一种无损多秘密分享视觉密码方案

郁 滨 沈 刚* 付正欣
(信息工程大学 郑州 450004)

摘 要：针对分享多幅秘密图像存在信息损失的问题，该文给出(n, n)无损多秘密分享视觉密码的定义，在此基础上基于环状共享份设计了一种(n, n)多秘密视觉密码方案，使秘密图像的信息损失为零。实验结果表明，该方案不仅实现了在多个参与者之间分享多幅秘密图像，而且秘密图像能够完全恢复。

关键词：视觉密码；多秘密；无损；完全恢复
中图分类号：TP309.7 **文献标识码**： A **文章编号**：1009-5896(2012)12-2885-06
DOI: 10.3724/SP.J.1146.2012.00300

A Lossless Multi-secret Sharing Visual Cryptography Scheme

Yu Bin Shen Gang Fu Zheng-xin
(*Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: Considering the information loss during sharing multiple secrets, a definition of (n, n) lossless multi-secret sharing visual cryptography is proposed. In addition, based on ring shares, an (n, n) multi-secret visual cryptography scheme, which shares secret images with no information loss, is designed. The experimental results show that in this scheme, not only multiple participants can share multiple secret images, but also secret images can be reconstructed perfectly.

Key words: Visual cryptography; Multi-secret; Lossless; Perfect reconstruction

1 引言

与单秘密视觉密码方案[1–3] (Visual Cryptography Schemes, VCS)不同，多秘密视觉密码方案(Multi-secret Visual Cryptography Schemes, MVCS)不仅使参与者在分享多幅秘密图像时保存一个共享份，减小了管理共享份的难度，而且满足实际应用需求，扩展了视觉密码的应用领域。

为了有效解决多幅图像的分享问题，Lin 等人[4]基于概率模型提出一种像素不扩展的(2, 2)-MVCS，叠加两个矩形共享份恢复第 1 幅秘密图像，翻转一个共享份再与另一个共享份叠加则得到第 2 幅秘密图像，相对差小于 1/6。Lee 等人[5]提出一种混合加密算法，在像素不扩展的条件下使相对差达到 43%左右，同时黑像素得到了完全恢复。Yang 等人[6]基于环状共享份提出了一种(k, n)-MVCS，在门限结构的基础上可以实现任意数量秘密图像的分享。另外，付正欣等人[7]结合区域标记和单秘密视觉密码的基矩阵，提出了一种基于通用存取结构的 MVCS。在上述方案中，原图像黑像素对应子像素块的汉明重量以一定的概率大于白像素对应子像素块的汉明重量，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。

为了解决信息损失的问题，Wu 等人[8]提出了一种(2, 2)-MVCS，在两个矩形共享份之间分享两幅秘密图像，像素扩展度为 4，相对差为 1/4。Shyu 等人[9]采用翻转操作，利用相关块构造的思想，实现了在两个矩形共享份之间分享多幅秘密图像。

由于矩形共享份在旋转或翻转操作中存在角度限制的问题，Wu 等人[10]提出了一种将共享份做成圆盘形状的方案，可以以任意的角度旋转共享份，实现了两幅秘密图像的分享。在此基础上，Shyu 等人[11]提出了一种基于圆盘状共享份的方案，能够在两个共享份之间分享任意数量的秘密图像，但恢复的秘密图像在形状上有失真。

Hsu 等人[12]将矩形共享份首尾相接做成环状，使共享份 T_2 旋转 0° 到 360° 的任意角度即可恢复秘密，虽然克服了旋转角度的限制和外形的失真，但仍只能分享两幅秘密图像。在环状共享份的基础上，Feng 等人[13]通过设计 4 种不同的视觉模式，实现了 t 幅秘密图像的分享，但其像素扩展度为 $3t$，相对差为 $1/(3t)$。付正欣等人[14]通过对秘密图像和环状共享份进行纵向区域分割，设计了一种(2,

2012-03-23 收到，2012-10-17 改回
国家自然科学基金(61070086)资助课题
*通信作者：沈刚 shenqi0123@163.com

2)-MVCS，不仅实现了 t 幅秘密图像的分享，而且将像素扩展度减小为 $2t$，相对差为 $1/(2t)$。

在上述方案中，原图像黑像素对应子像素块的汉明重量大于白像素对应子像素块的汉明重量，没有损失原秘密图像的信息，但其存取结构仅局限于(2, 2)门限结构，不适用于多个参与者。

针对上述问题，本文给出(n, n)无损多秘密分享视觉密码的定义，并结合(n, n)-VCS 的基矩阵，设计了(n, n)-MVCS 无损分享算法，最后对方案的有效性进行了理论证明和实验验证。

2 基本概念

设 n 个参与者分享 t 幅秘密图像，秘密图像为 S_i, i=1, 2,⋯, t，共享份为 T_j, j=1, 2,⋯, n，通过叠加操作恢复的秘密图像为 S_i'，像素扩展度为 m, $\bigcup_r[\bullet]$ 表示对任意 r 个共享份的叠加操作，$0<r\le n-1$，$H^1(H^0)$表示原秘密图像的黑(白)像素对应恢复图像的子像素块的汉明重量。

定义 1[6] 在恢复秘密图像 S_i 时每个共享份的旋转角度所组成的角度集合记为 Θ_i，$\Theta_i=\{(i-1)\cdot(j-1)\theta|j=1,2,\cdots,n\}$，其中 $(i-1)(j-1)\theta$ 表示在恢复秘密图像 S_i 时共享份 T_j 的旋转角度，$1\le i\le t$，$\theta=360^\circ/(t(n-1))$。

定义 2[6] n 个共享份按照 Θ_i 进行旋转操作记为 $\angle\{T_1,\cdots,T_j,\cdots,T_n\}^{\Theta_i}$，$\angle\{T_1,\cdots,T_j,\cdots,T_n\}^{\Theta_i}=\{\{T_j\}^{(i-1)(j-1)\theta}|j=1,2,\cdots,n\}$，其中 $\{T_j\}^{(i-1)(j-1)\theta}$ 表示在恢复秘密图像 S_i 时对共享份 T_j 顺时针旋转 $(i-1)\cdot(j-1)\theta$ 度，$1\le i\le t$。

比如 3 个参与者分享 3 幅秘密图像，每个共享份的旋转角度具体如图 1 所示。

定义 3 称一个多秘密视觉密码方案为(n, n)多秘密视觉密码，若方案满足以下条件：

(1)少于 n 个共享份无法恢复出任何一幅秘密图像，数学表示为

$$H^1\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right)=H^0\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right),\quad 0<r\le n-1,\ 0^\circ\le\varphi_j\le 360^\circ$$

(2)按照共享份旋转角度集合来旋转 n 个共享份，叠加后可以恢复出相应的秘密图像，数学表示为

$$H^1\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)\ge m-l_i$$
$$H^0\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)\le m-h_i$$
$$0\le l_i<h_i\le m$$

第(1)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。第(2)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可以通过视觉系统恢复出相应的秘密图像，并且对于不同的秘密图像，区分黑白像素的门限值可以不同。

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，满足 $S=R(S')$，则称该视觉密码方案是无损的，其秘密分享算法是无损分享算法。

在该方案中，经过无损分享算法得到的共享份叠加恢复的秘密图像存在像素扩展和对比度失真，但可以通过函数 R 从恢复的秘密图像中提取出原秘密图像的所有信息，亦即可以完全恢复出原秘密图像。

定理 1 对于一个(n, n)多秘密视觉密码方案，若其对比性条件为

$$H^1\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)=m-l_0$$
$$H^0\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)=m-h_0$$
$$0\le l_0<h_0\le m$$

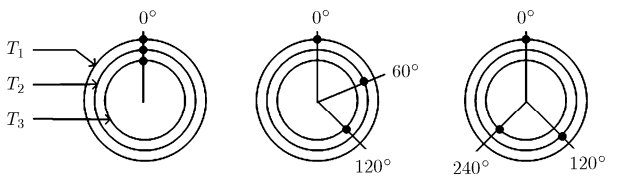
则该方案是无损的。

证明 由上述对比性条件可知，所有原秘密图像的黑(白)像素与恢复的秘密图像相关的 m 个子像素存在相同的对应关系，即黑像素对应 $m-l_0$ 个“1”和 l_0 个“0”，白像素对应 $m-h_0$ 个“1”和 h_0 个“0”，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，将 R_i 统一记为 R，其表达式为

$$S_i=R\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)=\begin{cases}0, & H=m-h_0\\ 1, & H=m-l_0\end{cases}$$

其中 H 为原秘密图像的像素对应恢复图像的子像素块的汉明重量。 证毕

由上式可知，函数 R 实际上是在叠加操作基础上增加了判断操作，计算复杂度没有增加，另外，随着科学技术的发展，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 提供了一种有效途径。因此符合定理 1 的(n, n)多秘密视觉密码方案在不违背视觉密码秘密恢复简单性的条件下可以实现秘密图像的完全恢复。



(a)$\angle\{T_1,T_2,T_3\}^{\{0^\circ,0^\circ,0^\circ\}}$ (b)$\angle\{T_1,T_2,T_3\}^{\{0^\circ,60^\circ,120^\circ\}}$ (c)$\angle\{T_1,T_2,T_3\}^{\{0^\circ,120^\circ,240^\circ\}}$

图 1 3 个参与者分享 3 幅秘密图像的旋转示例

3　方案设计

本节在(n,n)-VCS 基矩阵的基础上，结合共享份旋转操作，设计了一种符合定义 4 的 MVCS 构造方法，其中 $S=R(S')=\begin{cases}0, & H=m-1\\ 1, & H=m\end{cases}$。

3.1 秘密图像的子集划分

设 t幅秘密图像的大小均为 $X\times Y$, Y能被 $t(n–1)$整除，n 个共享份均由 $X\times Y$ 个子像素块组成，(n, n)-VCS 的基矩阵记为 $\boldsymbol{C}_0$和 $\boldsymbol{C}_1$，其中 $\boldsymbol{C}_0$由所有的 n 维偶数列组成，$\boldsymbol{C}_1$由所有的 n 维奇数列组成，共有 $m_c=2^{n-1}$列。为了便于设计，本文将所有的秘密图像进行子集划分，如图 2 所示，每行像素分为 $Y/(t(n–1))$个子集，每个子集包含 $t(n–1)$个像素。

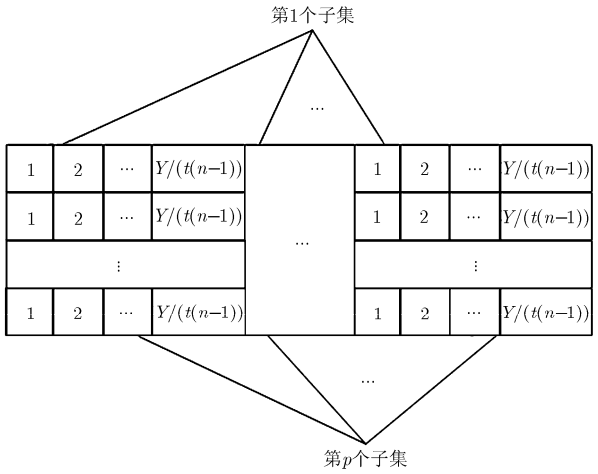


图 2 秘密图像划分子集示意图

其中，秘密图像 S_i第 q 行第 p 个子集中第 l 个像素记为 $S_i(q,p,l), i\in[1,t]$, $q\in[1,X]$, $p\in[1,Y/t(n-1)]$, $l\in[1,t(n-1)]$。$S_i(q, p, l)$对应第 j 个共享份的子像素块记为 T_j^{qpl}，大小为 $t(n–1)\times m_c$，由 $t(n–1)$行组成，每行记为 $T_j^{qpl}(l,:)$。而子像素块的具体构造如图 3 所示。

3.2 方案流程

结合环形共享份的优点，本文以秘密图像每行中的每个子集为加密单位，通过(n, n)-VCS 的基矩阵和共享份的旋转操作实现了MVCS的无损分享算法。具体地，在秘密分享时，首先对秘密图像划分子集，然后针对每个子集，结合(n, n)-VCS 的基矩阵，利用子集分享算法对共享份进行赋值，秘密分享的流程如图 4 所示。

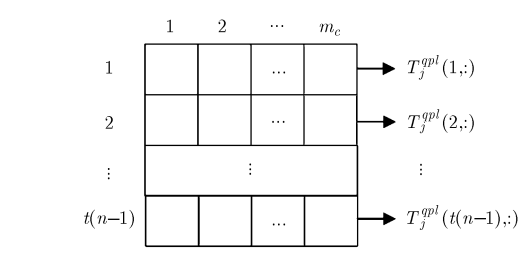


图 3 子像素块构造示意图

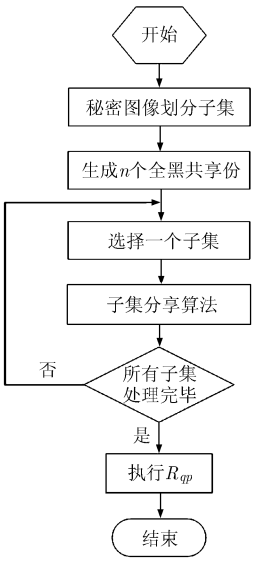


图 4 秘密分享流程图

子集分享算法在秘密分享流程中极为重要，其保证了多幅秘密图像的无损分享，具体算法如下：

步骤 1　对 $\boldsymbol{C}_0$和 $\boldsymbol{C}_1$进行随机列变换；

步骤 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 $T_j^{qpl}(l,:)=\boldsymbol{C}_1(j,:)$，否则$T_j^{qpl}(l,:)=\boldsymbol{C}_0(j,:)$；

步骤 3　对于第 p 个子集，依次处理第 i 幅秘密图像每行中的每个像素，i=2,3,…,t，若 $S_i(q,p,l)$=1，则 $T_j^{qp(((i-1)(j-1)+l-1)\bmod(t(n-1))+1)}(l,:)=T_j^{qpl}(l,:)$, j=2, 3,…,n–1, $T_n^{qp(((i-1)(j-1)+l-1)\bmod(t(n-1))+1)}(l,:)=\sim T_n^{qpl}(l,:)$，否则 $T_j^{qp(((i-1)(j-1)+l-1)\bmod(t(n-1))+1)}(l,:)=T_j^{qpl}(l,:)$, j=2,3, …,n;

步骤 4　输出 T_j，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同一组基矩阵 $\boldsymbol{C}_0$和 $\boldsymbol{C}_1$来进行分享，因此为了保证安全性，在整个秘密分享流程结束时，需要执行 R_{qp}，其为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 $t(n–1)\times m_c$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 5 所示。

秘密恢复的过程则非常简单，在恢复秘密图像 S_i时，n 个参与者只需按照相应的旋转角度集合Θ_i来旋转共享份并叠加即可，如图 6 所示。

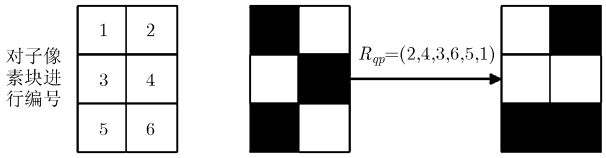


图 5 (2, 2)-MVCS 分享 3 幅秘密图像的随机置换举例

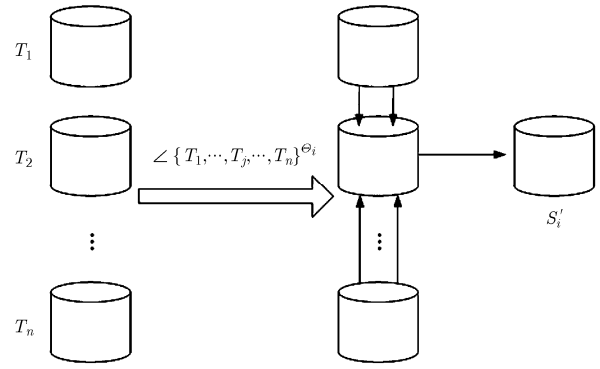


图 6 秘密恢复示意图

4 方案分析

本方案需要在安全性和对比性两个方面进行证明，证明其满足定义 3 的安全性条件和定理 1 的对比性条件。

引理 1 设 $P(C_i)$ 表示由 C_i 经过所有可能的列变换所组成的矩阵集合，$B_0 \in P(\boldsymbol{C}_0)$，$B_1 \in P(\boldsymbol{C}_1)$，若 B_0 和 B_1 的任意一行取反，记为 $B_0^{'}$ 和 $B_1^{'}$，则 $B_0^{'} \in P(\boldsymbol{C}_1)$，$B_1^{'} \in P(\boldsymbol{C}_0)$。

证明 B_0 是由所有的 n 维偶数列组成，$B_0=[b_1^0,b_2^0,\cdots,b_{2^{n-1}}^0]$，设 b_i^0，b_j^0 为 n 维偶数列，$b_i^0 \neq b_j^0$，不妨设第 n 行取反，当 $b_i^0(n)$ 由 0 变 1 时，b_i^0 中 1 的个数增加 1，当 $b_i^0(n)$ 由 1 变 0 时，b_i^0 中 1 的个数减少 1，无论 1 的个数增加还是减少 1，b_i^0 变为 n 维奇数列，同样 b_j^0 也变为 n 维奇数列，并且 $b_i^0 \neq b_j^0$。因此，$B_0^{'}$ 变为由所有的 n 维奇数列组成，即 $B_0^{'} \in P(\boldsymbol{C}_1)$，同理，$B_1^{'}$ 也变为由所有的 n 维奇数列组成，即 $B_1^{'} \in P(\boldsymbol{C}_0)$。 证毕

定理 2 少于 n 个共享份无法恢复出任何一幅秘密图像，数学表示为

$$H^1\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right)$$
$$=H^0\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right),$$
$$0<r\leq n-1,\ 0^\circ\leq\varphi_j\leq 360^\circ$$

证明 对于 $\bigcup_r[\{T_1^{qpl}\}^{\varphi_1},\cdots,\{T_j^{qpl}\}^{\varphi_j},\cdots,\{T_n^{qpl}\}^{\varphi_n}]$，根据子集分享算法和引理 1 可得 r 个子像素块的叠加包括以下两种情况。

(1)r 个子像素块对应的行含有全 1 行。对于任意 $S_i(q,p,l)$，

$$H^0\left(\bigcup_r\left[\{T_1^{qpl}(l,:)\}^{\varphi_1},\cdots,\{T_j^{qpl}(l,:)\}^{\varphi_j},\cdots,\{T_n^{qpl}(l,:)\}^{\varphi_n}\right]\right)=H^1\left(\bigcup_r\left[\{T_1^{qpl}(l,:)\}^{\varphi_1},\cdots,\{T_j^{qpl}(l,:)\}^{\varphi_j},\cdots,\{T_n^{qpl}(l,:)\}^{\varphi_n}\right]\right)=m_c$$

(2)r 个子像素块对应的行组成$(n,\ n)$-VCS 基矩阵的 r 行。对于任意 $S_i(q,\ p,\ l)$，

$$H^0\left(\bigcup_r\left[\{T_1^{qpl}(l,:)\}^{\varphi_1},\cdots,\{T_j^{qpl}(l,:)\}^{\varphi_j},\cdots,\{T_n^{qpl}(l,:)\}^{\varphi_n}\right]\right)=H^1\left(\bigcup_r\left[\{T_1^{qpl}(l,:)\}^{\varphi_1},\cdots,\{T_j^{qpl}(l,:)\}^{\varphi_j},\cdots,\{T_n^{qpl}(l,:)\}^{\varphi_n}\right]\right)=\frac{m_c}{2}+r-1$$

综上，对于任意 $S_i(q,\ p,\ l)$，

$$H^1\left(\bigcup_r\left[\{T_1^{qpl}\}^{\varphi_1},\cdots,\{T_j^{qpl}\}^{\varphi_j},\cdots,\{T_n^{qpl}\}^{\varphi_n}\right]\right)=H^0\left(\bigcup_r\left[\{T_1^{qpl}\}^{\varphi_1},\cdots,\{T_j^{qpl}\}^{\varphi_j},\cdots,\{T_n^{qpl}\}^{\varphi_n}\right]\right)$$

因此，

$$H^1\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right)=H^0\left(\bigcup_r\left[\{T_1\}^{\varphi_1},\{T_2\}^{\varphi_2},\cdots,\{T_j\}^{\varphi_j},\cdots,\{T_n\}^{\varphi_n}\right]\right)$$

证毕

定理 3 按照旋转角度集合来旋转 n 个共享份，叠加后满足

$$H^1\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)=t(n-1)m_c$$
$$H^0\left(\bigcup_n\left[\angle\{T_1,T_2,\cdots,T_n\}^{\Theta_i}\right]\right)=t(n-1)m_c-1$$

证明 由子集分享算法和引理 1 可知，当 $S_i(q,p,l)=1(0)$时，

$$T_1^{qpl}(l,:),\cdots,T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)}(l,:),\cdots,T_n^{qp(((i-1)(n-1)+l-1)\bmod t(n-1)+1)}(l,:)$$

共同组成了$(n,\ n)$-VCS 的基矩阵 $\boldsymbol{C}_1(\boldsymbol{C}_0)$。因此，

$$H^1\left(\bigcup_n\left[T_1^{qpl}(l,:),\cdots,T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)}(l,:),\cdots,T_n^{qp(((i-1)(n-1)+l-1)\bmod t(n-1)+1)}(l,:)\right]\right)=m_c$$

$$H^0\left(\bigcup_n\left[T_1^{qpl}(l,:),\cdots,T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)}(l,:),\cdots,T_n^{qp(((i-1)(n-1)+l-1)\bmod t(n-1)+1)}(l,:)\right]\right)=m_c-1$$

又 $T_1^{qpl}(z,:)=\underbrace{11\cdots1}_{m_c}$，$z\in[1,t(n-1)]$，$z\neq l$，因而，

$$H^1\left(\bigcup_n\left[T_1^{qpl},\cdots,T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)},\cdots,T_n^{qp(((i-1)(n-1)+l-1)\bmod t(n-1)+1)}\right]\right)=t(n-1)m_c$$

$$H^0\left(\bigcup_n\left[T_1^{qpl},\cdots,T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)},\cdots,T_n^{qp(((i-1)(n-1)+l-1)\bmod t(n-1)+1)}\right]\right)=t(n-1)m_c-1$$

由共享份的旋转方法可知，$T_j^{qp(((i-1)(j-1)+l-1)\bmod t(n-1)+1)}$ 表示将 T_j^{qpl} 旋转 $(i-1)(j-1)\theta$，记为 $\{T_j^{qpl}\}^{(i-1)(j-1)\theta}$，

因此对于任意 $S_i(q,p,l)$，$H^1(\cup_n[\angle\{T_1,\cdots,T_j,\cdots,T_n\}^{\Theta_i}]) = t(n-1)m_c$，$H^0(\cup_n[\angle\{T_1,\cdots,T_j,\cdots,T_n\}^{\Theta_i}]) = t(n-1)m_c - 1$。证毕

5　实验及结果分析

由于无损多秘密分享视觉密码方案能够实现秘密图像的完全恢复，因此在评价方案优劣时，不需要考虑方案的相对差，只需比较像素扩展度即可。在本方案中，原图像的一个像素对应恢复后的 $t(n-1)\times m_c$ 个像素，即像素扩展度为 $t(n-1)\times m_c$，m_c 为 (n, n)-VCS 的像素扩展度。表 1 是本方案与其他多秘密方案的一个综合对比，其中 m_v 为 (k, n)-VCS 的像素扩展度。

需要说明的是，在无损多秘密分享方案中，文献[14]的像素扩展度小于文献[13]，但当 n=2 时，本方案与文献[14]在参数上是相同的，因此文献[14]是本方案的一个特殊情况。

下面以 3 个共享份分享 3 幅秘密图像为例，对本文方案进行验证并与文献[6]在恢复结果上进行比较。图 7 给出了待分享的秘密图像，图 8 则包括本方案 3 个共享份的平面图和恢复结果以及文献[6]的恢复结果。

由图 8 可得：3 个共享份没有泄露秘密信息，并且任意两个共享份叠加也无法恢复任何一幅秘密图像，即定理 3; 3 个共享份按照设定的旋转角度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 $S=R(S')$

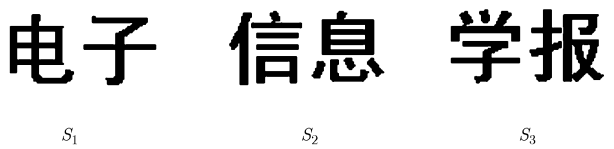


图 7 3 幅秘密图像

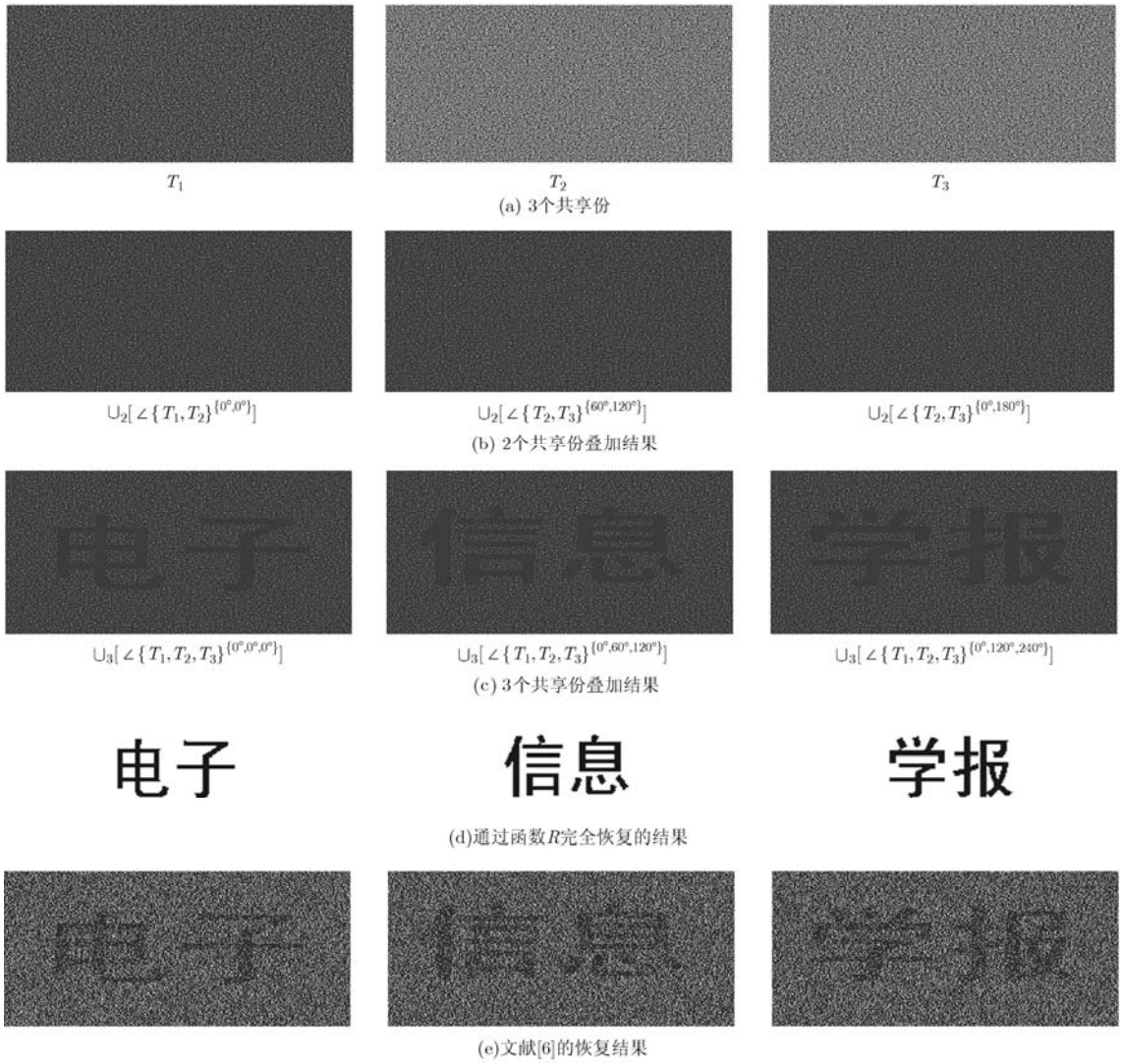


图 8 共享份及恢复结果

表 1 本文方案与其他多秘密方案的比较

参数	文献[5]	文献[6]	文献[13]	文献[14]	本文方案
是否无损	否	否	是	是	是
存取结构	(2, 2)	(k, n)	(2, 2)	(2, 2)	(n, n)
像素扩展度	1	$t\times m_v$	$3t$	$2t$	$t(n-1)\times m_c$
秘密数量	2	t	t	t	t

$=\begin{cases}0, & H=m-1\\ 1, & H=m\end{cases}$，可以得到完全恢复的秘密图像，即定理 4 和定理 1；文献[6]的恢复结果虽然整体上呈现秘密图像，但在图像细节上存在信息的损失，文献[6]所提出的方案是有损的。

6 结束语

本文设计了一种(n,n)多秘密视觉密码方案，可以在多个环状共享份之间无损分享任意数量的秘密信息。与其他多秘密方案不同，本文方案在不违背视觉密码恢复简单的条件下，可以通过叠加恢复后的秘密图像得到完全恢复的秘密图像。如何将无损多秘密分享视觉密码方案扩展到(k,n)门限结构有待进一步研究。

参 考 文 献

[1] Naor M and Shamir A. Visual cryptography[C]. Advances in Cryptology-Eurocrypt'94, Berlin, 1995, LNCS 950: 1–12.

[2] Ateniese G, Blundo C, De Santis A, *et al*.. Visual cryptography for general access structures[J]. *Information and Computation*, 1996, 129(2): 86–106.

[3] Fang Li-guo and Yu Bin. Research on pixel expansion of (2, n) visual threshold scheme[C]. 1st International Symposium on Pervasive Computing and Applications Proceedings (SPCA06), Ningbo, 2006: 856–860.

[4] Lin S J, Chen S K, and Lin J C. Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion[J]. *Journal of Visual Communication & Image Representation*, 2010, 21(8): 900–916.

[5] Lee K H and Chiu P L. A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images[J]. *Optics Communications*, 2011, 284(12): 2730–2741.

[6] Yang C N and Chung T H. A general multi-secret visual cryptography scheme[J]. *Optics Communications*, 2010, 283(24): 4949–4962.

[7] 付正欣, 郁滨, 房礼国. 一种新的多秘密分享视觉密码[J]. 电子学报, 2011, 39(3): 714–718.
Fu Zheng-xin, Yu Bin and Fang Li-guo. A new multi-secret sharing visual cryptography[J]. *Acta Electronica Sinica*, 2011, 39(3): 714–718.

[8] Wu C C and Chen L H. A study on visual cryptography[D]. [Master dissertation], National Chiao Tung University, Taipei, 1998.

[9] Shyu S J and Chen K. Visual multiple secret sharing based upon turning and flipping[J]. *Information Sciences*, 2011, 181(15): 3246–3266.

[10] Wu H C and Chang C C. Sharing visual multi-secrets using circle shares[J]. *Computer Standards & Interfaces*, 2005, 134(28): 123–135.

[11] Shyu S J, Huang S, Lee Y, *et al*.. Sharing multiple secrets in visual cryptography[J]. *Pattern Recognition*, 2007, 40(12): 3633–3651.

[12] Hsu H C, Chen T S, and Lin Y H. The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing[C]. Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, 2004: 996–1001.

[13] Feng J B, Wu H C, Tsaic C S, *et al*.. Visual secret sharing for multiple secrets[J]. *Pattern Recognition*, 2008, 41(12): 3572–3581.

[14] 付正欣, 郁滨, 房礼国. 基于环形共享份的多秘密视觉密码[J]. 电子与信息学报, 2010, 32(4): 880–883.
Fu Zheng-xin, Yu Bin, and Fang Li-guo. The multi-secret visual cryptography based on ring shares[J]. *Journal of Electronics & Information Technology*, 2010, 32(4): 880–883.

郁 滨： 男，1964年生，教授，博士生导师，主要研究方向为视觉密码和网络安全.

沈 刚： 男，1986年生，硕士生，研究方向为视觉密码.

付正欣： 男，1986年生，博士生，研究方向为视觉密码.