Tools & Applications, 2016, 75(21):13883 - 13911.

[3] 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.

[4] 胡浩,沈刚,郁滨,等. 基于随机栅格的异或区域递增式视觉密码方案[J]. 计算机研究与发展,2016,53(8):1857 - 1866.

[5] Droste S. New results on visual cryptography[C]//Annual International Cryptology Conference, 1996.

[6] Hou Y, Tu S. A visual cryptographic technique for chromatic images using multi-pixel encoding method[J]. Journal of Research and Practice in Information Technology, 2005, 37(2):179 - 191.

[7] Shyu S J. Image encryption by multiple random grids [J]. Pattern Recognition, 2009, 42(7): 1582 - 1596.

[8] Kafri O, Keren E. Encryption of pictures and shapes by random grids[J]. Optics Letters, 1987, 12(6): 377 - 379.

[9] Shyu S J. Image encryption by random grids[J]. Pattern Recognition, 2007, 40(3): 1014 - 1031.

[10] Chen T H, Tsao K H. Threshold visual secret sharing by random grids[J]. Journal of Systems and Software, 2011, 84(7): 1197 - 1208.

[11] Guo T, Liu F, Wu C. Threshold visual secret sharing by random grids with improved contrast[J]. Journal of Systems and Software, 2013, 86(8): 2094 - 2109.

[12] Hu H, Shen G, Fu Z, et al. Improved contrast for threshold random-grid-based visual cryptography[J]. KSII Transactions on Internet & Information Systems, 2018, 12(7): 3401 - 3420.

(下转第 281 页)

方不诚实者获取不了未知粒子信息。同样 Alex 和 Candy 将部分测量结果公布出来,通过验证也能发现 Bess 是不诚实的。同样参与者两方 Bess 和 Candy 不诚实,通过相关验证也能被发现。

3.3　对比分析

文献[16 - 17]提出了基于三粒子不对称纠缠信道的未知单粒子态和双粒子纠缠态的共享方案,并提出了基于四粒子不对称纠缠信道的未知双粒子纠缠态的共享方案,需要实施 GHZ 态测量和联合幺正操作。而本文利用五粒子不对称纠缠态解决了秘密共方案,操作简单,不需要实施 GHZ 态测量,幺正操作也不需要联合处理,最后一步进行即可。文献[2]利用对称粒子纠缠态作为量子信道完成未知单粒子秘密共享。本文利用非对称五粒子纠缠态除了解决了未知单粒子态的秘密共享,还有未知双粒子态的秘密共享,进一步增加了方案的可选择性。

4　结　语

本文基于五粒子不对称纠缠态,提出一个量子秘密共享的方案。安全分析表明,任何一方不靠其他参与者的协助都无法重构秘密,本文方案是安全的。下一步将深入研究不对称量子信道以及多方量子通信的量子秘密共享方案及其应用。

参　考　文　献

[1] 朱珍超. 基于量子理论的秘密共享协议和对话协议研究[D]. 西安:西安电子科技大学,2011.

[2] Abulkasim H, Hamad S, Bahnasy K E, et al. Authenticated quantum secret sharing with quantum dialogue based on Bell states[J]. Physica Scripta, 2016, 91(8): 085101.

[3] Grice W P, Evans P G, Lawrie B, et al. Quantum secret sharing with phase-encoded photons[C]//2014 Conference on Lasers and Electro-Optics (CLEO)-Laser Science to Photonic Applications. IEEE, 2014: 1 - 2.

[4] Frikken K B. Secure multiparty computation[C]//Algorithms and theory of computation handbook. Chapman & Hall/CRC, 2010: 927 - 938.

[5] Arrazola J M, Wallden P, Andersson E. Multiparty quantum signature schemes[EB]. arXiv: 1505.07509, 2015.

[6] 高明,汪学明. 基于量子理论的多方秘密共享方案的构建[J]. 计算机应用研究,2018,35(7):2135 - 2138,2142.

[7] 邵婷婷,张仕斌,昌燕. 基于 Bell 态的(3,3)量子秘密共享方案[J]. 计算机工程与设计,2019,40(5):1210 - 1213,1224.

[8] 王静涛. 量子秘密共享方案及其应用研究[D]. 北京:北京邮电大学,2018.

[9] 张国帅,许道云. 量子隐形传态的通用线路[J]. 软件学报,2019,30(12):3579 - 3589.

[10] Lu C B, Miao F Y, Hou J P, et al. Verifiable threshold quantum secret sharing with sequential communication[J]. Quantum Information Processing, 2018, 17(11): 310.

[11] Choi M J, Lee Y H, Lee S. Quantum secret sharing and Mermin operator[J]. Quantum Information Processing, 2018, 17(10): 258.

[12] Qin H W, Tang W K S, Tso R. Rational quantum secret sharing[J]. Scientific reports, 2018, 8(1): 11115.

[13] 于浩,贾玮,咎继业,等. 基于诱骗态的 BB84 协议量子秘密共享方案[J]. 量子电子学报,2019,36(3):348 - 353.

[14] Qin H W, Tso R. Efficient quantum secret sharing based on polarization and orbital angular momentum[J]. Journal of the Chinese Institute of Engineers, 2019, 42(2): 143 - 148.

[15] Bae J, Jin J W, Kim J, et al. Three-party quantum teleportation with asymmetric states[J]. Chaos, Solitons and Fractals, 2005, 24(4): 1047 - 1052.

[16] 张群永. 基于三粒子纠缠态的未知单粒子态量子秘密共享[J]. 量子电子学报,2012,29(4):421 - 426.

[17] 张群永. 基于四粒子纠缠态的量子秘密共享方案[J]. 量子电子学报,2016,33(6):718 - 723.

[18] 张群永. 基于不对称量子信道的量子态共享协议研究[D]. 苏州:苏州大学,2010.

[19] 李培培,谭晓青. 基于可重用的不对称三粒子纠缠态的量子秘密共享[J]. 计算机应用研究,2016,33(4):1120 - 1123,1127.

[20] 张建中,张文昊. 两个基于四粒子纠缠态的量子秘密共享方案[J]. 计算机应用研究,2016,33(1):225 - 228.

[21] 魏敏娜. 多方互动量子秘密共享方案设计与分析[D]. 南京:东南大学,2016.

[22] Song Y, Li Z H, Li Y M. A dynamic multiparty quantum direct secret sharing based on generalized GHZ states[J]. Quantum Information Processing, 2018, 17(9): 244.

[23] 刘成基,李志慧,司萌萌,等. 基于局域区分的六粒子正交纠缠态的量子秘密共享方案[J]. 信息网络安全,2018(4):56 - 64.

(上接第 276 页)

[13] Shen G, Liu F, Fu Z, et al. Visual cryptograms of random grids via linear algebra[J]. Multimedia Tools and Applications, 2018, 77(10): 12871 - 12899.

[14] Biham E, Itzkovitz A. Visual cryptography with polarization [OL]. https://www.researchgate.net/publication/2872008_Visual_Cryptography_with_Polarization, 2004.

[15] Tuyls P, Hollmann H D, Lint J H, et al. XOR-based visual cryptography schemes[J]. Designs, Codes and Cryptography, 2005, 37(1): 169 - 186.

[16] 郁滨,胡浩,陈武平,等. 一种共享份分块构造的异或区域递增式视觉密码方案[J]. 电子与信息学报,2015,37(8):1978 - 1983.