一种新的多秘密分享视觉密码

付正欣,郁 滨,房礼国
(信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文给出了一种新的多秘密分享视觉密码的定义,能够支持多授权子集和共享份操作.基于区域标记和单秘密视觉密码的基础矩阵,设计了多秘密分享与恢复的流程,给出一种实现方案.最后对方案的有效性进行了理论证明和实验验证.

关键词: 视觉密码; 多秘密分享; 区域标记
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2011) 03-0714-05

A New Multi-Secret Sharing Visual Cryptography

FU Zheng-xin, YU Bin, FANG Li-guo
(*Institute of Electronic Technology, Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: A definition of multi-secret sharing visual cryptography has been proposed, which supports multiple qualified sets and shares operations. Based on the area marking and the basis matrices of single secret sharing visual cryptography, the procedures of multi-secret sharing and recovering are designed. Furthermore, a scheme is realized. At last, the effectiveness is proved and verified by experiments.

Key words: visual cryptography; multi-secret sharing; area marking

1 引言

视觉密码是一种新型的秘密共享技术,它利用人类的视觉系统直接恢复秘密信息,而且具有"一次一密"的安全性[1],因此在提出后引起广大学者的关注和研究兴趣.近年来,视觉密码的研究内容主要涉及存取结构[2,3]、参数优化[4,5]及彩色图像[6,7]等多个方面.作为视觉密码的重要内容,多秘密分享视觉密码(Multi-secret sharing Visual Cryptography Scheme, MVCS)不仅可以解决分享多幅图像带来的共享份管理问题,由于其分享的秘密图像数量更多,因此还可以广泛地应用于信息的分级管理、共享份的身份认证等方面,逐渐成为国内外研究的热点.目前,MVCS 主要包括两类:基于存取结构的方案(Access-based MVCS, AMVCS)和基于共享份操作的方案(Operation-based MVCS, OMVCS).

AMVCS 利用不同的参与者集合恢复多幅秘密图像.在 Yu[8]等的方案中共有 n 个参与者,其中 k 个参与者分享一幅秘密图像,任意 $k-1$ 个参与者均分享一幅秘密图像,最多可恢复 $C(n,k-1)+1$ 个秘密图像.而 OMVCS 则通过操作两个共享份来恢复多幅秘密图像.Chen 等[9]提出了一种(2,2,2)方案,叠加两个正方形共享份可以恢复一幅秘密图像,然后将一个共享份旋转 90°、180°或 270°,再与另一个共享份叠加则得到第二幅秘密图像.Hsu 等[10]将方形共享份改进为首尾相接的环形共享份,使旋转角度扩展至 0°到 360°的任意角度,但仍局限于分享两幅秘密图像.Feng 等[11]通过设计 4 种不同的分享模式,实现了两个环形共享份恢复任意数量的秘密图像.

AMVCS 和 OMVCS 从不同的侧面实现了多秘密的分享,但均存在一定的不足:AMVCS 的每个授权子集只能分享一幅秘密图像,而 OMVCS 的所有秘密图像则只能由一个授权子集进行分享.由于两者的优势互补,因此设计一种能结合两者优点的多秘密分享视觉密码,可以有效地解决现有方案中多授权子集与共享份操作不能共存的矛盾,对多秘密视觉密码的研究具有重要的意义.但由于两者的设计方法不同,给该方面的研究带来了重重的困难.

结合 AMVCS 和 OMVCS 的优点,本文给出一种新的多秘密分享视觉密码的定义,设计了一种基于基础矩阵和区域标记的构造方案,对方案的有效性进行了证明.实验结果表明:本方案既可以利用不同的授权子集恢复多幅图像,也能通过旋转环形共享份恢复不同的图像.

收稿日期:2009-11-08;修回日期:2010-04-30
基金项目:国家自然科学基金(No.61070086);河南省杰出青年科学基金(No.094100510002)

2 多秘密分享视觉密码的定义

由于 AMVCS 和 OMVCS 的定义并不适用于本文,因此本节给出一种新的多秘密分享视觉密码的定义.首先介绍基于通用存取结构的单秘密视觉密码定义.

设 $P=\{1,2,\cdots,n\}$ 为参与者集合,2^P 表示 P 所有子集的集合,$\Gamma_{\text{Qual}}\subseteq 2^P$ 表示授权子集的集合,$\Gamma_{\text{Forb}}\subseteq 2^P$ 表示禁止子集的集合,且 $\Gamma_{\text{Qual}}\cap\Gamma_{\text{Forb}}=\varnothing$,$\Gamma_{\text{Qual}}\cup\Gamma_{\text{Forb}}=2^P$.$(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}})$ 称为一个存取结构,简记为 (Γ_Q,Γ_F).记 $\boldsymbol{V}(\{i_1,i_2,\cdots,i_s\},\boldsymbol{M})$ 表示矩阵 $\boldsymbol{M}$ 中 $i_1,i_2,\cdots,i_s$ 行或运算得到的行向量,$H(\boldsymbol{V})$ 表示 $\boldsymbol{V}$ 的汉明重量.

定义 1[4]　设 (Γ_Q,Γ_F) 是一个存取结构,则称两个以 $n\times m$ 布尔矩阵为元素的集合 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$,组成一个 (Γ_Q,Γ_F,m) 视觉密码方案(VCS).分享白(黑)像素时,从 $\boldsymbol{C}_0(\boldsymbol{C}_1)$ 中随机选取一个矩阵,对应 n 个共享份的 m 个子像素.其中 $\boldsymbol{C}_0$ 和 $\boldsymbol{C}_1$ 满足以下两个条件:

(1)任意的授权子集 $X=\{i_1,i_2,\cdots,i_p\}\in\Gamma_Q$ 均能恢复秘密图像.数学表示为:设 $\boldsymbol{M}_0\in\boldsymbol{C}_0$,$\boldsymbol{M}_1\in\boldsymbol{C}_1$,则 $H(\boldsymbol{V}(X,\boldsymbol{M}_0))\leqslant t_X-\alpha\cdot m$,$H(\boldsymbol{V}(X,\boldsymbol{M}_1))\geqslant t_X$;

(2)任意的禁止子集 $X=\{i_1,i_2,\cdots,i_f\}\in\Gamma_F$ 均不能恢复秘密图像.数学表示为:设 $\boldsymbol{D}_0(\boldsymbol{D}_1)$ 为 $\boldsymbol{C}_0(\boldsymbol{C}_1)$ 中所有矩阵的 $i_1,i_2,\cdots,i_f$ 行构成的矩阵集合,则 $\boldsymbol{D}_0=\boldsymbol{D}_1$.

上面的第一个条件是对比性条件,保证原图像的黑白像素在恢复图像中可以通过人眼分辨.第二个则是安全性条件,保证不符合条件的共享份集合不能恢复出秘密图像.α 称为相对差,m 称为像素扩展度,t_X 可以随 X 改变.

设 $S_1,S_2,\cdots,S_h$ 表示 h 幅秘密图像,且各图像之间互相独立.每幅秘密图像对应一个存取结构,其中 S_i 对应的存取结构 (Γ_Q,Γ_F),记为 $\Gamma^i(1\leqslant i\leqslant h)$.记 $w_0(i,\sum,X)$ $(w_1(i,\sum,X))$ 表示 X 中的共享份叠加后,秘密图像 S_i 中白(黑)像素对应的子像素块的汉明重量,$E[w_0(i,\sum,X)](E[w_1(i,\sum,X)])$ 表示 X 中的共享份叠加后,S_i 中白(黑)像素对应子像素块的汉明重量的期望值.

定义 1 强调原图像的每个像素都要满足对比性和安全性条件,但实际上,人眼观察图像不是以像素点为单位,而是取决于部分或整幅图像的平均效果[5].根据第 3 节的构造方案 $w_0(i,\sum,X)$ 和 $w_1(i,\sum,X)$ 并非定值,因此本文以子像素块为单位,利用 $E[w_0(i,\sum,X)]$ 与 $E[w_1(i,\sum,X)]$ 描述多秘密分享视觉密码的对比性和安全性条件.具体地,$E[w_0(i,\sum,X)]$ 与 $E[w_1(i,\sum,X)]$ 的差值越大表明恢复图像的视觉效果越好,而当差值为 0 时表明恢复图像是人眼无法辨别的.

定义 2　设 $(\Gamma^1,\Gamma^2\cdots,\Gamma^h)$ 是 n 个参与者分享 h 幅秘密图像的存取结构,且对于任意的 $i\in[1,h]$ 均存在 $(\Gamma_Q^i,\Gamma_F^i,m_i)$ - VCS,则称 $(\Gamma^1,\Gamma^2\cdots,\Gamma^h,m)$-MVCS 为一个多秘密分享视觉密码方案,其中 $m=\sum_{i=1}^{h}m_i$.方案满足以下条件:

(1)任意禁止子集 $X\in\Gamma_F^i$ 均不能恢复秘密图像 S_i.数学表示为:$E[w_0(i,\sum,X)]=E[w_1(i,\sum,X)]$.

(2)任意授权子集 $X\in\Gamma_Q^i$ 均可以恢复秘密图像 S_i.数学表示为:$E[w_0(i,\sum,X)]\leqslant t'_X-\alpha_i\cdot m_i$,$E[w_1(i,\sum,X)]\geqslant t_X'$.

(3)各秘密图像之间的恢复不互相影响.

其中,前两个条件分别是安全性条件和对比性条件,α_i 是 $(\Gamma_Q^i,\Gamma_F^i,m_i)$ - VCS 的相对差,t_X' 可以随 X 改变,$m=\sum_{i=1}^{h}m_i$ 称为像素扩展度,$\text{Min}\left\{\frac{\alpha_i\cdot m_i}{m}\,\middle|\,1\leqslant i\leqslant h\right\}$ 是方案的相对差.第三个条件是唯一性条件,即一个授权子集一次只能恢复一幅秘密图像.若 $X\in\Gamma_Q^i$ 且 $X\in\Gamma_Q^j$,$(1\leqslant i\neq j\leqslant h)$,则需要通过不同的共享份叠加方式来实现秘密图像 S_i 和 S_j 的恢复.

定义 2 有两种极端情况:① $\Gamma_Q^i\cap\Gamma_Q^j=\varnothing$,$1\leqslant i\neq j\leqslant h$,即各个授权集合不存在交集,那么 MVCS 就退化为 AMVCS;② $\Gamma_Q^i=\Gamma_Q^j$,$1\leqslant i\neq j\leqslant h$,即只有一个授权集合,那么 MVCS 就退化为 OMVCS.除了上述两种情况外,更一般的情形是授权集合部分相交,即存在 Γ_Q^i 和 Γ_Q^j,满足 $\Gamma_Q^i\neq\Gamma_Q^j$ 且 $\Gamma_Q^i\cap\Gamma_Q^j\neq\varnothing$ $(i\neq j)$.因此,定义 2 不仅涵盖了 AMVCS 和 OMVCS,而且能够适应授权集合之间的一般关系.

3 MVCS 的构造方法

本节以单秘密视觉密码方案的基础矩阵为构造单位,通过区域标记实现了像素点的灵活组合,设计了一种符合定义 2 的 MVCS 构造方法.

3.1 基本概念

设 h 幅秘密图像的大小均为 $a\times b$,那么每个共享份均由 $a\times b$ 个子像素块组成.

定义 3　一个子像素块用 $1\times m$ 的布尔矩阵来表示,其中 $m=\sum_{i=1}^{h}m_i$,m_i 是 $(\Gamma_Q^i,\Gamma_F^i,m_i)$ - VCS 的像素扩展度,$1\leqslant i\leqslant h$.记前 m_1 个像素为区域 1,随后 m_2 个像素为区域 2,依次类推,直到区域 h.

子像素块的组成结构如图 1(a)所示.为了便于设计,本文对每幅秘密图像的像素按列进行标记,具体如图 1(b)所示,其中每一列像素的标记相同,b 表示图像的宽度.在共享份中每个区域都有各自的标记,区域 i 根据标记对应秘密图像 S_i 中的一个像素,所有区域 i 的标记与 S_i 中标记是循环右移的关系.在一个共享份中,秘密图像 S_i 对应的所有区域 i 的标记如图 1(c)所

示，k 表示 S_i 中像素在共享份区域 i 的对应位置，其中 $2 \leqslant k \leqslant b$. 当 $k=1$ 时，标记与秘密图像中的像素标记一致. 各区域的标记与各秘密图像的标记一一对应，图 1 (d)给出一个完全标记的共享份图例. 其中 $1 \leqslant k_1, k_2, \cdots, k_h \leqslant b$，$f(k)=(k+b-1) \bmod b+1$. 由图 1($d$)可以看出，一个共享份只要确定了第一个子像素块的区域标记，那么其他子像素块的区域标记就可以推断出来.

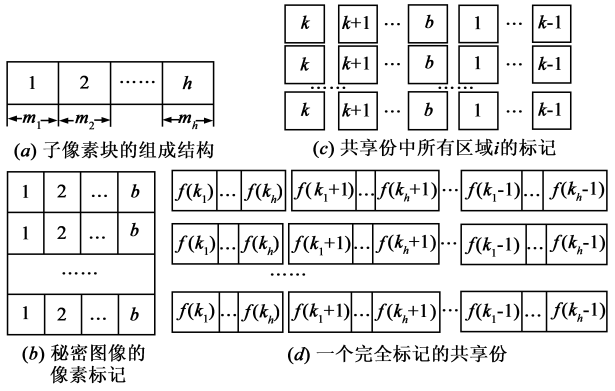


图1 共享份组成示意图

定义 4 将 n 个共享份的第一个子像素块的区域标记组成一个 $n \times h$ 的矩阵，记为区域标记矩阵 $\boldsymbol{K}=[k_{i,j}]_{n \times h}$.

显然，将所有共享份进行标记可以简化为对 $\boldsymbol{K}$ 中的元素进行赋值.

3.2 方案流程

结合 AMVCS 和 OMVCS 的特点，本文通过区域标记和基础矩阵实现了 MVCS 的秘密分享与恢复，既拥有多个授权子集，又可以使共享份叠加的方式灵活多变. 具体地，在秘密分享时，由区域的标记决定了该区域对应的单秘密视觉密码的基础矩阵，而在恢复秘密时，区域标记则决定了共享份的旋转角度. 秘密分享的流程如图 2 所示.

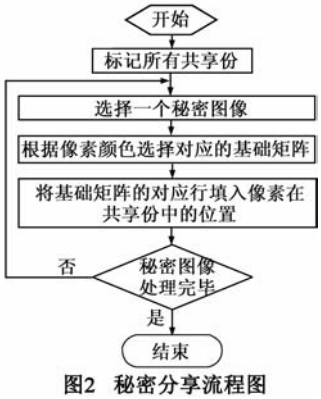


图2 秘密分享流程图

秘密恢复的过程则非常简单. 设 $X \in \Gamma_Q^i$，在恢复秘密图像 S_i 时，X 中的参与者需要旋转各自首尾相接的共享份，保证叠加共享份时，所有的第 i 区域的标记一致. 秘密恢复的过程如图 3 所示.

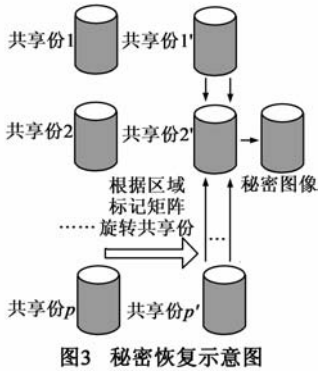


图3 秘密恢复示意图

从上述的秘密分享和恢复过程中可以看出，共享份的区域标记尤为重要，下一小节将提出一种区域标记算法.

3.3 区域标记算法

为了保证各秘密图像的恢复互不影响，需要共享份在叠加时，满足下列两个条件：(1)授权子集中标记相同的区域只有 1 个；(2)达到条件 1 的授权子集只有 1 个.

设 $X=\{i_1, i_2, \cdots, i_p\}$，记 $\boldsymbol{K}(X,j)=(\boldsymbol{K}(i_1,j), \boldsymbol{K}(i_2,j), \cdots, \boldsymbol{K}(i_p,j))$ 表示第 $i_1, i_2, \cdots, i_p$ 行、第 j 列的元素组成的向量. 根据共享份中区域标记与 $\boldsymbol{K}$ 的关系，上述 2 个条件与下面 2 个条件是等价的：(1)对于任意的 j', j''，满足 $\boldsymbol{K}(X,j') \neq u \cdot \boldsymbol{K}(X,j'')$，其中 $j_1 \leqslant j' \neq j'' \leqslant j_r$；(2)对任意 $Y \subset X$，且 Y 分享的秘密图像为 $\{y_1, y_2, \cdots, y_t\}$，则对于任意 $j' \in [j_1, j_r]$，$y' \in [y_1, y_t]$，满足 $\boldsymbol{K}(Y,j') \neq u \cdot \boldsymbol{K}(Y,y')$，其中 $j' \neq y'$，u 为常数.

下面给出一种满足上述条件的共享份区域标记算法.

Step1 建立一个空的区域标记矩阵 $\boldsymbol{K}$；

Step2 $\boldsymbol{K}$ 的第一行和第一列的所有元素为 1，$\boldsymbol{K}(2,2)=2$；

Step3 以 $\boldsymbol{K}(2,2)$ 为起点，按照从上至下、从左至右的顺序对未标记的区域加 1 递增；

Step4 根据矩阵 $\boldsymbol{K}$ 对所有的共享份进行区域标记，算法结束.

本文方案能分享的秘密图像 数量存在上限. 对于授权子集 X_i 而言，固定其中一个共享份，其余 $|X_i|-1$ 个共享份的任意旋转组合都可以对应一幅秘密图像，因此 X_i 分享的秘密图像数量上限为 $b^{|X_i|-1}$. 记所有的授权子集构成授权集合 $\Gamma_Q=\{X_1, X_2, \cdots, X_q\}$，则 Γ_Q 最多可以恢复 $\sum_{i=1}^{q} b^{|X_i|-1}$ 幅秘密图像，其中 b 表示秘密图像的宽度. 因此，当秘密图像数量在 $\sum_{i=1}^{q} b^{|X_i|-1}$ 以内时，上述算法才能有效.

4 有效性证明与实验分析

4.1 方案有效性证明

设 $w_0(i,j,X)$ ($w_1(i,j,X)$)表示 X 中的共享份叠加后，秘密图像 S_i 中白(黑)像素对应的子像素块中区域 j 的汉明重量，$E[w_0(i,j,X)]$($E[w_1(i,j,X)]$)表示 $w_0(i,j,X)$($w_1(i,j,X)$)的期望值，$E[w_0(i, \sum, X)]$($E[w_1(i, \sum, X)]$)表示 X 中的共享份叠加后，S_i 中白(黑)像素对应的子像素块的汉明重量的期望值，因此 $E[w_0(i, \sum, X)]=\sum_{j=1}^{h} w_0(i,j,X)$，$E[w_1(i, \sum,$

$X)]=\sum_{j=1}^{h} w_1(i,j,X)$.

引理 1　参与者集合 X 叠加共享份时,若区域 j 的标记不一致,且标记一致的共享份构成 X 的子集 $X_1, X_2, \cdots, X_p$,满足 $X_r \in \Gamma_F^j$,($X_r \in \{X_1, X_2, \cdots, X_p\}$),那么 X 的共享份叠加后,区域 j 不会显示任意的秘密图像信息,即 $E[w_0(i,j,X)]=E[w_1(i,j,X)], 1 \leqslant i \leqslant h$.

证明　由于秘密图像之间互相独立,因此无论区域 j 的标记是否一致,都无法恢复除 S_j 以外的秘密图像,故 $E[w_0(i,j,X)]=E[w_1(i,j,X)]$,其中 $1 \leqslant i \leqslant h$ 且 $i \neq j$. 而对 S_j 来讲:

$$w_0(j,j,X)=H(V(X_1,M_{\alpha_1})+V(X_2,M_{\alpha_2})+\cdots+V(X_p,M_{\alpha_p})),\alpha_r\in\{0,1\};$$

$$w_1(j,j,X)=H(H(V(X_1,M_{\beta_1})+V(X_2,M_{\beta_2})+\cdots+V(X_p,M_{\beta_p})),\beta_r\in\{0,1\},r\in[1,p].$$

其中 $\boldsymbol{M}_0 \in \boldsymbol{C}_0^j, \boldsymbol{M}_1 \in \boldsymbol{C}_1^j, \alpha_r, \beta_r$ 由 $X_1, X_2, \cdots, X_p$ 的标记决定. 由于基础矩阵之间的随机列排序特性,且 $H(V(X_r, M_{\alpha_r}))=H(V(X_r, M_{\beta_r}))$,因此,$E[w_0(j,j,X)]=E[w_1(j,j,X)]$. 综上,引理 1 证毕.

定理 1　设 $S_1, S_2, \cdots S_h$ 表示 h 幅秘密图像,其中 S_i 对应的存取结构为 (Γ_Q^i, Γ_F^i),若对于任意的 $i \in [1, h]$ 均存在 $(\Gamma_Q^i, \Gamma_F^i, m_i)$ - VCS,则通过本方案可以实现 $(\Gamma^1, \Gamma^2, \cdots, \Gamma^h, m)$ - MVCS,且 $m=\sum_{i=1}^{h} m_i$. 证明如下:

(1)安全性证明. 设 $X \in \Gamma_F^i$,当 X 中的共享份叠加后,$w_0(i,i,X)=w_1(i,i,X)$. 由于各秘密图像之间互相独立,则 $E[w_0(i,j,X)]=E[w_1(i,j,X)]$,其中 $j \in [1, h]$ 且 $j \neq i$. 因此,$E[w_0(i,\sum,X)]=E[w_1(i,\sum,X)]$,满足定义 2 的安全性条件,即 X 中的共享份叠加后,S_i 的白像素与黑像素各自对应的子像素块的汉明重量期望值相等,故 X 无法恢复秘密图像 S_i.

(2)对比性证明. 设 $X \in \Gamma_Q^i$,由定义 1 可知:$w_0(i,i,X) \leqslant t_X - \alpha \cdot m$, $w_1(i,i,X) \geqslant t_X$. 而其它区域的情况最多包括以下两种情况:①叠加时各共享份区域 j 的标记相同,且 $X \in \Gamma_F^j$,则 $w_0(i,j,X)=w_1(i,j,X)$;②叠加时各共享份区域 j 的标记不同,且标记一致的共享份构成 X 的子集 $X_1, X_2, \cdots, X_p$,满足 $X_r \in \Gamma_F^j (X_r \in \{X_1, X_2, \cdots, X_p\})$. 根据引理 1,$E[w_0(i,j,X)]=E[w_1(i,j,X)]$. 因此,$E[w_1(i,\sum,X)]=E[w_1(i,i,X)]+\sum_{j=1,j\neq i}^{h} E[w_1(i,j,X)] \geqslant t_X'$, $E[w_0(i,\sum,X)]=E[w_0(i,i,X)]+\sum_{j=1,j\neq i}^{h} E[w_0(i,j,X)] \leqslant t_X' - \alpha_i \cdot m_i$,其中 $t_X'=t_X+\tau$, $\tau=\sum_{j=1,j\neq i}^{h} E[w_1(i,j,X)]=\sum_{j=1,j\neq i}^{h} E[w_0(i,j,X)]$. 因此满足定义 2 的对比性条件,即 $X \in \Gamma_Q^i$ 可以恢复秘密图像 S_i.

(3)唯一性证明. 由区域标记算法可知,共享份叠加时,最多只能有一个区域的标记全部相等,因此各秘密图像的恢复不会相互影响.

综上,通过本方案可以实现 $(\Gamma^1, \Gamma^2, \cdots, \Gamma^h, m)$ - MVCS,同时由于 1 个子像素块由 h 个区域组成,故 $m=\sum_{i=1}^{h} m_i$.

4.2　实验分析

对视觉密码而言,像素扩展度和相对差是两个重要的参数,可以用来评判方案的优劣. 表 1 是本方案与其他多秘密分享方案的一个综合对比,其中 $\Gamma^1, \Gamma^2, \cdots, \Gamma^h$ 是 $S_1, S_2, \cdots, S_h$ 的存取结构,且对于任意的 $i \in [1, h]$ 均存在 $(\Gamma_Q^i, \Gamma_F^i, m_i)$ - VCS, $m=\sum_{i=1}^{h} m_i$.

表 1　本方案与其他多秘密分享方案参数对比

		$\Gamma_Q^i \neq \Gamma_Q^j$, $1 \leqslant i \neq j \leqslant h$	$\Gamma_Q^1=\cdots=\Gamma_Q^h$, $\Gamma_Q^1=\{\{1,2\}\}$	$\Gamma_Q^i=\Gamma_Q^j \neq \Gamma_Q^k$, $1 \leqslant i \neq j \neq k \leqslant h$
文献[8]	像素扩展度	m	N/A	N/A
	相对差	$1/m$	N/A	N/A
文献[11]	像素扩展度	N/A	$3h$	N/A
	相对差	N/A	$1/(3h)$	N/A
本文方案	像素扩展度	m	$2h$	m
	相对差	$1/m$	$1/(2h)$	$1/m$

从表 1 可以看出,本文方案不仅可以满足 3 种不同的多秘密分享的需求,而且方案的参数与已有方案相比也具有明显的优势. 下面以 3 个参与者分享 2 幅图像为例,对本方案的有效性进行验证.

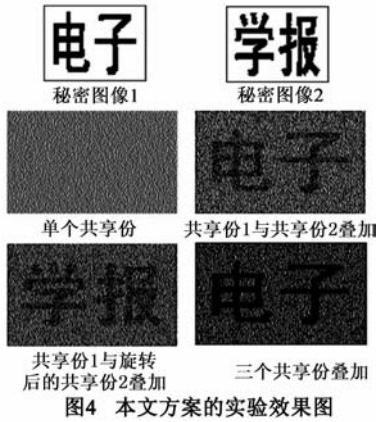


图4　本文方案的实验效果图

设参与者集合 $P=\{1,2,3\}$,秘密图像集合 $S=\{S_1, S_2\}$, $\Gamma_Q^1=\{\{1,2\},\{1,2,3\}\}$, $\Gamma_Q^2=\{\{1,2\}\}$, $\Gamma_F^1=2^P-\Gamma_Q^1$, $\Gamma_F^2=2^P-\Gamma_Q^2$,则根据文献[2]的方法可以得到:

$(\Gamma_Q^1, \Gamma_F^1, 2)$ - VCS 的基础矩阵为:$\boldsymbol{C}_0^1=\begin{bmatrix}1&0\\1&0\\0&0\end{bmatrix}$, $\boldsymbol{C}_1^1=\begin{bmatrix}1&0\\0&1\\0&0\end{bmatrix}$. $(\Gamma_Q^2, \Gamma_F^2, 2)$ - VCS 的基础矩阵为:$\boldsymbol{C}_0^2=\begin{bmatrix}1&0\\1&0\\1&0\end{bmatrix}$, $\boldsymbol{C}_1^2=\begin{bmatrix}1&0\\0&1\\1&1\end{bmatrix}$. 依据区域标记算法,得到区域标

记矩阵为:$\boldsymbol{K}=\begin{bmatrix}1 & 1\\ 1 & 2\\ 1 & 3\end{bmatrix}$.按照本文的秘密分享和秘密恢复流程,得到共享份和恢复图像如图 4 所示.

从图 4 分析可知:单个共享份没有泄露任何秘密图像的信息;共享份 1 和共享份 2 可以通过旋转操作恢复 S_1 和 S_2;S_1 可以由{1,2}和{1,2,3}两个授权子集恢复.实验表明本文方案可以同时支持多授权子集与共享份操作,达到了预期的效果.

5 总结与展望

基于 AMVCS 和 OMVCS 各自的特点,本文给出了一种新的多秘密分享视觉密码的定义.提出了一种区域标记的算法,用以得出区域标记矩阵,结合单秘密视觉密码的基础矩阵,设计了有效的秘密分享和恢复流程,并从理论上对方案有效性进行了证明.本文方案像素扩展度 $m=\sum_{i=1}^{h}m_i$,当秘密图像较多时,不便于共享份的存储和恢复图像的辨认,有待进一步改善.

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography[A]. Advances in Cryptology-Eurocrypt'94, LNCS[C]. Berlin: Springer-Verlag, 1995.950:1 – 12.

[2] ATENIESE G, BLUNDO C, De SANTIS A, STINSON D R. Visual cryptography for general access structures[J]. Information and Computation, 1996, 129(2):86 – 106.

[3] 黄东平,王道顺,黄连生,等.一种新的(k,n)阈值可视密钥分存方案[J].电子学报.2006,34(3):503 – 507.
HUANG Dong-ping, WANG Dao-shun, HUANG Lian-shen, et al. A Novel (k, n) threshold scheme for visual secret sharing [J]. Acta Electronica Sinica, 2006, 34(3):503 – 507. (in Chinese)

[4] HSU C S, TU S F, HOU Y C. An optimization model for visual cryptography schemes with unexpanded shares[A]. Foundations of Intelligent Systems—16th International Symposium, LNAI [C]. Berlin: Springer-Verlag, 2006.4203:58 – 67.

[5] LIN S J, LIN J C, FANG W P. Visual Cryptography (VC) with non-expanded shadow images Hilbert-curve approach [A]. Proceeding on IEEE International Conference on Intelligence and Security Informatics[C]. Taipei: IEEE, 2008.271 – 272.

[6] YANG C N, CHEN T S. Colored visual cryptography scheme based on additive color mixing[J]. Pattern Recognition, 2008, 41(10):3114 – 3129.

[7] NG F Y, WONG D S. On the security of a visual cryptography scheme for color images[J]. Pattern Recognition, 2009, 42(5): 929 – 940.

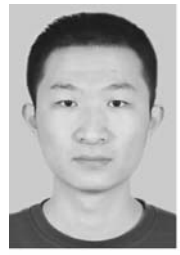
[8] YU B, XU X H, FANG L G. Multi-secret sharing threshold visual cryptography scheme[A]. 2007 International Conference on Computational Intelligence and Security[C]. Harbin: IEEE, 2007.815 – 818.

[9] CHEN L H, WU C C. A Study on Visual Cryptography[D]. Taipei: National Chiao Tung University, 1998.

[10] HSU H C, CHEN T S, LIN Y H. The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing[A]. Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control[C]. Taipei: IEEE, 2004.996 – 1001.

[11] FENG J B, WUB H C, TSAIC C S, et, al. Visual secret sharing for multiple secrets[J]. Pattern Recognition, 2008, 41 (12):3572 – 3581.

作者简介:



付正欣 男,1986 年 10 月出生于山东省曹县.博士研究生.主要研究方向为视觉密码.
E-mail:fzx2515@163.com

郁 滨 男,1964 年 7 月出生于河南省郑州市.现为信息工程大学电子技术学院教授、博士生导师.主持和参与国家自然科学基金、863 计划、军队及各类合作开发项目 30 余项,获得国家专利 2 项,发表学术论文 90 多篇.主要研究方向为视觉密码和网络安全.
E-mail:byu2009@163.com