软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(7):1757−1771 [doi: 10.13328/j.cnki.jos.004611]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种可完全恢复的门限多秘密视觉密码方案*

付正欣[1], 沈 刚[1], 李 斌[2], 郁 滨[1]

[1](信息工程大学,河南 郑州 450001)

[2](信息保障技术重点实验室,北京 100072)

通讯作者: 沈刚, E-mail: shenqi0123@163.com

摘 要: 针对门限结构下恢复多幅秘密图像存在信息损失的问题,给出了一个完全恢复的门限多秘密视觉密码定义,能够适应门限值与秘密数量之间的各种对应关系.在此基础上,通过构造具有上下门限值的单门限多秘密视觉密码方案,并设计旋转规则融合算法和区域合并算法,提出了一种多门限方案.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;单门限;多门限;信息损失;完全恢复

中图法分类号: TP309

中文引用格式: 付正欣,沈刚,李斌,郁滨.一种可完全恢复的门限多秘密视觉密码方案.软件学报,2015,26(7):1757−1771. http://www.jos.org.cn/1000-9825/4611.htm

英文引用格式: Fu ZX, Shen G, Li B, Yu B. Threshold multi-secret visual cryptography scheme with perfect recovery. Ruan Jian Xue Bao/Journal of Software, 2015,26(7):1757−1771 (in Chinese). http://www.jos.org.cn/1000-9825/4611.htm

Threshold Multi-Secret Visual Cryptography Scheme with Perfect Recovery

FU Zheng-Xin[1], SHEN Gang[1], LI Bin[2], YU Bin[1]

[1](Information Engineering University, Zhengzhou 450001, China)

[2](Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: To address the issue of information loss in recovering multiple secret images for threshold structure, this paper develops a definition of threshold multi-secret visual cryptography with perfect recovery, which can adapt to various corresponding relationship between the threshold value and the secret number. Based on the given definition, a single-threshold multi-secret visual cryptography scheme with upper and lower thresholds is constructed, and a multiple-threshold scheme is then proposed by designing the rotation rule fusion algorithm and the region merging algorithm. Furthermore, the effectiveness is proved theoretically and verified by experiments.

Key words: visual cryptography; multi-secret; single-threshold; multiple-threshold; information loss; perfect recovery

视觉密码(visual cryptography scheme,简称 VCS)[1]是秘密共享技术在数字图像领域的一种应用,继承了秘密共享的特点,同时具有自身独特的秘密恢复一般性和简单性.

作为视觉密码研究的一个主要分支,多秘密视觉密码方案(multi-secret visual cryptography scheme,简称 MVCS)是指参与者仅保存一个共享份,通过共享份组合或叠加方式的变化来恢复多幅秘密图像的一类视觉密码.其中,叠加方式通常包括翻转、旋转、平移等操作,而共享份则分别采用矩形、圆形和柱面等形状.鉴于以上丰富的设计方法,多秘密视觉密码形成了一个研究热点.

目前,在门限结构下分享多幅秘密图像,依据门限数量不同,多秘密视觉密码方案包括单门限 MVCS 和多门限 MVCS 两类,二者在构造方法上具有相似的设计思想,大部分都是通过单秘密方案的基矩阵来实现的,并且单门限 MVCS 是设计多门限 MVCS 的基础.

* 基金项目: 国家自然科学基金(61070086); 信息保障技术重点实验室开放基金(KJ-13-107)
收稿时间: 2013-05-09; 定稿时间: 2014-03-27

在单门限 MVCS 中,门限值只有一个,数量达到门限值的共享份可以通过叠加方式的变化来恢复多幅秘密图像.显然:矩形共享份通过旋转、翻转等叠加方式最多能够分享 4 幅秘密图像[2];方形共享份是矩形的一种特殊情况,最多能够分享 8 幅秘密图像[3];圆形共享份在旋转叠加时不存在角度限制问题,从而可以恢复更多的图像[4,5],但是,恢复的秘密图像在形状上存在失真.进一步的研究是将共享份做成柱面,解决了旋转角度限制和外形失真的问题[6−8].尽管上述方案实现了多幅秘密图像的分享,但存取结构仅局限于(2,2)门限结构,不适用于多个参与者.对此,Yang 等人[9]基于概率特性提出了一种(k,n)-MVCS 方案,在该方案恢复的秘密图像中,原秘密图像黑白像素以一定的概率被恢复出来,虽然整体上呈现出秘密图像,但会损失原秘密图像的部分信息.为此,Yu 等人[10]提出了一种确定性的单门限多秘密视觉密码方案,实现了秘密图像的完全恢复.

在多门限 MVCS 中,门限值有多个,每个的门限值对应恢复一定数量的秘密图像.其中,Katoh 等人[11]设计了具有两个门限值的 MVCS:第 1 个门限值为 2,即两个共享份恢复一幅秘密图像;第 2 个门限值为 3,即 3 个共享份恢复另一幅秘密图像.在共享份和秘密图像数量上均有待提高.Yu 等人[12]结合(k,n)-VCS 和(k−1,k−1)-VCS,将共享份数量增加至 n 个,但门限值依然为 2 个,分别为 k 和 k−1.乔等人[13]和 Yu 等人[14]分别利用基矩阵连接的方法提出了具有多个门限值的 MVCS.为减小像素扩展度,Shyu 等人[15]提出了一种多门限 MVCS.但在以上方案中,每个门限值都只对应恢复一幅秘密图像.付等人[16]结合单门限 MVCS 构造了一种基于概率特性的多门限 MVCS,每个门限值对应恢复多幅秘密图像,但损失了原秘密图像的部分信息.

针对以上问题,本文提出了门限多秘密视觉密码可以完全恢复的充分条件,在此基础上给出了一般性的设计方法,实现了秘密图像的完全恢复.

本文第 1 节给出门限多秘密视觉密码的一般定义,并证明以汉明重量定义的对比性条件是门限多秘密视觉密码可以完全恢复的充分条件.第 2 节依据充分条件构造一种具有上下门限值的单门限 MVCS,为第 3 节的方案设计奠定基础.第 3 节在完全恢复的条件下设计一种多门限 MVCS,并给出有效性证明.实验分析在第 4 节给出.第 5 节得出本文的结论.

1 完全恢复的充分条件

由于基于概率特性的方案在恢复每个像素时存在不确定性,因而会损失原秘密图像的部分信息,导致无法从恢复的秘密图像中提取出原秘密图像的所有信息.与基于概率特性的方案定义不同,本节给出了一种门限多秘密视觉密码的定义,明确了在恢复每个像素时必须满足确定的对比性条件.

设 n 个参与者分享 t 组秘密图像,第 i 组有 d_i 幅秘密图像,每幅秘密图像记为 S_{iu},i=1,2,…,t,u=1,2,…,d_i,秘密图像大小相等,共享份为 T_j,j=1,2,…,n,$\bigcup_r[\cdot]$ 表示对任意 r 个共享份的叠加操作,0<r≤n−1,H^1(H^0)表示原秘密图像的黑(白)像素对应恢复图像中子像素块的汉明重量,E^1(E^0)表示原秘密图像的黑(白)像素对应恢复图像中子像素块的汉明重量期望值.

定义 1. 在恢复秘密图像 S_{iu} 时,每个共享份的旋转角度所组成的集合记为Δ_{iu},Δ_{iu}={θ_{iuj}|j=1,2,…,n},其中,不同的秘密图像对应的共享份旋转角度集合也有所不同,θ_{iuj} 表示在恢复秘密图像 S_{iu} 时共享份 T_j 的旋转角度,1≤i≤t,1≤u≤d_i,θ_{iuj}∈[0°,360°].

定义 2. n 个共享份按照Δ_{iu}进行旋转操作记为 $\angle\{T_1,...,T_j,...,T_n\}^{\Delta_{iu}}$,$\angle\{T_1,...,T_j,...,T_n\}^{\Delta_{iu}}=\{\{T_j\}^{\theta_{iuj}}\mid j=1,2,...,n\}$,其中,$\{T_j\}^{\theta_{iuj}}$ 表示在恢复秘密图像 S_{iu} 时对共享份 T_j 顺时针旋转 θ_{iuj}.

定义 3. 一个多秘密视觉密码方案有 t 个门限值 k_1,k_2,…,k_t,对应恢复 t 组秘密图像,2≤k_1<k_2<…<k_t≤n,像素扩展度为 m.称该方案为(k_1,k_2,…,k_t,n)-MVCS,若方案满足以下条件:

1. 数量位于区间[k_i,k_{i+1}]的共享份能够恢复出第 i 组所有的秘密图像,数学表示为

$$H^1\left(\bigcup_r[\angle\{T_1,T_2,...,T_n\}^{\Delta_{iu}}]\right)>H^0\left(\bigcup_r[\angle\{T_1,T_2,...,T_n\}^{\Delta_{iu}}]\right),k_i\leqslant r<k_{i+1},k_{t+1}=n+1,u=1,2,...,d_i.$$

2. 数量小于 k_1 的共享份不能恢复出任何一幅秘密图像,数学表示为

$$E^1\left(\bigcup_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}]\right)=E^0\left(\bigcup_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}]\right),0\leqslant r<k_1,0°\leqslant\varphi_j\leqslant 360°.$$

第 1 个条件是对比性条件,符合条件的共享份集合按照相应的旋转角度进行旋转叠加后,可由视觉系统通过汉明重量的不同,观察出相应的秘密图像信息;第 2 个条件是安全性条件,不符合条件的共享份集合以任意角度旋转都无法恢复出秘密图像信息.

定义 3 涵盖了门限值与秘密数量的各种对应关系.

(1) 一对多关系.当 t=1 时,即,门限值只有一个,那么该定义退化为 Yu 等人[10]所提出的单门限方案;

(2) 多对一关系.当 $d_1=d_2=\ldots=d_t=1$ 时,即,每个门限都对应恢复一幅秘密图像,那么该定义就退化为 Yu 等人[14]所提出的多门限方案;

(3) 多对多关系.当不满足前两种情况时,那么该定义更加具有一般性.

定义 4. 设一个视觉密码方案的原秘密图像为 S,经过秘密分享算法后得到共享份集合 T,通过叠加操作得到恢复的秘密图像 S'.若存在一个函数 R 且其计算复杂度与叠加操作相同,满足 $S=R(S')$,则称该视觉密码方案是可以完全恢复的.

在该方案中,叠加恢复的秘密图像虽然存在像素扩展和对比度失真现象,但是没有损失原秘密图像的任何信息,在不增加恢复操作计算复杂度的前提下,可以通过函数 R 从恢复的秘密图像中提取出原秘密图像的全部信息,亦即完全恢复出原秘密图像.另外,具有计算能力的智能移动终端在现实应用中日益普及,为执行函数 R 提供了一条有效途径,没有违背视觉密码秘密恢复的简单性原则.

定理 5. 符合定义 3 的门限多秘密视觉密码方案是可以完全恢复的.

证明:由定义 3 的对比性条件可知,对于所有恢复图像的每一个子像素块而言,必然存在 $a,b\in N,0\leqslant a<b\leqslant m$,满足:

$$H^1(\bigcup\nolimits_r[\angle\{T_1,T_2,\ldots,T_n\}^{\Delta_{iu}}])\geqslant m-a, H^0(\bigcup\nolimits_r[\angle\{T_1,T_2,\ldots,T_n\}^{\Delta_j}])\leqslant m-b.$$

即:在所有恢复图像的每一个子像素块中,原秘密图像的黑像素至少对应 $m-a$ 个“1”,白像素至多对应 $m-b$ 个“1”.因此,可以通过这种确定的对应关系来完全恢复原秘密图像的每个像素,其关系表达式为

$$S_i=R(\bigcup\nolimits_r[\angle\{T_1,T_2,\ldots,T_n\}^{\Delta_{iu}}])=\begin{cases}0, & H\leqslant m-b\\ 1, & H\geqslant m-a\end{cases},$$

其中,H 为子像素块的汉明重量.由上述关系表达式可知:函数 R 实际上是在叠加操作的基础上增加了判断操作,计算复杂度没有增加.定理证毕. □

综上,定义 3 给出的对比性条件是门限 MVCS 可以完全恢复的充分条件.

2 具有上下门限值的单门限 MVCS

依据上述充分条件,本节在柱面共享份的基础上,以 $\left(\overline{\overline{k'}}{k},n\right)$-VCS 的基矩阵[15]为加密单位构造具有上下门限值的单门限 $\left(\overline{\overline{k'}}{k},n\right)$-MVCS,为设计完全恢复的多门限方案奠定基础.需要说明的是,门限结构(k,n)是 $\left(\overline{\overline{k'}}{k},n\right)$ 的一种特例,即当 $k'=n$ 时,$\left(\overline{\overline{k'}}{k},n\right)$ 与(k,n)是等效的.另外,$\left(\overline{\overline{k'}}{k},n\right)$-VCS 表达的是数量位于区间$[k,k']$的共享份能恢复出一幅秘密图像($k$ 和 k'分别代表恢复秘密图像所需共享份数量的下限值和上限值,$k\leqslant k'\leqslant n$),而本文 $\left(\overline{\overline{k'}}{k},n\right)$-MVCS 表达的是数量位于区间$[k,k']$的共享份能够恢复出多幅秘密图像.

由于文献[14]中 $\left(\overline{\overline{k'}}{k},n\right)$-VCS 的基矩阵是本文方案构造的基础,因此给出 $\left(\overline{\overline{k'}}{k},n\right)$-VCS 基矩阵的构造如下[14]:设 $N=\{J|J\subset\{1,\ldots,n\}\wedge|J|\in[k,k']\}$,对任意的$\{i_1,\ldots,i_e\}\in N$ 和 $f\in\{0,1\}$,存在布尔矩阵 $B_f(i_1,\ldots,i_e)$,它由 n 行组成,第 1 行是 $B_f^{(e,e)}$ 的第 1 行,...,第 i_e 行是 $B_f^{(e,e)}$ 的第 e 行,其余行全由 1 组成,其中,$B_f^{(e,e)}$ 是(e,e)-VCS 的基矩阵,即 $B_0^{(e,e)}$

由所有的 e 维偶数列组成,$B_1^{(e,e)}$ 由所有的 e 维奇数列组成;$\left(\frac{k'}{=},n\right)$-VCS 的基矩阵 M_f 由所有的 $B_f(i_1,\ldots,i_e)$ ($\{i_1,\ldots,i_e\}\in N$)连接而成,然后删去 M_0 和 M_1 中相同的列,形成最终的基矩阵.

为构造具有上下门限值的单门限 $\left(\frac{k'}{=},n\right)$-MVCS,首先给出一种$(k,n)$门限结构下共享份的非规则旋转算法.

2.1 非规则旋转算法

在旋转各个共享份时,旋转角度都是相对的,本节以第 1 个共享份为参照(即,不进行旋转操作),在恢复第 u 幅秘密图像时,对应的共享份旋转角度集合记为Φ_u,u=1,2,…,d,记列向量$\Phi=(\Phi_1,\Phi_2,\ldots,\Phi_d)^T$,建立一个与$\Phi$相对应的共享份旋转标记矩阵 $W=(W_1,W_2,\ldots,W_d)^T$,$W_u=\{w_{uj}|j=1,2,\ldots,n\}$,$w_{uj}\in N$,具体算法如下:

输入:门限结构(k,n)和秘密图像数量 d,$2\leqslant k\leqslant n$;

输出:共享份旋转标记矩阵 W 和变量 h,$h\in N$.

Step 1. 对于所有的 u 和 j,令 $w_{uj}=0$;

Step 2. 若 d=1,转入 Step 8,否则,转入 Step 3;

Step 3. 设 $1\leqslant u'<u$,对于 $j\in[1,n]$,w_{uj} 与所有的 $w_{u'j}$ 的距离组成的集合记为 $D_j=\{d|d=w_{uj}-w_{u'j},u'=1,2,\ldots,u-1\}$;

Step 4. 令 u=1;

Step 5. 令 $u=u+1$,对于 j=2,3,…,k,使 $w_{uj}=w_{u-1,n}+1$;

Step 6. 如果 $k=n$,转入 Step 7;

否则,对于 $j=k+1,\ldots,n$,对 w_{uj} 进行赋值,使之满足 D_j 与任意 $k-1$ 个 $D_{j'}$ 没有交集,$j'<j$;

Step 7. 若 $u=d$,则转入 Step 8;否则,转入 Step 5;

Step 8. 令 $h=w_{d,n}+1$;

Step 9. 输出 W 和变量 h,算法结束.

在上述算法的基础上,令 $\Phi=W\cdot\frac{360^\circ}{h}$,其中,$\cdot$表示点乘,即可得到共享份的旋转角度集合.

上述共享份旋转算法之所以称为非规则旋转算法,是因为其得到的共享份旋转角度呈现非规则的特性,随着(k,n)门限结构和秘密图像数量的变化而不断发生变化.非规则旋转算法保证了不同的秘密图像对应的共享份旋转角度集合也不同,并且保证了各秘密图像的恢复互不影响.

下面以(2,2)门限结构下分享 3 幅秘密图像为例,说明共享份旋转角度集合的生成过程.

以 $k=n$=2 和 d=3 为输入,依照非规则旋转算法流程输出 $W=\begin{bmatrix}W_1\\W_2\\W_3\end{bmatrix}=\begin{bmatrix}0&0\\0&1\\0&2\end{bmatrix}$ 和 h=3.因此,共享份的旋转角度集合:

$$\Phi=\begin{bmatrix}\Phi_1\\\Phi_2\\\Phi_3\end{bmatrix}=\begin{bmatrix}0^\circ&0^\circ\\0^\circ&120^\circ\\0^\circ&240^\circ\end{bmatrix}.$$

该公式表示:在恢复秘密图像 S_1 时,T_1 和 T_2 不做旋转;在恢复秘密图像 S_2 时,T_1 不做旋转,T_2 旋转 120°;在恢复秘密图像 S_3 时,T_1 不做旋转,T_2 旋转 240°.

2.2 构造方法

设 t 幅秘密图像的大小均为 $X\times Y$,Y 能被 h 整除,n 个共享份均由 $X\times Y$ 个子像素块组成,$\left(\frac{k'}{=},n\right)$-VCS 的基矩阵记为 G_0 和 G_1,其像素扩展度为 m_g.

为了便于设计,在非规则旋转算法的基础上,本节将所有的秘密图像进行子集划分,每行像素分为 Y/h 个子

集,每个子集包含 h 个像素.

定义 6. 秘密图像 S_u 第 q 行第 p 个子集中第 l 个像素记为 $S_u(q,p,l)$,$u\in[1,d]$,$q\in[1,X]$,$p\in[1,Y/h]$,$l\in[1,h]$.

定义 7. 在第 j 个共享份中,秘密图像第 q 行第 p 个子集中第 l 个像素所对应的子像素块记为 T_j^{qpl},大小为 $h\times m_g$,由 h 行组成,每行记为 $T_j^{qpl}(l,:)$.

在秘密分享时,首先根据门限结构与秘密数量设计共享份的旋转角度.在此基础上,对秘密图像划分子集.然后,针对每个子集,结合 $\left(\overline{\overline{k'}}{k},n\right)$-VCS 的基矩阵,利用子集分享算法对共享份进行赋值,秘密分享的示意图如图 1 所示.

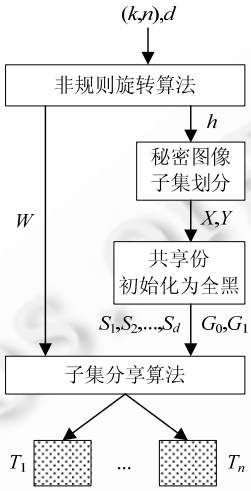


Fig.1 Sketch map of the secrets sharing for the single-threshold MVCS

图 1 单门限 MVCS 秘密分享示意图

子集分享算法保证了利用非规则旋转算法恢复的图像不存在信息损失,具体算法如下:

输入:共享份旋转标记矩阵 W、秘密图像 $S_1,S_2,...,S_d,G_0(G_1)$和初始化共享份 $T_1,T_2,...,T_n$;

输出:共享份 $T_1,T_2,...,T_n$.

Step 1. 对 G_0 和 G_1 进行列变换,使得 G_0 和 G_1 的第 1 行相同;

Step 2. 对于第 p 个子集里第 1 幅秘密图像每行中的每个像素:

- 若 $S_1(q,p,l)$=1,则 $T_j^{qpl}(l,:)=G_1(j,:)$;
- 否则, $T_j^{qpl}(l,:)=G_0(j,:)$;

Step 3. 对于第 p 个子集,依次处理第 u 幅秘密图像每行中的每个像素,u=2,3,…,d:

- 若 $S_u(q,p,l)$=1,则 $T_j^{qp((w_{uj}+l-1)\bmod h+1)}(l,:)=G_1(j,:)$, j=2,3,…,n;
- 否则, $T_j^{qp((w_{uj}+l-1)\bmod h+1)}(l,:)=G_0(j,:)$, j=2,3,…,n;

Step 4. 输出 $T_1,T_2,...,T_n$,算法结束.

由上述算法可知:由于每个子集里的所有像素采用相同组基矩阵 G_0 和 G_1 来进行分享,因此为了保证安全性,在整个秘密分享结束时,需要执行 R_{qp},表示在秘密图像每行的每个子集中,所有像素对应的子像素块进行相同的随机置换操作,取值为 1 到 $h\times m_g$ 的一个随机排列.

例如,对于(2,2)-MVCS 分享 3 幅秘密图像,子像素块的大小为 3×2,对其像素进行统一编号,经过随机置换操作的结果如图 2 所示.

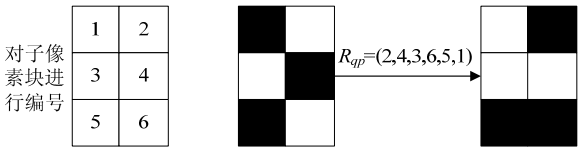


Fig.2 An example of random permutation

图 2 随机置换操作举例

秘密恢复的过程则非常简单,在恢复秘密图像 S_u 时,n 个参与者只需按照相应的旋转角度集合 Φ_u 来旋转共享份,其中,任意不少于 k 个共享份的叠加都可以恢复出相应的秘密图像.

3 多门限 MVCS

本节以具有上下门限值的单门限 MVCS 为单位,通过设计旋转规则融合算法和区域合并算法,给出了一种符合定义 3 的多门限 MVCS.

3.1 旋转规则融合算法

在定义 3 中,t 个门限值对应恢复 t 组秘密图像,将其独立来看,每组相当于一个单门限 MVCS,组与组之间的旋转规则可以相同,也可以不同,而后者在设计方案时不能保证满足确定的对比性条件,因此,本节采用前者,将各组秘密图像恢复时的旋转规则进行融合统一,融合后的旋转规则记为 Φ', $\Phi'=(\Phi_1',\Phi_2',...,\Phi_{d'}')^T$, 其中,$d'$=max($d_1$, d_2,…,d_t),下面给出旋转规则融合算法.

输入:多门限结构(k_1,k_2,…,k_t,n)和各组秘密图像数量 d_1,d_2,…,d_t;

输出:旋转规则 Φ'.

Step 1. 将多门限结构(k_1,k_2,…,k_t,n)拆分成单门限结构(k_1,n),(k_2,n),…,(k_t,n),则其对应恢复 d_1,d_2,…,d_t 幅秘密图像;

Step 2. 计算 d'=max(d_1,d_2,…,d_t);

Step 3. 依据第 2.1 节的非规则旋转算法,依次以(k_i,n)和 d'作为输入,求解相应的旋转规则,得到 W_i,h_i;

Step 4. 计算 h'=max(h_1,h_2,…,h_t),从 W_1,W_2,…,W_t 中找出对应于 h 的 W';

Step 5. 输出 $\Phi'=W'\cdot\frac{360°}{h'}$, 算法结束.

上述的旋转规则算法保证了各组秘密图像的恢复具有相同的旋转规则,下面以(2,3,3)-MVCS 分享两组秘密图像为例,说明旋转规则融合的生成过程,其中,第 1 组有 3 幅秘密图像,第 2 组有 2 幅秘密图像.

- 首先,以 k_1=2,n=3 和 d'=3 为输入,依照非规则旋转算法流程输出 $W_1=\begin{bmatrix}0&0&0\\0&1&2\\0&3&6\end{bmatrix}$ 和 h_1=7;
- 其次,以 k_2=3,n=3 和 d'=3 为输入,依照非规则旋转算法流程输出 $W_2=\begin{bmatrix}0&0&0\\0&1&1\\0&2&2\end{bmatrix}$ 和 h_2=3.

因此,融合后的旋转角度集合为

$$\Phi'=\begin{bmatrix}0&0&0\\0&1&2\\0&3&6\end{bmatrix}\cdot\frac{360°}{7}.$$

该公式表示:

- 在恢复第 1 组秘密图像时

$$S'_{11}=\bigcup_2[\angle\{T_1,T_2,T_3\}^{\{0°,0°,0°\}}],S'_{12}=\bigcup_2\left[\angle\{T_1,T_2,T_3\}^{\left\{0°,\frac{1}{7}\times360°,\frac{2}{7}\times360°\right\}}\right],S'_{13}=\bigcup_2\left[T_1,\{T_2\}^{\frac{3}{7}\times360°},\{T_3\}^{\frac{6}{7}\times360°}\right];$$

- 在恢复第 2 组秘密图像时

$$S'_{21}=\bigcup_3[\angle\{T_1,T_2,T_3\}^{\{0°,0°,0°\}}],S'_{22}=\bigcup_3\left[\angle\{T_1,T_2,T_3\}^{\left\{0°,\frac{1}{7}\times360°,\frac{2}{7}\times360°\right\}}\right].$$

3.2 方案流程

设每幅秘密图像的大小均为 $X\times Y$,Y 能被 h'整除,n 个共享份均由 $X\times Y$ 个子像素块组成.

现有多门限方案的设计方法是:首先,将单秘密方案的基矩阵进行连接;然后,根据所有秘密图像相应位置的像素,选择不同的基矩阵来进行秘密分享,但尚未解决在完全恢复的条件下相同的门限值对应恢复多幅秘密图像的问题.本节在旋转规则融合算法的基础上,结合$\left(\frac{k'}{k},n\right)$-MVCS 构造方法和区域合并算法,给出了一种完全恢复的多门限方案.具体的秘密分享过程如图 3 所示.

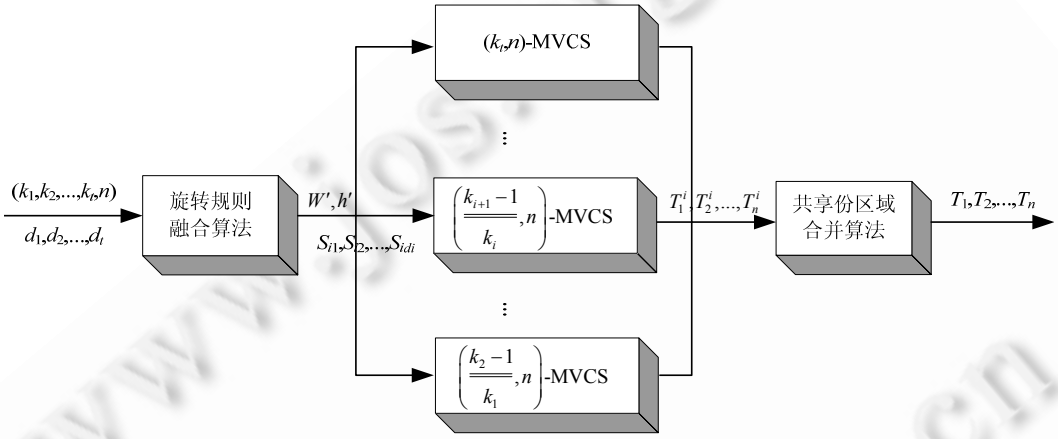


Fig.3 Sketch map of the secrets sharing for the multiple-threshold MVCS

图 3 多门限 MVCS 秘密分享示意图

其中,共享份区域合并算法保证了组与组之间恢复的秘密图像互不干扰,具体步骤如下:

输入:每个$\left(\frac{k_{i+1}-1}{k_i},n\right)$-MVCS 分享模块生成的共享份 $T_1^i,T_2^i,...,T_n^i$,大小为 $h'X\times m_g^iY$,其中,m_g^i 表示$\left(\frac{k_{i+1}-1}{k_i},n\right)$-VCS 的像素扩展度;

输出:最终的共享份 $T_1,T_2,\ldots,T_n$.

Step 1. 生成 n 个空白共享份 $T_1,T_2,\ldots,T_n$,令其大小为 $h'X\times Y\sum_1^t m_g^i$,即,每个子像素块的大小为 $h'\times\sum_1^t m_g^i$;

Step 2. 依次将各个分享模块生成的共享份 $T_1^i,T_2^i,...,T_n^i$ 的对应子像素块进行连接,将其赋值给 $T_1,T_2,\ldots,T_n$ 的对应子像素块;

Step 3. 输出 $T_1,T_2,\ldots,T_n$,算法结束.

在恢复各组秘密图像时,按照融合后的旋转规则分别进行旋转叠加,即可恢复相应的秘密图像.

3.3 有效性证明

引理 8. 方案流程中的$\left(\overline{\overline{k'}}{k},n\right)$-MVCS 是一种符合定义 3 的单门限多秘密视觉密码方案,即满足以下条件:

1. 少于 k 个共享份和多于 k'个共享份都无法恢复出任何一幅秘密图像,数学表示为

$$E^1(\bigcup\nolimits_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}])=E^0(\bigcup\nolimits_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}]),$$

其中,$1\leqslant r\leqslant k,k'<r\leqslant n,0°\leqslant\varphi_j\leqslant 360°$.

2. 按照融合后的旋转规则Φ'来旋转 n 个共享份,其中,数量位于区间$[k,k']$的共享份可以恢复出相应的秘密图像,数学表示为

$$H^1(\bigcup\nolimits_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}])>H^0(\bigcup\nolimits_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}]),k\leqslant r\leqslant k'.$$

证明:

1. 安全性证明.

对于$\bigcup_r[\{T_1^{qpl}\}^{\varphi_1},...,\{T_j^{qpl}\}^{\varphi_j},...,\{T_n^{qpl}\}^{\varphi_n}]$,根据第 2.2 节的子集分享算法可得,$r$ 个子像素块的叠加包括以下 3 种情况:

(1) r 个子像素块对应的行含有全 1 行.对于任意一幅秘密图像:

$$H^0(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=H^1(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=m_g.$$

(2) r 个子像素块对应的行含有与秘密图像无关的随机行.对于任意一幅秘密图像:

$$E^0(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=E^1(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}]).$$

(3) r 个子像素块对应的行组成$\left(\frac{k'}{k},n\right)$-VCS 基矩阵的 r 行:

- 当 $1\leqslant r<k$ 时,对于任意一幅秘密图像:

$$H^0(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=H^1(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])<m_g;$$

- 当 $k'<r\leqslant n$ 时,对于任意一幅秘密图像:

$$H^0(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=H^1(\bigcup\nolimits_r[\{T_1^{qpl}(l,:)\}^{\varphi_1},...,\{T_j^{qpl}(l,:)\}^{\varphi_j},...,\{T_n^{qpl}(l,:)\}^{\varphi_n}])=m_g.$$

综上,对于任意一幅秘密图像:

$$E^1(\bigcup\nolimits_r[\{T_1^{qpl}\}^{\varphi_1},...,\{T_j^{qpl}\}^{\varphi_j},...,\{T_n^{qpl}\}^{\varphi_n}])=E^0(\bigcup\nolimits_r[\{T_1^{qpl}\}^{\varphi_1},...,\{T_j^{qpl}\}^{\varphi_j},...,\{T_n^{qpl}\}^{\varphi_n}]).$$

因此, $E^1(\bigcup_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}])=E^0(\bigcup_r[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},...,\{T_j\}^{\varphi_j},...,\{T_n\}^{\varphi_n}])$.

2. 对比性证明.

按照融合后的旋转规则Φ'依次旋转共享份,由子集分享算法可知:

对于秘密图像 S_u, $T_1^{qpl}(l,:),...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)}(l,:),...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}(l,:)$ 共同组成了$\left(\overline{\overline{k'}}{k},n\right)$-VCS 的基矩阵.

由于 $k\leqslant r\leqslant k'$,因此:

$$H^1(\bigcup\nolimits_r[T_1^{qpl}(l,:),...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)}(l,:),...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}(l,:)])>$$
$$H^0(\bigcup\nolimits_r[T_1^{qpl}(l,:),...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)}(l,:),...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}(l,:)]);$$

又 $T_1^{qpl}(z,:),...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)}(z,:),...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}(z,:)$ 中任取 k 个,至少有一个为 $\underbrace{11...1}_{m_g},z\in[1,h'],z\neq l.$

因而:

$$H^1(\bigcup\nolimits_r[T_1^{qpl},...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)},...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}])>H^0(\bigcup\nolimits_r[T_1^{qpl},...,T_j^{qp((w'_{uj}+l-1)\bmod h'+1)},...,T_n^{qp((w'_{un}+l-1)\bmod h'+1)}]).$$

因此,对于任意一幅秘密图像: $H^1(\bigcup_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}])>H^0(\bigcup_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}])$.

引理证毕. □

定理 9. 通过本方案实现的$(k_1,k_2,\ldots,k_t,n)$-MVCS 满足定义 3 的安全性和对比性条件.

证明:

1. 安全性证明.

由于 $2\leqslant k_1<k_2<\ldots<k_t\leqslant n$,所以数量小于 k_1 的共享份都能满足每个$\left(\overline{\overline{\frac{k'}{k}}},n\right)$-MVCS 分享模块的安全性条件,而共享份区域合并算法不会影响各个分享模块的安全性条件,因此,数量小于 k_1 的共享份不能恢复出任何一幅秘密图像.

2. 对比性证明.

按照融合后的旋转规则Φ'旋转各个共享份,对于数量位于区间$[k_i,k_{i+1})$的共享份进行叠加操作,在恢复第 i 组的任意一幅秘密图像时,恢复图像中每个子像素块包括以下两个区域:

(1) 分享模块$\left(\overline{\overline{\frac{k_2-1}{k_1}}},n\right)$-MVCS,…,$\left(\overline{\overline{\frac{k_i-1}{k_{i-1}}}},n\right)$-MVCS,$\left(\overline{\overline{\frac{k_{i+2}-1}{k_{i+1}}}},n\right)$-MVCS,…,$(k_t,n)$-MVCS 对应的区域.由引理 8 安全性证明中的第(3)种情况可知,子像素块中该区域对应的汉明重量满足 $H^1=H^0$;

(2) 分享模块$\left(\overline{\overline{\frac{k_{i+1}-1}{k_i}}},n\right)$-MVCS 对应的区域.由引理 8 的对比性证明可知,子像素块中该区域对应的汉明重量满足 $H^1>H^0$.

因此,数量位于区间$[k_i,k_{i+1}]$的共享份能够恢复出第 i 组所有的秘密图像,即,满足:

$$H^1(\bigcup\nolimits_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}])>H^0(\bigcup\nolimits_r[\angle\{T_1,T_2,...,T_n\}^{\Phi'}]),k_i\leqslant r<k_{i+1}.$$

定理证毕. □

4 实验分析

表 1 是本文方案与其他多秘密方案的一个综合对比.

Table 1 Comparison of parameters between our scheme and others

表 1 本文方案与其他多秘密方案的参数对比

参数	文献[9]	文献[10]	文献[14]	文献[15]	文献[16]	本文方案
能否完全恢复	否	是	是	是	否	是
存取结构	(k,n)	(k,n)	$(k_1,k_2,\ldots,k_t,n)$	$(k_1,k_2,\ldots,k_t,n)$	$(k_1,k_2,\ldots,k_t,n)$	$(k_1,k_2,\ldots,k_t,n)$
秘密数量	任意	任意	t	t	任意	任意
门限值与秘密数量关系	一对多	一对多	多对一	多对一	多对多	多对多

由图 4 可知,本文方案在秘密图像能够完全恢复的同时,实现了门限值与秘密数量多对多的对应关系,能够进一步满足实际应用需求.

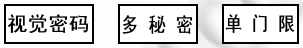


Fig.4 Secret images for verifying the one-to-many relationship

图 4 一对多关系验证实验待分享的秘密图像

为了进一步说明本文方案在完全恢复的条件下门限值与秘密数量关系的有效性和一般性,下面分别从一对多、多对一和多对多的对应关系进行实验验证.需要说明的是:为了更好地呈现实验结果,实验中的图像均为展开的平面图.

(1) 一对多关系

图 5~图 7 分别给出了(2,2),(2,3),(3,3)门限结构下分享 3 幅秘密图像的实验结果.

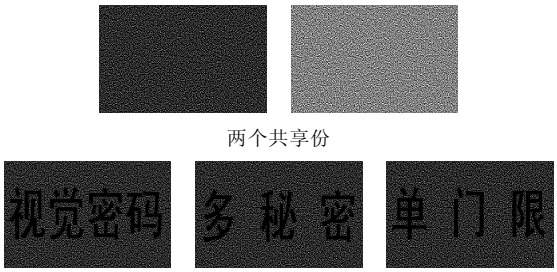


Fig.5 Experimental results of (2,2)-MVCS for three secret images

图 5 (2,2)-MVCS 分享 3 幅秘密图像的实验结果

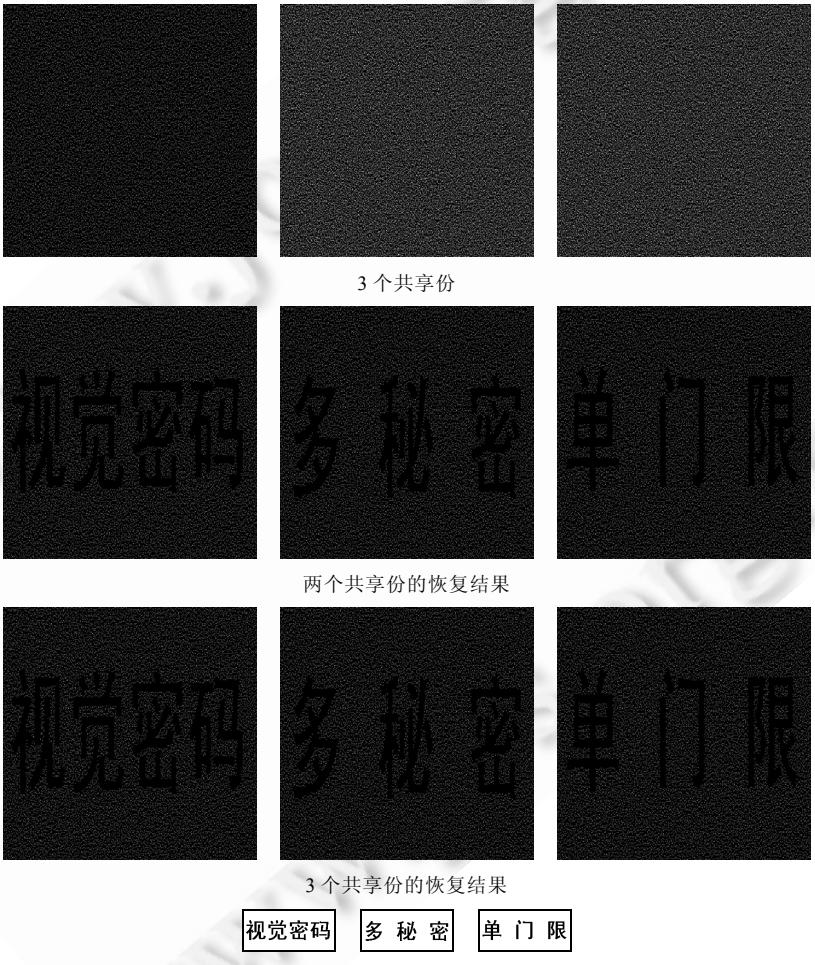


Fig.6 Experimental results of (2,3)-MVCS for three secret images

图 6 (2,3)-MVCS 分享 3 幅秘密图像的实验结果

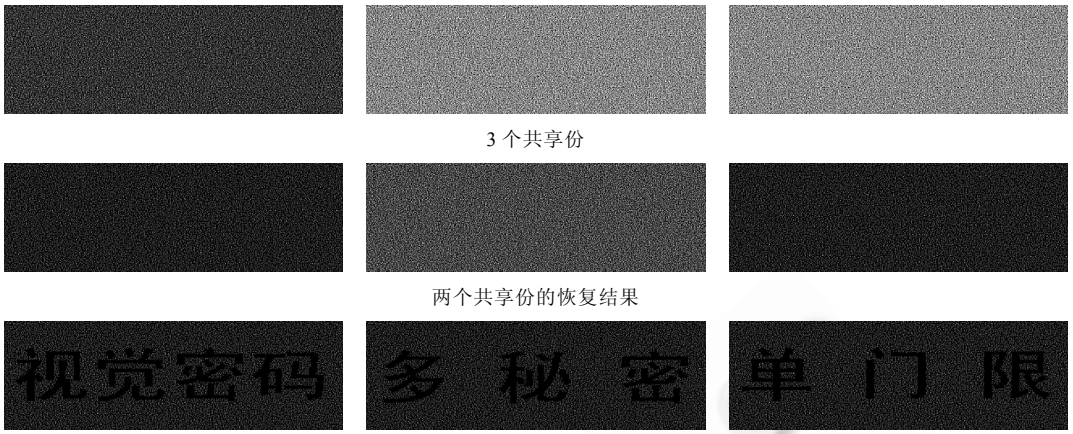


Fig.7 Experimental results of (3,3)-MVCS for three secret images

图 7 (3,3)-MVCS 分享 3 幅秘密图像的实验结果

在图 5 中,(2,2)-VCS 的基矩阵为 $M_0=\begin{bmatrix}1&0\\1&0\end{bmatrix}, M_1=\begin{bmatrix}1&0\\0&1\end{bmatrix}$,依据非规则旋转算法得到 $W=\begin{bmatrix}0&0\\0&1\\0&2\end{bmatrix}$, h=3.因此,

$$S_1'=\bigcup\nolimits_2[\angle\{T_1,T_2\}^{\{0°,0°\}}], S_2'=\bigcup\nolimits_2[\angle\{T_1,T_2\}^{\{0°,120°\}}], S_3'=\bigcup\nolimits_2[\angle\{T_1,T_2\}^{\{0°,240°\}}].$$

在图 6 中,(2,3)-VCS 的基矩阵为 $M_0=\begin{bmatrix}1&1&0\\1&1&0\\1&1&0\end{bmatrix}, M_1=\begin{bmatrix}1&1&0\\1&0&1\\0&1&1\end{bmatrix}$,依据非规则旋转算法得到 $W=\begin{bmatrix}0&0&0\\0&1&2\\0&3&6\end{bmatrix}$, h=7.因此,

$$S_1'=\bigcup\nolimits_2[\angle\{T_1,T_2,T_3\}^{\{0°,0°,0°\}}], S_2'=\bigcup\nolimits_2\left[\angle\{T_1,T_2,T_3\}^{\left\{0°,\frac{1}{7}\times360°,\frac{2}{7}\times360°\right\}}\right], S_3'=\bigcup\nolimits_2\left[T_1,\{T_2\}^{\frac{3}{7}\times360°},\{T_3\}^{\frac{6}{7}\times360°}\right].$$

在图 7 中,(3,3)-VCS 的基矩阵为 $M_0=\begin{bmatrix}0&1&1&0\\0&1&0&1\\0&0&1&1\end{bmatrix}, M_1=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}$,依据非规则旋转算法得到:

$$W=\begin{bmatrix}0&0&0\\0&1&1\\0&2&2\end{bmatrix}, h=3.$$

因此,

$$S_1'=\bigcup\nolimits_3[\angle\{T_1,T_2,T_3\}^{\{0°,0°,0°\}}], S_2'=\bigcup\nolimits_3[\angle\{T_1,T_2,T_3\}^{\{0°,120°,120°\}}], S_3'=\bigcup\nolimits_3[\angle\{T_1,T_2,T_3\}^{\{0°,240°,240°\}}].$$

由图 5~图 7 可得:共享份没有泄露秘密信息,并且数量少于门限值的共享份叠加也无法恢复任何一幅秘密图像;数量达到门限值的共享份按照非规则旋转算法进行旋转后叠加,能够恢复出相应的秘密图像.同时,按照原秘密图像与恢复秘密图像的函数关系 $S=R(S')=\begin{cases}0, & H=m-1\\1, & H=m\end{cases}$,可以得到完全恢复的秘密图像.

(2) 多对一关系

图 8 给出了(2,4,4)-MVCS 分享两幅秘密图像的实验结果.其中,

- $\left(\begin{matrix}3\\=\\2\end{matrix},4\right)$-VCS 的基矩阵为 $G_0^1=\begin{bmatrix}1&1&1&0&0&0\\1&1&0&1&0&0\\1&1&0&0&1&0\\1&1&0&0&0&1\end{bmatrix}, G_1^1=\begin{bmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix}$;
- (4,4)-VCS 的基矩阵为 $G_0^2=\begin{bmatrix}0&1&1&1&0&0&0&1\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{bmatrix}, G_1^2=\begin{bmatrix}1&0&0&0&1&1&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{bmatrix}$.

根据旋转规则融合算法,得到恢复秘密图像的旋转规则为 $\Phi'=\begin{bmatrix}0&0&0\\0&0&0\end{bmatrix}\cdot\frac{360°}{1}$, 即,不旋转.

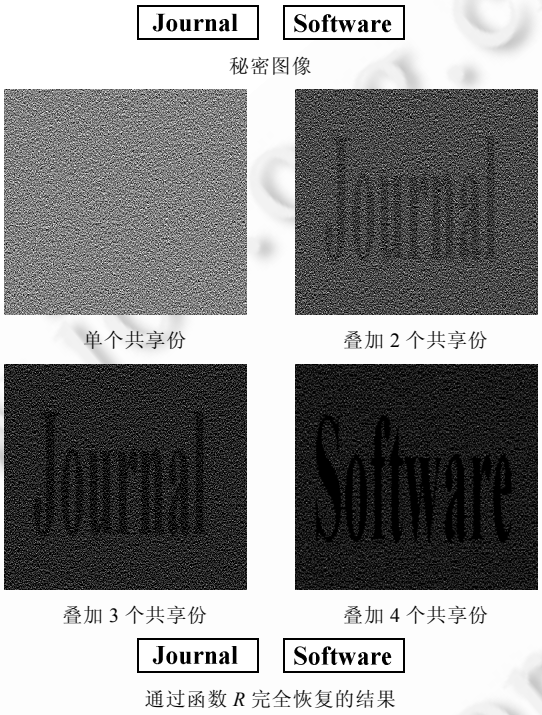


Fig.8 Experimental results of (2,4,4)-MVCS for two secret images

图 8 (2,4,4)-MVCS 分享两幅秘密图像的实验结果

对于本实验,像素扩展度为 14,如果仅在图像宽度上进行扩展,会带来严重的失真.为了减小失真程度,结合秘密图像的大小比例,本实验在宽度上扩展 2 倍,同时在高度上扩展 7 倍,达到了较好的实验效果.

由图 8 可得:单个共享份没有泄露秘密信息;数量达到门限值的共享份叠加,能够恢复出相应的秘密图像.同时,按照下面的函数关系,可以得到完全恢复的秘密图像:

- 对于第 1 幅秘密图像, $S=R(S')=\begin{cases}0, & H=14-4\text{或}14-2\\1, & H=14-3\text{或}14-1\end{cases}$;
- 对于第 2 幅秘密图像, $S=R(S')=\begin{cases}0, & H=14-1\\1, & H=14\end{cases}$.

(3) 多对多关系

图 9 所示为多对多关系验证实验待分享的秘密图像.图 10 给出了(2,3,3)-MVCS 分享两组秘密图像的实验

结果,每组秘密图像各有两幅秘密图像.其中,

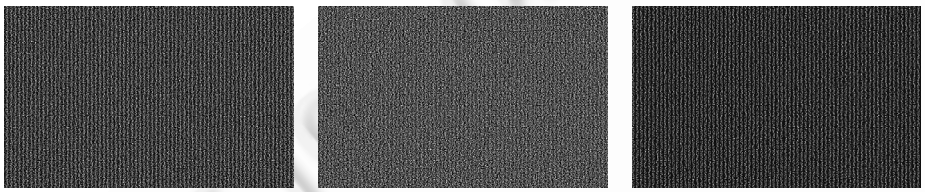
- $\left(\begin{matrix}2\\=\\2\end{matrix},3\right)$-VCS 的基矩阵为 $G_0^1=\begin{bmatrix}1&0&1&0&1&1\\1&0&1&1&1&0\\1&1&1&0&1&0\end{bmatrix}$,$G_1^1=\begin{bmatrix}1&0&1&0&1&1\\0&1&1&1&1&0\\1&1&0&1&0&1\end{bmatrix}$;
- (3,3)-VCS 的基矩阵为 $G_0^2=\begin{bmatrix}0&1&1&0\\0&1&0&1\\0&0&1&1\end{bmatrix}$,$G_1^2=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}$.

根据旋转规则融合算法,得到恢复秘密图像的旋转规则为 $\boldsymbol{\Phi}'=\begin{bmatrix}0&0&0\\0&1&2\end{bmatrix}\cdot\frac{360°}{3}$.

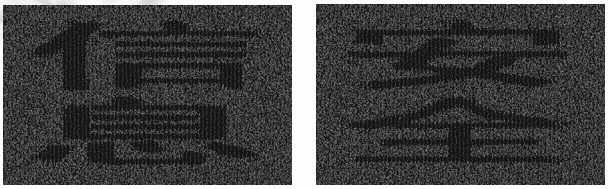
第 1 组秘密图像　　第 2 组秘密图像

Fig.9　Secret images for verifying the many-to-many relationship

图 9　多对多关系验证实验待分享的秘密图像



3 个共享份



两个共享份的恢复结果

3 个共享份的恢复结果

通过函数 R 完全恢复的结果

Fig.10　Experimental results of (2,3,3)-MVCS for two groups of secret images

图 10　(2,3,3)-MVCS 分享两组秘密图像的实验结果

由图 10 可以得到:3 个共享份满足安全性条件;门限值 2 对应恢复出两幅秘密图像,门限值 3 对应恢复出另外两幅秘密图像,满足对比性条件.同时,依据本文方案的构造方法与 $\left(\begin{matrix}2\\=\\2\end{matrix},3\right)$-VCS 和(3,3)-VCS 基矩阵的对比性

能够计算得出:

- 对应于第 1 组秘密图像的 $S=R(S')=\begin{cases}0, & H=30-2\\ 1, & H=30-1\end{cases}$;
- 对应于第 2 组秘密图像的 $S=R(S')=\begin{cases}0, & H=30-1\\ 1, & H=30\end{cases}$.

由此可以实现秘密图像的完全恢复,达到了预期效果.

5 结 论

本文对完全恢复的门限多秘密视觉密码进行了研究,给出了门限多秘密视觉密码可以完全恢复的充分条件,并构造了一种具有一般性的门限多秘密视觉密码方案,完善了完全恢复方案的存取结构,拓展了应用范围.但本文方案的像素扩展度 $m=h'\times\sum_{1}^{t}m_g^i$, 如何在完全恢复条件下使得像素扩展度最小,还有待进一步加以研究.

致谢 在此,我们向对本文的工作给予支持和建议的同行表示诚挚的感谢.

References:

[1] Naor M, Shamir A. Visual cryptography. In: Proc. of the Advances in Cryptology-Eurocrypt'94. LNCS, Berlin: Springer-Verlag, 1995. 1−12. [doi: 10.1007/BFb0053419]

[2] Fu ZX, Yu B. Research on rotation visual cryptography scheme. In: Proc. of the Int'l Symp. on Information Engineering and Electronic Commerce (IEEC 2009). Ternopil: IEEE Computer Society, 2009. 533−536. [doi: 10.1109/IEEC.2009.118]

[3] Shyu SJ, Chen K. Visual multiple secret sharing based upon turning and flipping. Information Sciences, 2011,181(15):3246−3266. [doi: 10.1016/j.ins.2011.02.003]

[4] Wu HC, Chang CC. Sharing visual multi-secrets using circle shares. Computer Standards & Interfaces, 2005,134(28):123−135. [doi: 10.1016/j.csi.2004.12.006]

[5] Shyu SJ, Huang SY, Lee YK, Wang RZ, Chen K. Sharing multiple secrets in visual cryptography. Pattern Recognition, 2007,40(12): 3633−3651. [doi: 10.1016/j.patcog.2007.03.012]

[6] Hsu HC, Chen TS, Lin YH. The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing. In: Proc. of the IEEE IEEE Int'l Conf. on Networking, Sensing & Control (ICNSC 2004). IEEE Computer Society, 2004. 996−1001. [doi: 10.1109/ICNSC.2004.1297083]

[7] Feng JB, Wu HC, Tsai CS, Chang YF, Chu YP. Visual secret sharing for multiple secrets. Pattern Recognition, 2008,41(12): 3572−3581. [doi: 10.1016/j.patcog.2008.05.031]

[8] Fu ZX, Yu B, Fang LG. The multi-secret visual cryptography based on ring shares. Journal of Electronics & Information Technology, 2010,32(4):880−883 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2009.00410]

[9] Yang CN, Chung TH. A general multi-secret visual cryptography scheme. Optics Communications, 2010,283(24):4949−4962. [doi: 10.1016/j.optcom.2010.07.051]

[10] Yu B, Shen G. Multi-Secret visual cryptography with deterministic contrast. Multimedia Tools and Applications, 2014,72(2): 1867−1886. [doi: 10.1007/s11042-013-1479-8]

[11] Katoh T, Imai H. Some visual secret sharing schemes and their share size. In: Proc. of the Int'l Conf. on Cryptology and Information Security, Joint Conf. of '96 Int'l Computer Symp. 1996. 41−47. http://cttir.lib.fcu.edu.tw/FCUWeb/wSite/ct?ctNode=289&mp=1&xItem=28552&doId=0000017107

[12] Yu B, Xu XH, Fang LG. Multi-Secret sharing threshold visual cryptography scheme. In: Wang YP, Zhang QF, Liu HL, eds. Proc. of the Int'l Conf. on Computational Intelligence and Security. Harbin: IEEE Computer Society, 2007. 815−818. [doi: 10.1109/CISW.2007.4425620]

[13] Qiao MQ, Zhu YD, Liu HP. Multi-Secret sharing visual cryptography and its application to cheater detection. Natural Sciences Journal of Harbin Normal University, 2007,23(2):61−65 (in Chinese with English abstract).

[14] Yu B, Fu ZX, Fang LG. A modified multi-secret sharing visual cryptography scheme. In: Proc. of the 2008 Int'l Conf. on Computational Intelligence and Security Workshop. Suzhou: IEEE Computer Society, 2008. 351−354. [doi: 10.1109/CIS.2008.120]

[15] Shyu SJ, Jiang HW. General constructions for threshold multiple-secret visual cryptographic schemes. IEEE Trans. on Information Forensics and Security, 2013,8(5):733−743. [doi: 10.1109/TIFS.2013.2250432]

[16] Fu ZX, Yu B, Fang LG. A new multi-secret sharing visual cryptography. Acta Electronica Sinica, 2011,39(3):714−718 (in Chinese with English abstract).

附中文参考文献:

[8] 付正欣,郁滨,房礼国.基于环形共享份的多秘密视觉密码.电子与信息学报,2010,32(4):880−883. [doi: 10.3724/SP.J.1146.2009.00410]

[13] 乔明秋,朱悦冬,刘焕平.多秘密共享可视密码及在防止欺骗上的应用.哈尔滨师范大学自然科学学报,2007,23(2):61−65.

[16] 付正欣,郁滨,房礼国.一种新的多秘密分享视觉密码.电子学报,2011,39(3):714−718.

付正欣(1986－),男,山东曹县人,博士,讲师,主要研究领域为视觉密码.

李斌(1962－),男,高级工程师,主要研究领域为信息安全.

沈刚(1986－),男,博士生,主要研究领域为视觉密码.

郁滨(1964－),男,博士,教授,博士生导师,主要研究领域为信息安全,视觉密码.