基于压缩算法的存取式多秘密视觉密码

付正欣* 郁 滨 房礼国
(信息工程大学 郑州 450004)

摘 要：依据多幅秘密图像的像素组合与基矩阵之间的映射关系，该文分析了目前存取式多秘密视觉密码存在的冗余基矩阵问题，提出了一种减小基矩阵规模的压缩算法。该算法以一列像素为处理单元，且满足秘密图像的整体对比性。在此基础上，设计了新的存取式多秘密视觉密码的秘密分享与恢复流程。与现有的方案相比，该方案能够有效减小共享份的尺寸，且对于简单图像的压缩效果更加明显。

关键词：视觉密码；多秘密；存取式；冗余基矩阵；压缩算法
中图分类号：TP309.7 **文献标识码**： A **文章编号**：1009-5896(2013)05-1055-08
DOI: 10.3724/SP.J.1146.2012.00415

The Access-based Multi-secret Visual Cryptography with Compression Algorithm

Fu Zheng-xin Yu Bin Fang Li-guo
(*Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: According to the mapping relationship between the multiple secret images' pixel combinations and the basis matrices, the redundant basis matrices are analyzed in the access-based multi-secret visual cryptography. A compression algorithm is proposed to decrease the size of basis matrices. The algorithm takes one column pixels as disposal unit, and satisfies the entire contrast of secret images. Based on the algorithm, new secret sharing and recovering procedures are designed for the access-based multi-secret visual cryptography. Compared with previous schemes, the present scheme can diminish the size of shares effectively, and the compression effects are obvious for the simple images.

Key words: Visual cryptography; Multiple secrets; Access-based; Redundant basis matrices; Compression algorithm

1 引言

视觉密码[1](visual cryptography)是秘密共享[2,3](secret sharing)的一个分支，主要解决图像信息的分享与恢复问题，其命名源于通过视觉系统完成秘密图像的恢复。视觉密码因其独特的恢复运算，引起了学者的广泛关注。经过近 20 年的发展，视觉密码在理论完善[4−6]、方案优化[7−9]和方案应用[10−12]方面取得了长足的进展。

多秘密视觉密码(Multi-secret sharing Visual Cryptography Scheme, MVCS)是视觉密码的一个重要研究内容。MVCS 通过共享份集合或叠加方式的变化，实现了每个参与者仅需保存一个共享份，即可恢复多个秘密。通过对图像集合分配不同的职责，MVCS 可以应用于信息的分级管理、共享份的身份认证等方面，有效地扩展了视觉密码的应用领域。目前，MVCS 主要包括存取式(Access-based MVCS, AMVCS) 和操作式 (Operation-based MVCS, OMVCS)[13−15]两类。

在 AMVCS 中，各秘密图像的授权集合之间不存在交集。在恢复秘密图像时，需要根据对应的授权集合叠加相应的共享份。Droste[16]提出了一种 *S*-Extended 视觉密码方案，每个共享份均是有意义的图像，叠加所有共享份可以恢复秘密图像。*S*-Extended 方案其本质是一种特殊的 AMVCS，每个共享份均可以恢复遮盖图像，所有共享份恢复秘密图像。Katoh 等人[17]设计了 3 个参与者分享两幅图像的 AMVCS，其中 2 个参与者分享秘密图像 S_1，3 个参与者分享另一个图像 S_2，在参与者和秘密图像数量上均有待提高。Yu 等人[18]将 AMVCS 扩展至 n 个参与者，所有 k 个参与者的集合分享一个秘密图像 S_0，而所有 $k-1$ 个参与者的集合分享 $\binom{n}{k-1}$ 个秘密图像 $S_i, 1 \le i \le \binom{n}{k-1}$，有效提高了参与者和秘

2012-04-12 收到，2013-03-18 改回
国家自然科学基金(61070086)资助课题
*通信作者：付正欣 fzx2515@163.com

密图像的数量提高。Fu 等人[19]设计了一种$(k_1,k_2,\cdots,k_h,n)$的 AMVCS, n 个参与者中的任意 k_i 个能恢复密图 $S_i(1\le i\le h)$，增加了恢复图像的参与者组合方式。文献[20]讨论了通用存取结构下的 AMVCS，突破了门限结构的限制，使参与者可以任意组合成授权子集。

尽管以上 AMVCS 在存取结构上有所区别，但其在基矩阵构造和算法设计方面却是类似的。首先将多个单秘密方案的基矩阵进行交叉连接组成 AMVCS 的基矩阵，然后以各秘密图像在相同位置的像素组合为单位完成分享流程。事实上，AMVCS 的设计不应简单地归结于单秘密方案的扩展，而需要依据多幅图像的像素组合确定对应的基矩阵集合。

本文从 AMVCS 中的像素组合与基矩阵之间的关系入手，研究了逐点分享算法存在的冗余基矩阵问题，提出了一种减小基矩阵规模的压缩算法，设计了以秘密图像的列组合为单位的秘密分享流程。实验结果表明，本文压缩算法能够有效减小 AMVCS 的共享份存储空间。

2 基本概念

2.1 AMVCS 定义

AMVCS 以单秘密视觉密码方案为基础，首先给出单秘密方案的定义。

设参与者集合 $\wp=\{1,2,\cdots,n\}$，若 $\Gamma_{\text{Qual}}\subseteq 2^{\wp}$，$\Gamma_{\text{Forb}}\subseteq 2^{\wp}$ 且 $\Gamma_{\text{Qual}}\bigcup\Gamma_{\text{Forb}}=2^{\wp}$，$\Gamma_{\text{Qual}}\bigcap\Gamma_{\text{Forb}}=\varnothing$，称 $(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}})$ 为通用存取结构(general access structure)[4]，简记为(Γ_Q,Γ_F)。记 $V(\{i_1,i_2,\cdots,i_s\},\boldsymbol{M})$ 表示矩阵 $\boldsymbol{M}$ 中第 $i_1,i_2,\cdots,i_s$ 行或运算得到的行向量，$H(\boldsymbol{U})$表示行向量 $\boldsymbol{U}$ 的汉明重量。

定义 1[4] 设(Γ_Q,Γ_F)是一个通用存取结构，称两个以 $n\times m$ 布尔矩阵为元素的集合 C_0 和 C_1，组成一个 (Γ_Q,Γ_F) 视觉密码方案(VCS)。C_0 是分享白像素的映射空间，C_1 是分享黑像素的映射空间，满足以下两个条件：

(1) $\forall X\in\Gamma_Q$，设 $\boldsymbol{M}_0\in C_0,\boldsymbol{M}_1\in C_1$，则 $H(V(X,\boldsymbol{M}_0))\le t_X-\alpha\cdot m$，$H(V(X,\boldsymbol{M}_1))\ge t_X$。

(2) $\forall X\in\Gamma_F$，设 $\boldsymbol{M}_0\in C_0,\boldsymbol{M}_1\in C_1$，则 $H(V(X,\boldsymbol{M}_0))=H(V(X,\boldsymbol{M}_1))$。

其中，条件(1)是对比性条件，指任意的授权子集均能恢复秘密图像。条件(2)是安全性条件，保证禁止子集得不到秘密图像的任何信息。α 称为相对差，m 称为像素扩展度，t_X 可以随 X 改变。$C_0=P(\boldsymbol{M}_0)$，$C_1=P(\boldsymbol{M}_1)$，$\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$ 称为基矩阵(basis matrices)，P 表示对矩阵进行完全列排序。

设 $S_1,S_2,\cdots,S_h$ 表示 h 幅秘密图像，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^i,Γ_F^i)，记为 $\Gamma^i,1\le i\le h$。

定义 2 设$(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$是 n 个参与者分享 h 个秘密图像的存取结构，对于任意的 $i\in\{1,2,\cdots,h\}$ 均存在 $(\Gamma_Q^i,\Gamma_F^i)-\text{VCS}$，且 $\Gamma_Q^i\bigcap\Gamma_Q^j=\varnothing$，$1\le i\ne j\le h$。称 2^h 个以 $n\times m$ 布尔矩阵为元素的集合 $C_{t_1,t_2,\cdots,t_h}$ 组成一个 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS。$C_{t_1,t_2,\cdots,t_h}$ 是像素组合 $\{t_1,t_2,\cdots,t_h\}$ 的映射空间 $(t_i\in S_i,t_i=0,1)$，满足以下两个条件：

(1) $\forall X\in\Gamma_Q^i$，设 $\boldsymbol{M}_0\in C_{t_1,\cdots,t_i=0,\cdots,t_h}$，$\boldsymbol{M}_1\in C_{t_1,\cdots,t_i=1,\cdots,t_h}$，则 $H(V(X,\boldsymbol{M}_0))\le t_X-\alpha_i\cdot m$, $H(V(X,\boldsymbol{M}_1))\ge t_X$。

(2) $\forall X\in\Gamma_F^i$，设 $\boldsymbol{M}_0\in C_{t_1,\cdots,t_i=0,\cdots,t_h}$，$\boldsymbol{M}_1\in C_{t_1,\cdots,t_i=1,\cdots,t_h}$，则 $H(V(X,\boldsymbol{M}_0))=H(V(X,\boldsymbol{M}_1))$。

其中条件(1)是对比性条件，表示 S_i 的授权子集能恢复第 i 个秘密图像。条件(2)是安全性条件，保证 S_i 的禁止子集无法得到第 i 个秘密图像的任何信息。α_i 是恢复 S_i 时的相对差，m 称为像素扩展度，t_X 随 X 改变。$C_{t_1,t_2,\cdots,t_h}=P(\boldsymbol{M}_{t_1,t_2,\cdots,t_h})$，$\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$ 称为 AMVCS 的基矩阵。

2.2 冗余基矩阵

AMVCS 在分享秘密图像像素时，根据秘密图像 $S_1,S_2,\cdots,S_h$ 在相同位置上的 h 个像素点的颜色组合 $\{t_1,t_2,\cdots,t_h\}$，选择一个矩阵集合 $C_{t_1,t_2,\cdots,t_h}$，t_i 根据 S_i 中像素颜色的白黑选择 0 或 1。再随机地从 $C_{t_1,t_2,\cdots,t_h}$ 中选取一个矩阵 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$，确定了 n 个共享份的 m 个子像素的颜色。

从上述分享算法的描述中可以看出：$\{t_1,t_2,\cdots,t_h\}$ 与 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$ 是一一映射的关系。实际上，目前 AMVCS 直接将 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$ 的数量定义为 2^h，而没有考虑 $\{t_1,t_2,\cdots,t_h\}$ 的取值空间，因此基矩阵可能存在冗余。

定义 3 对于 $S_1,S_2,\cdots,S_h$，记像素组合 $\{t_1,t_2,\cdots,t_h\}$ 的取值空间为 $\boldsymbol{T}$, AMVCS 中基矩阵的取值空间为 $\boldsymbol{M}$，若 $\{g_1,g_2,\cdots,g_h\}\notin\boldsymbol{T}$，且 $\boldsymbol{M}_{g_1,g_2,\cdots,g_h}\in\boldsymbol{M}$，称 $\boldsymbol{M}_{g_1,g_2,\cdots,g_h}$ 为冗余基矩阵。

以图 1 为例(黑色边框并非图像的内容，只为了突出图像)，两幅二值图像的像素组合包括{0, 0}, {0, 1}, {1, 0} 3 种，不存在{1, 1}组合，即$\{1,1\}\notin\boldsymbol{T}$，但在目前的 AMVCS 中 $\boldsymbol{M}_{11}\in\boldsymbol{M}$，因此 $\boldsymbol{M}_{11}$ 在基矩阵空间中就是冗余的。当 $\boldsymbol{M}_{00},\boldsymbol{M}_{01},\boldsymbol{M}_{10}$ 组成 AMVCS 的基矩阵集合时，$\boldsymbol{M}_{00},\boldsymbol{M}_{01},\boldsymbol{M}_{10}$ 存在减小规模的可能性，具体见定理 1。

定理 1 设 $\boldsymbol{M}$ 是$(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$的 AMVCS 基矩阵空间，若 $\forall\boldsymbol{M}_{t_1,t_2,\cdots,t_h}\in\boldsymbol{M}$，均有 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}=\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$

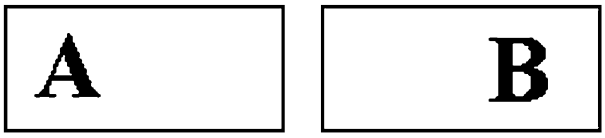


图 1 3 种像素组合的两幅图像

$\circ \boldsymbol{B}$，则 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$ 也是 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 基矩阵，其中“$\circ$”表示矩阵连接。

证明　设 X 为参与者集合，由于 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}=\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}\circ\boldsymbol{B}$，因此

$$\begin{aligned}&H\left(V(X,\boldsymbol{M}_{t_1,t_2,\cdots,t_h})\right)\\&=H\left(V(X,\boldsymbol{M}'_{t_1,t_2,\cdots,t_h})\right)+H\left(V(X,\boldsymbol{B})\right)\\&=H\left(V(X,\boldsymbol{M}'_{t_1,t_2,\cdots,t_h})\right)+t'_X\end{aligned}\tag{1}$$

(1)当 $X\in\Gamma_Q^i$，根据定义 2 的条件(1)，$H(V(X,\boldsymbol{M}_{t_1,\cdots,t_i=0,\cdots,t_h}))\le t_X-\alpha_i\cdot m$，$H(V(X,\boldsymbol{M}_{t_1,\cdots,t_i=1,\cdots,t_h}))\ge t_X$。由式(1)，可得 $H(V(X,\boldsymbol{M}'_{t_1,\cdots,t_i=0,\cdots,t_h}))\le t_X-t'_X-\alpha'_i\cdot m',H(V(X,\boldsymbol{M}'_{t_1,\cdots,t_i=1,\cdots,t_h}))\ge t_X-t'_X$，因此 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$ 满足定义 2 的条件(1)，其中 $m'=m-\beta$，$\alpha'_i=\dfrac{\alpha_i\cdot m}{m'}$，$\beta$ 是 $\boldsymbol{B}$ 的列数。

(2)当 $X\in\Gamma_F^i$，根据定义 2 的条件(2)，$H(V(X,\boldsymbol{M}_{t_1,\cdots,t_i=0,\cdots,t_h}))=H(V(X,\boldsymbol{M}_{t_1,\cdots,t_i=1,\cdots,t_h}))$，两边同时减去 t'_X，结合式(1)，可得 $H(V(X,\boldsymbol{M}'_{t_1,\cdots,t_i=0,\cdots,t_h}))=H(V(X,\boldsymbol{M}'_{t_1,\cdots,t_i=1,\cdots,t_h}))$。

综上，$\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$ 满足 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 两个条件，因此 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$ 也是 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 的基矩阵。　　证毕

定理 1 表明：若 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 的基矩阵 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$ 含有相同的列，则删去相同列以后的矩阵 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$，仍然是 $(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 的基矩阵。同时 $m'<m$，$\alpha'_i>\alpha_i$，即减小了像素扩展度，提高了相对差。

3　AMVCS 的构造方法

本节首先给出一种解决 AMVCS 中冗余基矩阵的压缩算法，在此基础上，设计了 AMVCS 的秘密分享与恢复流程。

3.1 压缩算法

在 2.2 节中，利用两幅特殊的图像分析了 AMVCS 中存在冗余基矩阵的可能性，像素组合的取值空间是以整幅图像为对象，而在实际的方案构造中，共享份一般仅在宽度上进行扩展，因此本文选择秘密图像的列像素组合为分享单位，保证了每一列的原像素具有相同的像素扩展度。若对于同一列像素组合存在冗余基矩阵，则可以对方案的基矩阵进行简化。

设秘密图像 $S_1,S_2,\cdots,S_h$ 的大小为 $a\times d$，$(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 的 AMVCS 的基矩阵为 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$。对授权集合 X 而言，在第 i 幅图像的第 j 列中，原白像素在恢复图像中的灰度级为 $w_{i,j}=\dfrac{H(V(X,\boldsymbol{M}_0))}{m}$，原黑像素在恢复图像中的灰度级为 $b_{i,j}=\dfrac{H(V(X,\boldsymbol{M}_1))}{m}$，$i\in\{1,2,\cdots,h\}$，$j\in\{1,2,\cdots,d\}$。为了保持整幅图像的对比性，有以下准则：$w_{i,\max}<b_{i,\min}$。其中 $w_{i,\max}=\{w_{i,j}\mid w_{i,j}\ge w_{i,k},1\le k\ne j\le d\}$，表示第 i 幅恢复图像中原白像素对应的最大灰度级；$b_{i,\min}=\{b_{i,j}\mid b_{i,j}\le b_{i,k},1\le k\ne j\le d\}$，表示第 i 幅恢复图像中原黑像素对应的最小灰度级。

算法输入：h 幅秘密图像的某一列 $\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_h$，$\boldsymbol{s}_i(i=1,2,\cdots,h)$ 为 $a\times1$ 的二值向量，$\boldsymbol{Z}$ 为 1×2^h 的零向量，基矩阵 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$。

算法输出：压缩后的基矩阵 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$。

步骤 1　对 $\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_h$ 相同位置的像素组合进行计数。对于 $q\in\{1,2,\cdots,a\}$，$\boldsymbol{Z}_{s_1(q),s_2(q),\cdots,s_h(q)}$ 自加 1；

步骤 2　若 $\boldsymbol{Z}_{t_1,t_2,\cdots,t_h}$ 为零，则删除基矩阵 $\boldsymbol{M}_{t_1,t_2,\cdots,t_h}$ $(t_i\in\{0,1\},i\in\{1,2,\cdots,h\})$；

步骤 3　在满足整体对比性的条件下，删除剩余基矩阵中的相同列，得到压缩后的基矩阵 $\boldsymbol{M}'_{t_1,t_2,\cdots,t_h}$，算法结束。

关于压缩算法有两点需要说明。

(1)压缩算法是对基矩阵的进一步简化处理，而与具体的基矩阵设计方法无关。本文采用最常用的 AMVCS 基矩阵设计方法[17−20]，即交叉连接单秘密方案的基矩阵，$\boldsymbol{M}_{t_1,t_2,\cdots,t_h}=\boldsymbol{M}_{t_1}^1\circ\boldsymbol{M}_{t_2}^2\circ\cdots\circ\boldsymbol{M}_{t_h}^h$。其中 $(\boldsymbol{M}_0^i,\boldsymbol{M}_1^i)$ 是 (Γ_Q^i,Γ_F^i) 的 VCS 的基矩阵，“$\circ$”表示矩阵连接，像素扩展度 $m=\sum_{i=1}^h m_i$，m_i 是 (Γ_Q^i,Γ_F^i) 的 VCS 的像素扩展度。

(2)若步骤 1 结束后，$\boldsymbol{Z}$ 的每个元素均大于 0，即不存在冗余基矩阵，则压缩算法对于减小基矩阵规模是无效的。

3.2 分享与恢复算法

通常的 AMVCS 方案以秘密图像的一个像素组合为单位完成秘密分享，本文在压缩算法的基础上，以秘密图像的一列组合为单位完成多幅秘密图像的分享过程，具体流程如图 2 所示。

在恢复秘密图像时，与通常的 AMVCS 相同，只需将共享份简单的叠加即可(图 3)。设 $X\in\Gamma_Q^i$，在恢复秘密图像 S_i 时，X 中的参与者叠加各自的共享份。

4　实验与分析

在评价多秘密视觉密码方案时，除了像素扩展度和相对差之外，方案所适用的存取结构以及分享

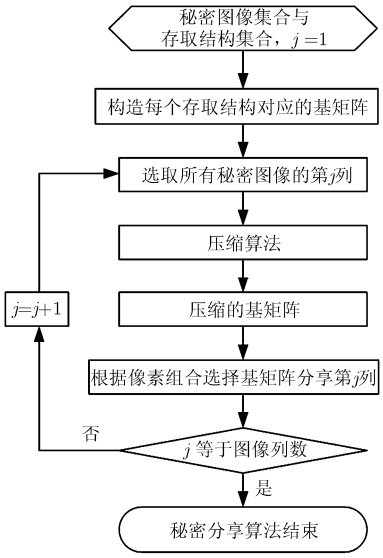


图 2 秘密分享算法流程图

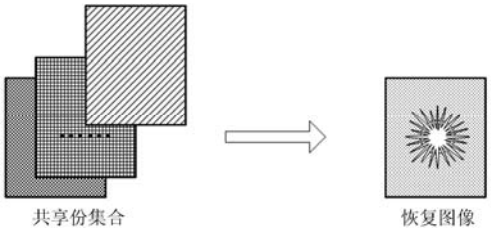


图 3 秘密恢复算法流程图

秘密图像的数量也是重要的性能指标。本文方案与其他多秘密视觉密码方案的比较见表 1。从表中可以看出，在存取结构方面，只有本文方案与文献[19]适用于通用存取结构；在秘密数量方面，本文方案与大多数方案一样，都可以分享多幅秘密图像；在安全性方面，本文方案满足定义 2 的安全性条件，因此是理论安全的。

在像素扩展度与相对差方面，文献[13,15,16]的结果较好，但适用的存取结构简单，且文献[15,16]分享的秘密数量有限，同时文献[13,15]是条件安全的。当存在冗余基矩阵时，本文方案比文献[14,18,19]的像素扩展度更小，相对差更大；当不存在冗余基矩阵时，本文方案与文献[14,18,19]的像素扩展度和相对差相同。

本文方案优化像素扩展度的效果与秘密图像是有关的。下面基于通用存取结构，以 3 组图像组合为例，说明本文方案在像素扩展度方面的压缩效果。

设共有 3 个参与者，参与者 1 和参与者 2 分享秘密图像 S_1，参与者 1 和参与者 3 分享秘密图像 S_2，即 $P=\{1,2,3\}$，$\Gamma_Q^1=\{\{1,2\}\}$，$\Gamma_F^1=2^P-\Gamma_Q^1$，$\Gamma_Q^2=\{\{1,3\}\}$，$\Gamma_F^2=2^P-\Gamma_Q^2$。根据单秘密方案的设计方法，则 (Γ_Q^1,Γ_F^1) 对应的基矩阵为 $\boldsymbol{M}_0^1=\begin{bmatrix}1&0\\1&0\\1&1\end{bmatrix}$，$\boldsymbol{M}_1^1=\begin{bmatrix}1&0\\0&1\\1&1\end{bmatrix}$，$(\Gamma_Q^2,\Gamma_F^2)$ 对应的基矩阵为 $\boldsymbol{M}_0^2=\begin{bmatrix}1&0\\1&1\\1&0\end{bmatrix}$，$\boldsymbol{M}_1^2=\begin{bmatrix}1&0\\1&1\\0&1\end{bmatrix}$。交叉连接两个单秘密方案的基矩阵，可得

$$\boldsymbol{M}_{00}=\begin{bmatrix}1&0&1&0\\1&0&1&1\\1&1&1&0\end{bmatrix},\quad \boldsymbol{M}_{01}=\begin{bmatrix}1&0&1&0\\1&0&1&1\\1&1&0&1\end{bmatrix}$$

$$\boldsymbol{M}_{10}=\begin{bmatrix}1&0&1&0\\0&1&1&1\\1&1&1&0\end{bmatrix},\quad \boldsymbol{M}_{11}=\begin{bmatrix}1&0&1&0\\0&1&1&1\\1&1&0&1\end{bmatrix}$$

表 1 本文方案与其他多秘密视觉密码方案的比较

方案	文献[13]	文献[14]	文献[15]	文献[16]	文献[18]	文献[19]	本文方案
方案类型	操作式	操作式	操作式	存取式	存取式	存取式	存取式
存取结构	(2, 2) 门限结构	(k, n) 门限结构	(2, 2) 门限结构	(2, 3) 门限结构	$(k_1,\cdots,k_h,n)$ 门限结构	$(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 通用存取结构	$(\Gamma^1,\Gamma^2,\cdots,\Gamma^h)$ 通用存取结构
安全性	条件安全	理论安全	条件安全	理论安全	理论安全	理论安全	理论安全
秘密数量	$h\geq 2$	$h\geq 2$	2	2	$h\geq 2$	$h\geq 2$	$h\geq 2$
像素扩展度	$3h$	$h\cdot m_{k,h}$	1	$m_{2,2}+m_{3,3}$	$\sum_{i=1}^{h} m_{ki,n}$	$\sum_{i=1}^{h} m_i$	$\leq\sum_{i=1}^{h} m_i$
相对差	$(3h)^{-1}$	$(h\cdot m_{k,h})^{-1}$	0.43	$(m_{2,2}+m_{3,3})^{-1}$	$\left(\sum_{i=1}^{h} m_{ki,n}\right)^{-1}$	$\left(\sum_{i=1}^{h} m_i\right)^{-1}$	$\geq\left(\sum_{i=1}^{h} m_i\right)^{-1}$

(1)冗余基矩阵个数为 1　当两幅秘密图像的相同列中不存在像素组合“00”时，则分享这一列的像素时只用到 $\boldsymbol{M}_{01},\boldsymbol{M}_{10},\boldsymbol{M}_{11}$，而这 3 个基矩阵存在相同的一列 $[0\ 1\ 1]^{\mathrm{T}}$，删去相同的列得到压缩的基矩阵，可得

$$\boldsymbol{M}_{01}^{'}=\begin{bmatrix}1&0&1\\1&0&1\\1&1&0\end{bmatrix},\ \boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&1&0\end{bmatrix},\ \boldsymbol{M}_{11}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}$$

同理，当两幅秘密图像的一列中不存在像素组合“11”时，则分享这一列的像素时只用到 $\boldsymbol{M}_{00},\boldsymbol{M}_{01},\boldsymbol{M}_{10}$，而这 3 个基矩阵存在相同的一列 $[1\ 1\ 1]^{\mathrm{T}}$，删去相同的列得到压缩的基矩阵，也可以得到压缩后的基矩阵

$$\boldsymbol{M}_{00}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&1&0\end{bmatrix},\ \boldsymbol{M}_{01}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&0&1\end{bmatrix},\ \boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&0&0\\0&1&1\\1&1&0\end{bmatrix}$$

但当两幅秘密图像的一列中不存在像素组合“01”或“10”时，基矩阵不能压缩。

(2)冗余基矩阵个数为 2　只有 00 和 01 时，$\boldsymbol{M}_{00}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&1&0\end{bmatrix},\boldsymbol{M}_{01}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&0&1\end{bmatrix}$。需要说明的是，尽管 $\boldsymbol{M}_{00}^{'},\boldsymbol{M}_{01}^{'}$ 还存在相同列，但删去以后违反整体对比性，因此需要保留。

只有 00 和 10 时，$\boldsymbol{M}_{00}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&1&0\end{bmatrix},\boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&0&0\\0&1&1\\1&1&0\end{bmatrix}$。只有 01 和 10 时，$\boldsymbol{M}_{01}^{'}=\begin{bmatrix}0&1\\0&1\\1&0\end{bmatrix}$，$\boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&0\\0&1\\1&0\end{bmatrix}$。只有 01 和 11 时，$\boldsymbol{M}_{01}^{'}=\begin{bmatrix}1&0&1\\1&0&1\\1&1&0\end{bmatrix}$，$\boldsymbol{M}_{11}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}$。只有 10 和 11 时，$\boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&1&0\end{bmatrix}$，$\boldsymbol{M}_{11}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}$。只有 00 和 11 时，不能压缩。

(3)冗余基矩阵个数为 3　仅有一个基矩阵时，所有列均视为相同的列，按照整体对比性的准则进行处理。

只有 00 时，$\boldsymbol{M}_{00}^{'}=\begin{bmatrix}0&1&0\\0&1&1\\1&1&0\end{bmatrix}$。只有 01 时，$\boldsymbol{M}_{01}^{'}=\begin{bmatrix}0&1\\0&1\\1&0\end{bmatrix}$。只有 10 时，$\boldsymbol{M}_{10}^{'}=\begin{bmatrix}1&0\\0&1\\1&0\end{bmatrix}$。只有 11 时，$\boldsymbol{M}_{11}^{'}=\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}$。

按照第 3 节的算法分别对 3 组图像进行处理，第 1 组图像为复杂的一般图像，由 Lina 和摄像师组成，实验结果如图 4 所示，其中“+”表示共享份叠加。

第 2 组图像为一般的文字图像，实验结果如图 5 所示。

第 3 组图像为简单的文字图像，实验结果如图 6 所示。

分析上述的 3 组实验可知：

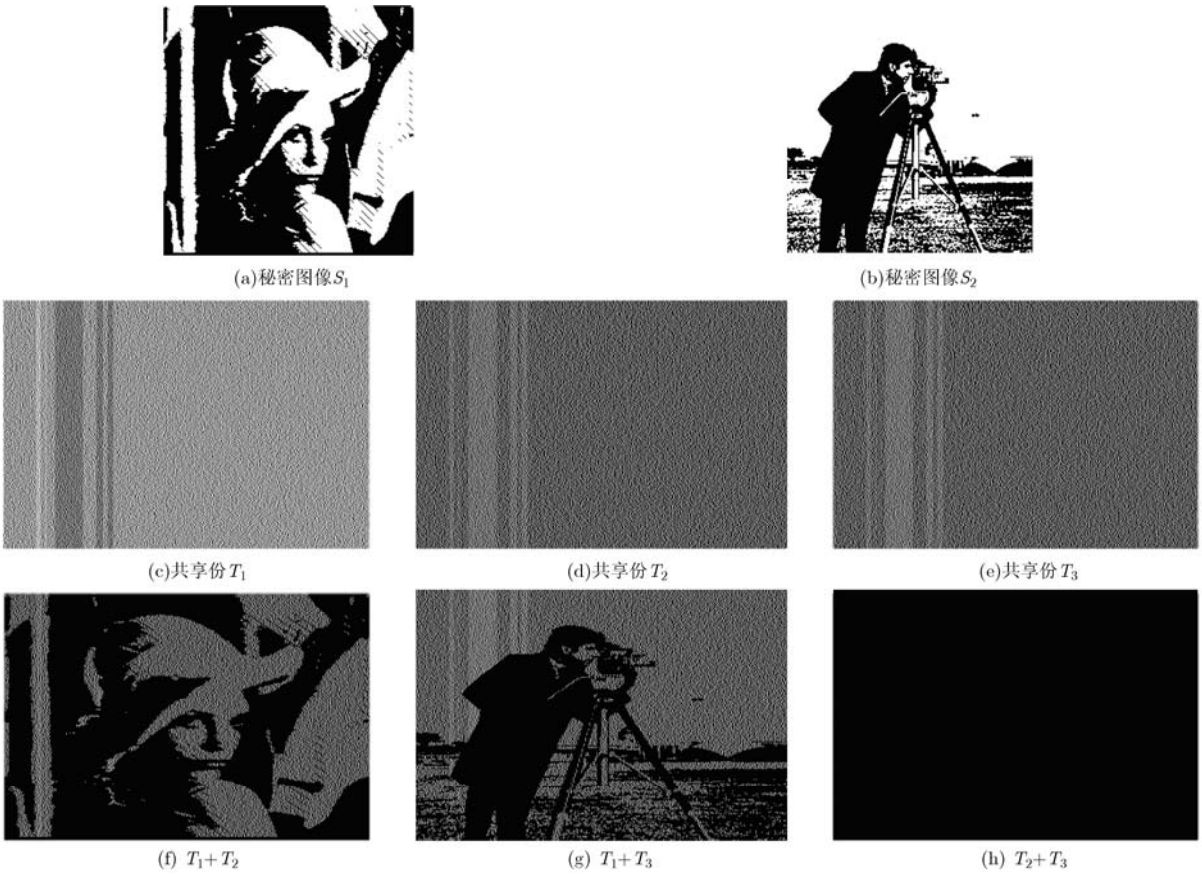
(1)授权子集能够恢复秘密图像　参与者 1 和参与者 2 恢复秘密图像 1，参与者 1 和参与者 3 恢复秘密图像 2。需要指出的是，尽管在恢复图像中存在条纹状的不同灰度级别，但由于原图像是二值图像，因此除了全黑以外的灰度级均对应着原图像的白像素，不会影响原图像信息的获取。

(2)禁止子集无法恢复秘密图像　单独的共享份会呈现出条纹状的随机信息，由于压缩基矩阵时，删除的冗余列的汉明重量是不固定的，因此无法判断条纹与像素组合的关系。同时，参与者 2 和参与者 3 恢复的图像为全黑，也无法得到秘密图像的信息。

(3)本算法的压缩效果随秘密图像而改变，相比而言，简单图像的压缩率更高。第 1，第 2 组存在条纹状，表明秘密图像的部分列组合存在冗余；第 3 组不存在条纹状，表明秘密图像的所有列组合均存在冗余。具体的压缩比例见表 2。

5　结束语

本文提出了一种存取式多秘密视觉密码方案，通过压缩基矩阵的规模，可以有效的减小共享份的尺寸。与目前逐点分享的 AMVCS 不同，本文方案以秘密图像的列组合为分享单位，保证了方案的安全性和对比性，且能够减小简单图像的恢复尺寸。本方案的压缩算法仅适用于存取式方案，因此如何应用于操作式方案有待进一步研究。

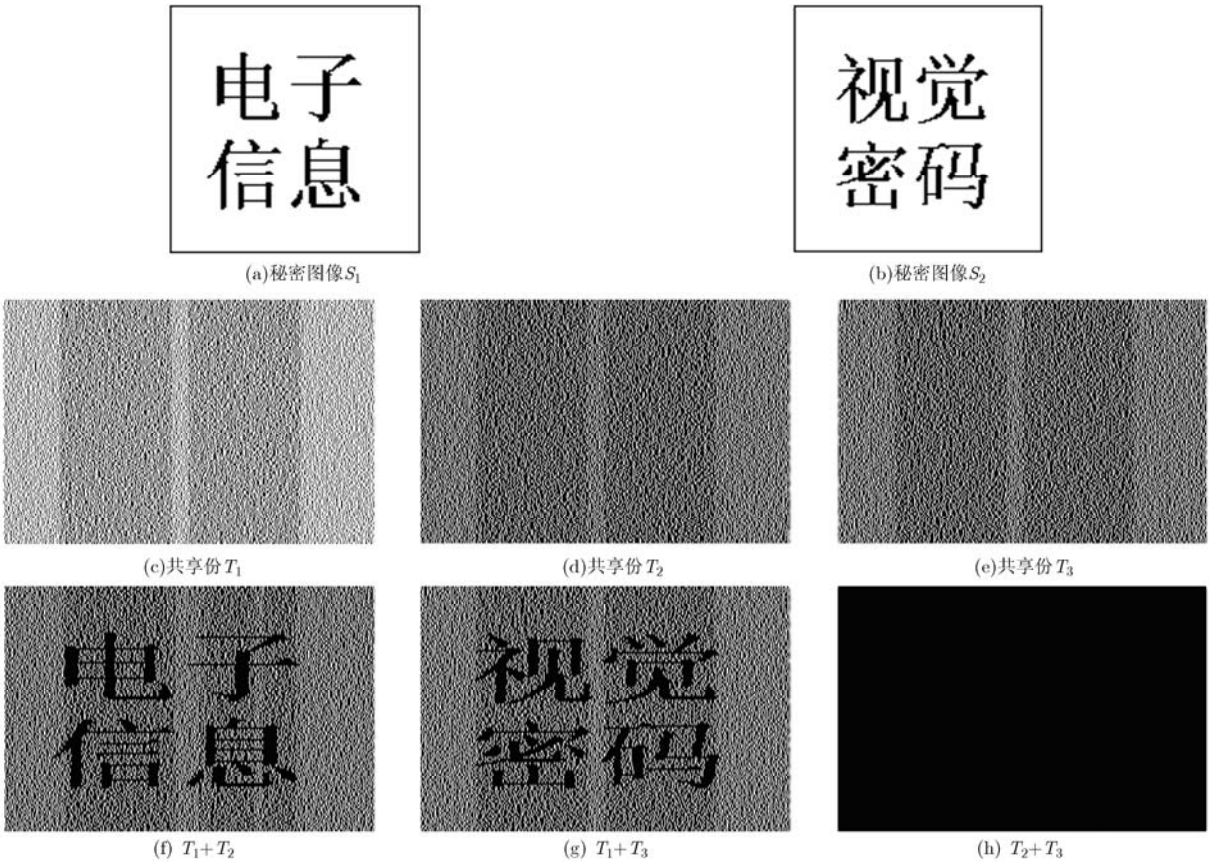


(a)秘密图像S_1 (b)秘密图像S_2

(c)共享份T_1 (d)共享份T_2 (e)共享份T_3

(f) T_1+T_2 (g) T_1+T_3 (h) T_2+T_3

图 4 第 1 组图像的实验效果



(a)秘密图像S_1 (b)秘密图像S_2

(c)共享份T_1 (d)共享份T_2 (e)共享份T_3

(f) T_1+T_2 (g) T_1+T_3 (h) T_2+T_3

图 5 第 2 组图像的实验效果

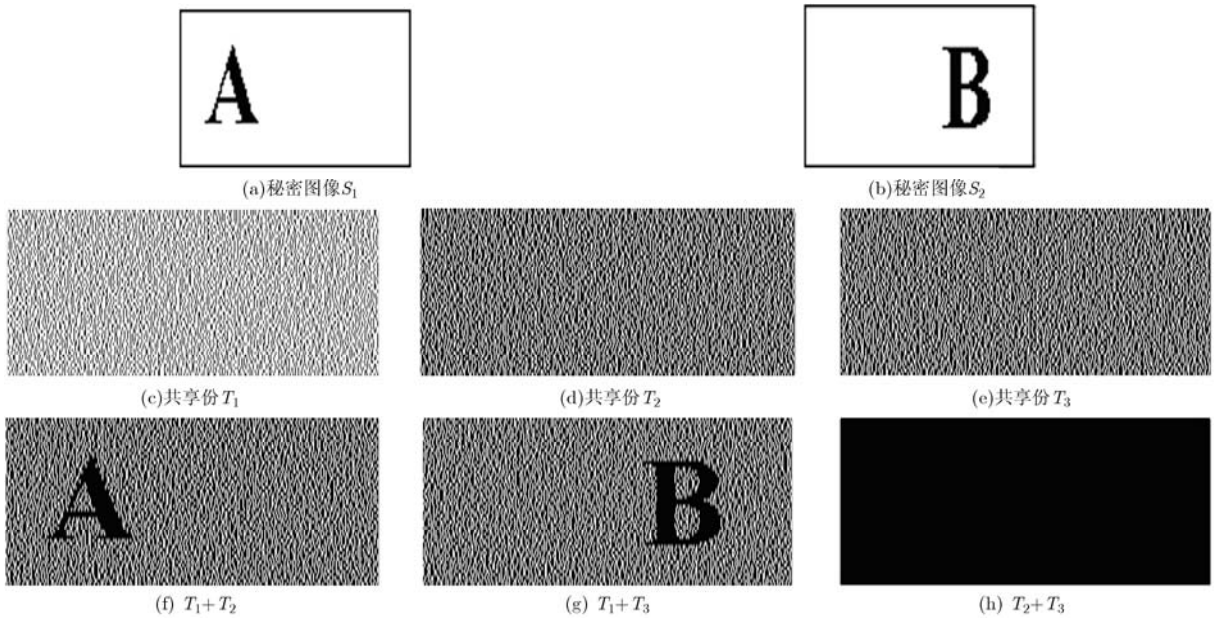


图 6 第 3 组图像的实验效果

表 2 通用存取结构下不同秘密图像组合的压缩比例

秘密图像	原图像尺寸	文献[19]恢复图像尺寸	本文压缩算法恢复图像尺寸	压缩率(%)
第 1 组	256×256	1024×256	983×256	4.3
第 2 组	256×256	1024×256	886×256	13.5
第 3 组	54×120	216×120	162×120	25.3

参 考 文 献

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

[2] Blakley G R. Safeguarding cryptographic keys[C]. Proceedings of the National Computer Conference, NJ, USA, 1979: 242–268.

[3] Shamir A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612–613.

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

[5] Hajiabolhassan H and Cheraghi A. Bounds for visual cryptography schemes[J]. *Discrete Applied Mathematics*, 2010, 158(6): 659–665.

[6] 郁滨, 卢锦元, 房礼国. 基于迭代算法的可验证视觉密码[J]. 电子与信息学报, 2011, 33(1): 163–167.
Yu Bin, Lu Jin-yuan, and Fang Li-guo. Verifiable visual cryptography based on iterative algorithm[J]. *Journal of Electronics & Information Technology*, 2011, 33(1): 163–167.

[7] Blundo C, Santis A D, and Stinson D R. On the contrast in visual cryptography schemes[J]. *Journal of Cryptography*, 1999, 12: 261–289.

[8] Liu F, Wu C, and Lin X. Step construction of visual cryptography schemes[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(1): 27–38.

[9] Shyu S J and Chen M C. Optimum pixel expansions for threshold visual secret sharing schemes[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 960–969.

[10] Surekha B, Swamy G N, and Rao K S. A multiple watermarking technique for images based on visual cryptography[J]. *International Journal of Computer Applications*, 2010, 1(11): 66–71.

[11] Guo J, Soo C, and Lee H. Watermarking in halftone images with parity-matched error diffusion[J]. *Signal Processing*, 2011, 91(1): 126–135.

[12] Liu F, Wu C, and Lin X. Cheating immune visual cryptography scheme[J]. *IET Information Security*, 2011, 5(1): 51–59.

[13] 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.

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

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

2730–2741.

[16] Droste S. New results on visual cryptography[C]. Advances in Cryptography-CRYPTO' 96, 1996, LNCS, 1109: 401–415.

[17] Katoh T and Imai H. Some visual secret sharing schemes and their share size[C]. Proceedings of International Conferences on Cryptology and Information Security, China, 1996: 41–47.

[18] Yu B and Xu X H. Multi-secret sharing threshold visual cryptography scheme[C]. International Conference on Computational Intelligence and Security, Harbin, China, 2007: 815–818.

[19] Yu B, Fu Z X, and Fang L G. A modified multi-secret sharing visual cryptography scheme[C]. 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 2008: 351–354.

[20] 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): 712–718.
Fu Zheng-xin, Yu Bin, and Fang Li-guo. A new multi-secret sharing visual cryptography[J]. *Acta Electronica Sinica*, 2011, 39(3): 712–718.

付正欣： 男，1986年生，博士生，研究方向为视觉密码.

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.

房礼国： 男，1981年生，讲师，主要研究方向为视觉密码和网络安全.