异或视觉密码的理想存取结构研究

付正欣*[①] 沈 刚[①] 孔志印[②] 郁 滨[①]
[①](解放军信息工程大学 郑州 450004)
[②](信息保障技术重点实验室 北京 100072)

摘 要：该文给出异或视觉密码的理想存取结构的定义，分析了其特征，研究了理想存取结构的共享份构造方法。在此基础上，提出将通用存取结构划分为若干个理想存取结构的算法，设计了通用存取结构的秘密分享与恢复流程。与现有的方案相比，该方案实现了秘密图像的完全恢复，且明显地减小了共享份的规模。

关键词：视觉密码；异或运算；理想存取结构；通用存取结构；完全恢复
中图分类号： TP309.7 **文献标识码**： A **文章编号**：1009-5896(2014)07-1642-06
DOI: 10.3724/SP.J.1146.2013.01395

Investigation on Ideal Access Structure of XOR-based Visual Cryptography

Fu Zheng-xin[①] Shen Gang[①] Kong Zhi-yin[②] Yu Bin[①]
[①](*PLA Information Engineering University*, *Zhengzhou* 450004, *China*)
[②](*Science and Technology on Information Assurance Laboratory*, *Beijing* 100072, *China*)

Abstract: The definition of ideal access structure of XOR-based visual cryptography is given in this paper. The characteristics of ideal access structure are analyzed, and the construction algorithm of shares under ideal access structure is designed. Based on the above results, a new algorithm is proposed for dividing the general access structure into some ideal access structures, and the secret sharing and recovering algorithms are presented. Compared with the previous schemes, the proposed scheme realizes the perfect recovery of secret image, and the sizes of shares can be decreased efficiently.

Key words: Visual cryptography; XOR operation; Ideal access structure; General access structure; Perfect recovery

1 引言

视觉密码[1]结合了秘密共享与数字图像处理技术，使用户仅利用视觉系统即可完成秘密图像的恢复，引起了学者的广泛关注[2−7]。在视觉密码提出之初，共享份以透明胶片为载体，解密图像通过直接叠加共享份并利用视觉系统观察平均效果来实现。这种方式的恢复实质上是对共享份进行或(OR)运算，其代数结构为加法半群，致使白像素无法完全恢复，因此恢复图像存在对比度的失真。

为了解决秘密图像完全恢复的问题，Biham 等人[8]提出了基于偏振光的视觉密码，利用共享份偏振方向的平行或正交设计了异或(XOR)运算，实现了$(2,2)$方案的完全恢复，大大改善了基于透明胶片的恢复图像质量。尽管恢复秘密图像时需要特殊的光学设备，但文献[8]的意义在于实现了群结构的视觉密码方案，为共享份的载体提供了更多的选择。Viet 等人[9]引入取反(reversing)运算，令每个参与者需要保存 c 个共享份，在恢复秘密图像时需要进行 c+1 次取反运算和 $kc-1$ 次或运算，可以将相对差由 $1/m$ 提高至 $1-(1-1/m)^c$，其中 m 表示(k,n)方案的像素扩展度。文献[9]利用复印机的取反功能实现了共享份的黑白像素反转，恢复算法不使用计算机，依然保持了秘密恢复的简便性，大大改善了恢复图像的相对差，但仍未实现完全恢复。在此基础上，Yang 等人[10]将 XOR 运算分解为 3 次或运算和 4 次取反运算，通过 m 次迭代，实现了(k,n)方案的完全恢复，但恢复算法需要 mk+$2m-1$ 次或运算和 $4m-3$ 次取反运算，增加了恢复操作的复杂度。以上方案丰富了共享份的实现载体，改善了视觉密码方案的恢复效果，同时保持了恢复简单的特点，为异或视觉密码的研究提供了思路。

Tuyls 等人[11]给出(k,n)异或视觉密码方案(XOR-based Visual Cryptography Scheme, XVCS)的定义。文献[11]构造了完全恢复的(n,n)方案，像

2013-09-07 收到，2014-04-12 改回
国家自然科学基金(61070086)和信息保障技术重点实验室开放基金(KJ-13-107)资助课题
*通信作者：付正欣 fzx2515@163.com

素扩展度和相对差均为 1；证明了(2,n)方案与二值纠错码的等价关系，最优像素扩展度为$\lfloor \log_2 n \rfloor$且相对差为$\lfloor \log_2 n \rfloor^{-1}$；对于 $2<k<n$ 的(k,n)方案，则通过(k,n)矩阵对和最大距离可分码两种方法予以实现，前者的像素扩展度较小但没有一般表达式，后者的像素扩展度为$2^{k-1}\cdot C(n,k)$。为了减小共享份的规模，Wang 等人[12]综合运用或运算和异或运算设计了一种(2,n)方案，实现了共享份的像素不扩展，但是相对差为 1/2，即恢复图像在质量上仍然存在失真。在文献[12]的基础上，Chao 等人[13]通过构造共享份分配矩阵，设计了一种(k,n)方案，实现了秘密图像的完全恢复，但方案的恢复算法需要拆分共享份，因此必须借助计算机实现恢复算法，在一定程度上违背了视觉密码的初衷。以上方案仅适用于门限结构，Liu 等人[14]提出了一种逐步构造法，构造了通用存取结构下的异或视觉密码方案，可以仅利用 XOR 运算实现图像的完全恢复，但 1 个参与者可能保存多个共享份，增加了共享份管理的难度。以上方案均以实现视觉密码方案的完全恢复为目标，着重于研究秘密共享与恢复算法的设计，却忽视了完全恢复时的存取结构特征。

针对上述问题，本文首先给出了异或视觉密码的理想存取结构，并研究了其基本特征。在此基础上，提出了一种将通用存取结构划分为若干理想存取结构的方法，设计了通用存取结构下的秘密分享和恢复算法，利用 XOR 运算即可实现秘密图像的完全恢复，而且具有较小的共享份规模。

2　基本概念

定义 1[2]　记参与者集合$P=\{1,2,\cdots,n\}$，其幂集记为2^P。称能够恢复秘密图像的参与者集合为授权子集，不能恢复秘密图像的参与者集合为禁止子集，记Γ_Q表示所有授权子集的集合，Γ_F表示所有禁止子集的集合，$\Gamma_Q\subseteq 2^P, \Gamma_F\subseteq 2^P, \Gamma_Q\bigcap\Gamma_F=\varnothing$，称$\Gamma=(\Gamma_Q,\Gamma_F)$为参与者集合$P$之上的存取结构。

定义 2[2]　记$\Gamma_0=\{A\in\Gamma_Q:\forall B\subset A\Rightarrow B\notin\Gamma_Q\}$，称$\Gamma_0$为最小授权集合。若$A\in\Gamma_0$，则称 A 为最小授权子集。

在本文中只考虑强存取结构，即对于$\Gamma=(\Gamma_Q,\Gamma_F)$，有$\Gamma_Q\cup\Gamma_F=2^P, \Gamma_Q$单调递增，且$\Gamma_F$单调递减。授权子集的集合$\Gamma_Q=\mathrm{cl}(\Gamma_0)$，其中$\mathrm{cl}(\Gamma_0)=\{B\subseteq 2^P:\exists A\in\Gamma_0 \text{ s.t. } B\supseteq A\}$表示最小授权集合$\Gamma_0$的闭包，禁止子集的集合$\Gamma_F=\{2^P-\mathrm{cl}(\Gamma_0)\}$，因此$\Gamma_Q$和$\Gamma_F$都可以由$\Gamma_0$表示。

设参与者集合$X=\{i_1,i_2,\cdots,i_p\}\subseteq\{1,2,\cdots,n\}$ $(1\le i_1<i_2<\cdots<i_p\le n)$，记$\boldsymbol{M}[X]$表示矩阵$\boldsymbol{M}$中第$i_1,i_2,\cdots,i_p$行组成的子矩阵，XOR($\boldsymbol{M}$)表示将矩阵$\boldsymbol{M}$所有行进行 XOR 运算后的行向量，$H(\boldsymbol{V})$表示行向量$\boldsymbol{V}$的汉明重量，通用存取结构下的异或视觉密码方案定义如下。

定义 3[11]　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)异或视觉密码方案(XVCS)。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$H(\mathrm{XOR}(\boldsymbol{M}_0[X]))\le t_X-\alpha\cdot m, H(\mathrm{XOR}(\boldsymbol{M}_1[X]))\ge t_X$。

(2) $\forall X\in\Gamma_F$，记$D_0=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in C_0\}$，$D_1=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in C_1\}$，则$D_0=D_1$。

其中，条件(1)是对比性条件，表明最小授权子集的参与者，通过异或运算能够恢复秘密图像。条件(2)是安全性条件，表明禁止子集的参与者，得不到秘密图像的任何信息。t_X表示恢复图像中原黑像素对应子像素块的最小汉明重量。m称为像素扩展度，表示 1 个原像素被分享成为共享份中的 m 个子像素，其越小越好。α称为相对差，表示恢复图像与原图像在视觉上的一致性，其越大越好。当 m=1 且α=1 时，共享份与秘密图像规模相等，且恢复图像与秘密图像相同，称该方案为理想的视觉密码方案(ideal visual cryptography scheme)。

例 1　(2, 4)-XVCS[11]

$$C_0=\left\{\begin{bmatrix}00\\00\\00\\00\end{bmatrix},\begin{bmatrix}01\\01\\01\\01\end{bmatrix},\begin{bmatrix}10\\10\\10\\10\end{bmatrix},\begin{bmatrix}11\\11\\11\\11\end{bmatrix}\right\},\quad C_1=\left\{\begin{bmatrix}00\\01\\10\\11\end{bmatrix},\begin{bmatrix}01\\10\\11\\00\end{bmatrix},\begin{bmatrix}10\\11\\00\\01\end{bmatrix},\begin{bmatrix}11\\00\\01\\10\end{bmatrix}\right\}$$

对于 (2, 4)-XVCS, $\Gamma_0=\{X\,|\,|X|=2, X\in 2^P\}$，$\Gamma_Q=\{X\,||X|\ge 2, X\in 2^P\}$且$\Gamma_F=2^P-\Gamma_Q$。不同参与者集合的解密能力分析如下：

(1)当$X\in\Gamma_F$且$X\ne\varnothing$时，即 X 由 1 个参与者组成，设$D_0=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in C_0\}$，$D_1=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in C_1\}$，则$D_0=D_1=\{[00],[01],[10],[11]\}$，满足定义 3 的条件(2)；

(2)当$X=\varnothing$时，X由 0 个参与者组成，$D_0=D_1=\varnothing$，满足定义 3 的条件(2)；

(3)当$X\in\Gamma_0$时，X由 2 个参与者组成，$\forall\boldsymbol{M}_0\in C_0$　有　$H(\mathrm{XOR}(\boldsymbol{M}_0[X]))=0$, $\forall\boldsymbol{M}_1\in C_1$　有　$H(\mathrm{XOR}(\boldsymbol{M}_1[X]))\ge 1$，满足定义 3 的条件(1)；

(4)当 X 由 3 个参与者组成时，$\forall\boldsymbol{M}_0\in C_0$有$H(\mathrm{XOR}(\boldsymbol{M}_0[X]))\le 2$, $\forall\boldsymbol{M}_1\in C_1$有$H(\mathrm{XOR}(\boldsymbol{M}_1[X]))\ge 1$；

(5)当X由 4 个参与者组成时，$H(\mathrm{XOR}(\boldsymbol{M}_0[X]))$

$=0$, $H(\mathrm{XOR}(\boldsymbol{M}_1[X]))\geq 0$。

情况(4)和情况(5)表明：当 $X\in\Gamma_Q-\Gamma_0$ 时，X 中的共享份 XOR 运算不再满足定义 3 的条件(1)。$\Gamma_0,\Gamma_Q-\Gamma_0,\Gamma_F$ 的直接恢复能力如图 1 所示，其中黑色表示无法恢复秘密图像，白色表示能够恢复秘密图像，阴影部分则表示可能恢复秘密图像。尽管当 $X\in\Gamma_Q-\Gamma_0$ 时可能无法直接恢复秘密图像，但可以通过 X 中的部分参与者恢复秘密图像[11]，这与 X 属于授权集合并不矛盾。

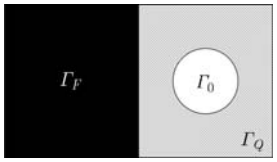

图1 各集合XOR运算的恢复能力

定义 4 记$*$表示一种集合运算，其运算规则为 $A*B=(A\cup B)-(A\cap B)$，其中 A 和 B 为两个集合。

定义 5 设参与者集合 $X=\{p_1,p_2,\cdots,p_x\}\in 2^P$，令 T_i 表示第 i 个参与者的共享份，记秘密恢复函数为 $R(X)=T_{p1}\oplus T_{p2}\oplus\cdots\oplus T_{px}$，表示对 X 的所有共享份进行异或运算。

定理 1 设 $A,B\in 2^P$，则有 $R(A*B)=R(A)\oplus R(B)$ 成立。

证明 设 $C=A\cap B$，则参与者集合 A 和 B 可以分别表示为 $A=\{c_1,c_2,\cdots,c_x,a_1,a_2,\cdots,a_y\}$ 和 $B=\{c_1,c_2,\cdots,c_x,b_1,b_2,\cdots,b_z\}$，其中 c_i, a_j, b_k两两互不相等，$0\leq i\leq x,0\leq j\leq y,0\leq k\leq z$。显然，由定义 4 可得

$$\begin{aligned}A*B&=\{c_1,c_2,\cdots,c_x,a_1,a_2,\cdots,a_y,b_1,b_2,\cdots,b_z\}\\&\quad-\{c_1,c_2,\cdots,c_x\}\\&=\{a_1,a_2,\cdots,a_y,b_1,b_2,\cdots,b_z\}\end{aligned}$$

又由秘密恢复函数定义可得式(1)~式(3):

$$R(A)=T_{c1}\oplus\cdots\oplus T_{c1}\oplus T_{a1}\oplus\cdots\oplus T_{ay}\tag{1}$$

$$R(B)=T_{c1}\oplus\cdots\oplus T_{cx}\oplus T_{b1}\oplus\cdots\oplus T_{bz}\tag{2}$$

$$R(A*B)=T_{a1}\oplus\cdots\oplus T_{ay}\oplus T_{b1}\oplus\cdots\oplus T_{bz}\tag{3}$$

式(1)，式(2)左右同时异或得：

$$R(A)\oplus R(B)\quad=T_{a1}\oplus\cdots\oplus T_{ay}\oplus T_{b1}\oplus\cdots\oplus T_{bz}$$

再由式(3)，可得 $R(A*B)=R(A)\oplus R(B)$。

证毕

3 理想的存取结构

本节首先给出了理想存取结构的定义，然后研究其基本特征，最后提出了理想存取结构下的秘密分享算法。

定义 6 对于存取结构 $\Gamma=(\Gamma_Q,\Gamma_F)$，其最小授权集合为 $\Gamma_0=\{Q_1,Q_2,\cdots,Q_t\}$，记秘密图像为 S，若 $\forall Q\in\Gamma_0$，均有 $R(Q)=S$ 成立，称该存取结构是理想的。

引理 1 设 Γ_0 是理想存取结构的最小授权集合，若 $Q_{i,1},Q_{i,2},\cdots,Q_{i,2k-1}\in\Gamma_0$，且 $Q'=Q_{i,1}*Q_{i,2}*\cdots*Q_{i,2k-1}$，其中 $k\in N^+$，则有 $Q'\in\Gamma_Q$。

证明 由于 $Q_{i,1},Q_{i,2},\cdots,Q_{i,2k-1}\in\Gamma_0$，则 $R(Q_{i,1})=R(Q_{i,2})=\cdots=R(Q_{i,2k-1})=S$，因此

$$\begin{aligned}&R(Q_{i,1})\oplus R(Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k-1})\\&\quad=\underbrace{S\oplus S\oplus\cdots\oplus S}_{2k-1}=S\end{aligned}\tag{4}$$

又由定理 1 可得

$$\begin{aligned}&R(Q_{i,1})\oplus R(Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k-1})\\&\quad=R(Q_{i,1}*Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k-1})=\cdots\\&\quad=R(Q_{i,1}*Q_{i,2}*\cdots*Q_{i,2k-1})=R(Q')\end{aligned}\tag{5}$$

由式(4)和式(5)，可得：$R(Q')=S$。

根据图 1 中 $\Gamma_0,\Gamma_Q-\Gamma_0,\Gamma_F$ 的直接恢复能力可知，$Q'\in\Gamma_0\cup(\Gamma_Q-\Gamma_0)=\Gamma_Q$。 证毕

引理 2 设 Γ_0 是理想存取结构的最小授权集合，$Q_{i,1},Q_{i,2},\cdots,Q_{i,2k}\in\Gamma_0$，且 $Q''=Q_{i,1}*Q_{i,2}*\cdots*Q_{i,2k}$，其中 $k\in N^+$，则 $\forall Q_j\in\Gamma_0$，均有 $Q''\subsetneq Q_j$。

证明 由于 $Q_{i,1},Q_{i,2},\cdots,Q_{i,2k}\in\Gamma_0$，则 $R(Q_{i,1})=R(Q_{i,2})=\cdots=R(Q_{i,2k})=S$，因此，

$$\begin{aligned}&R(Q_{i,1})\oplus R(Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k})\\&\quad=\underbrace{S\oplus S\oplus\cdots\oplus S}_{2k}=0\end{aligned}\tag{6}$$

又由定理 1 可得

$$\begin{aligned}&R(Q_{i,1})\oplus R(Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k})\\&\quad=R(Q_{i,1}*Q_{i,2})\oplus\cdots\oplus R(Q_{i,2k})=\cdots\\&\quad=R(Q_{i,1}*Q_{i,2}*\cdots*Q_{i,2k})=R(Q'')\end{aligned}\tag{7}$$

由式(6)和式(7)，可得：$R(Q'')=0$。

(1)根据异或视觉密码方案中 $\Gamma_0,\Gamma_Q-\Gamma_0,\Gamma_F$ 的 XOR 运算的直接恢复能力，则 $Q''\notin\Gamma_0$。

(2) 设 $\exists Q_j\in\Gamma_0$ 满足 $Q''\subset Q_j$。由于 $R(Q_j)=R(Q''\cup(Q_j-Q''))=R(Q''*(Q_j-Q''))=R(Q'')\oplus R(Q_j-Q'')$，且 $R(Q_j)=S$, $R(Q'')=0$，因此，$R(Q_j-Q'')=R(Q_j)\oplus R(Q'')=S$。而 $Q_j-Q''\subset Q_j$，根据最小授权集合的定义，$Q_j-Q''\in\Gamma_F$，因此 $R(Q_j-Q'')=0$。两者相矛盾，故 $\forall Q_j\in\Gamma_0$，均有 $Q''\not\subset Q_j$。

综上，$\forall Q_j\in\Gamma_0$，均有 $Q''\subsetneq Q_j$ 成立。 证毕

定理 2 对于存取结构 $\Gamma=(\Gamma_Q,\Gamma_F)$，记最小授权集合 $\Gamma_0=\{Q_1,Q_2,\cdots,Q_t\}$，若存取结构是理想的，则该存取结构必满足如下两个条件：

(1) Γ_0 的奇数个元素“$*$”运算的结果属于授权集合，即 $Q_{i,1}*Q_{i,2}*\cdots*Q_{i,2k-1}\in\Gamma_Q$。

(2) Γ_0 的偶数个元素“$*$”运算的结果不包含于

任意的最小授权子集，即 $\forall Q_j \in \Gamma_0$，均有 $Q_{i,1} * Q_{i,2} * \cdots * Q_{i,2k} \subsetneq Q_j$。

证明　由引理 1，引理 2 可证。

定理 2 描述了理想存取结构的必要条件，下面给出理想存取结构下的共享份生成算法。设存取结构 $\Gamma = (\Gamma_Q, \Gamma_F)$ 是理想的，设计理想存取结构的共享份生成算法(算法 1)如图 2 所示。

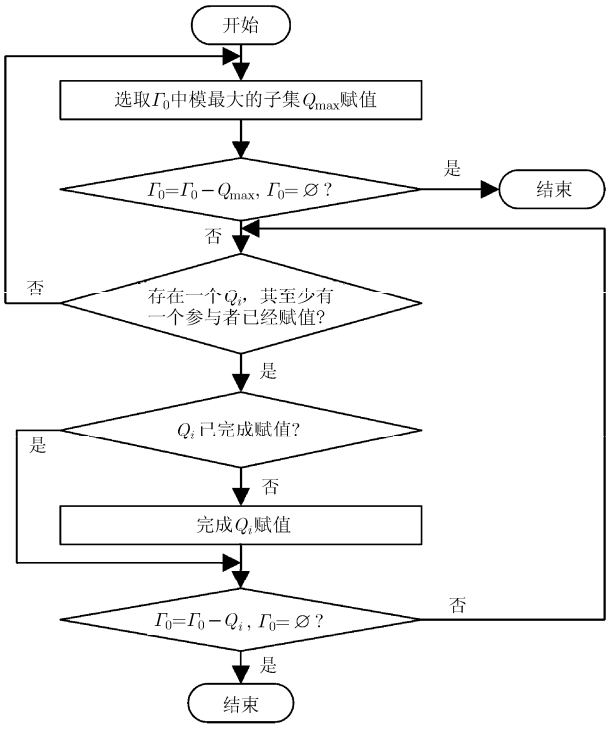

图 2 理想存取结构的共享份生成算法(算法 1)流程

在图 2 中为 $Q_{\max}$ 和 Q_i 赋值的具体方法如下：

(1)对于 $Q_{\max}$，利用(n,n)-XVCS 的共享份构造方法。设秘密图像 S 规模为 $a \times b$，随机生成 $|Q_{\max}|-1$ 个规模为 $a \times b$ 的共享份 $T_1, T_2, \cdots, T_{|Q_{\max}|-1}$，最后有 $T_{|Q_{\max}|} = S \oplus T_1 \oplus T_2 \oplus \cdots \oplus T_{|Q_{\max}|-1}$。

(2)对于 Q_i，设 $Q_i = \{A_1, A_2, \cdots, A_x, B_1, B_2, \cdots, B_y\}$, $(1 \le x, y \le n-1)$，其中参与者 $A_1, A_2, \cdots, A_x$ 的共享份 $T_{A1}, T_{A2}, \cdots, T_{Ax}$ 已经生成，而参与者 $B_1, B_2, \cdots, B_y$ 的共享份 $T_{B1}, T_{B2}, \cdots, T_{By}$ 尚未构造。随机生成与秘密图像规模相等的共享份 $T_{B1}, T_{B2}, \cdots, T_{B(y-1)}$，最后计算 $T_{By} = S \oplus T_{A1} \oplus \cdots \oplus T_{Ax} \oplus T_{B1} \oplus \cdots \oplus T_{B(y-1)}$。

4　通用存取结构的 XVCS 方案设计

理想的存取结构具有像素不扩展、完全恢复等优点，但其限制条件严格。将通用存取结构划分为若干个理想的存取结构，对通用存取结构的研究具有重要意义，同时也是难点问题。本节首先给出一种通用存取结构的划分算法，在此基础上设计通用存取结构的秘密分享与恢复算法。

4.1 通用存取结构的划分

下面给出一个将通用存取结构划分为若干理想存取结构的算法如表 1 所示。

表 1 理想存取结构算法

输入：通用存取结构的最小授权集合 Γ_0，集合 $Q = F = \varnothing$，i=1
输出：d 个理想存取结构的最小授权集合 $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$
步骤 1　从 Γ_0 中选取一个元素 X 放入 Q，将 X 从 Γ_0 删去；
步骤 2　从 Γ_0 中遍历与 Q 满足定理 2 中条件(1)和条件(2)的集合 Y。若 Y 存在，则将 Y 从 Γ_0 中移入 Q，转步骤 3；若 Y 不存在，则令 $\Gamma_0^i = Q$, $\Gamma_0 = \Gamma_0 \cup F$, $Q = F = \varnothing$, i=i+1 转步骤 1；
步骤 3　对于 Q，记偶数个元素“$*$”运算的结果为 Z_e。$\forall A \in \Gamma_0$，若满足 $Z_e \subseteq A$，则将 Z_e 从 Γ_0 中移入 F；
步骤 4　对于 Q，记奇数个元素“$*$”运算的结果为 Z_o。若 $Z_o \in \Gamma_0$，则将 Z_o 从 Γ_0 中移入 Q；
步骤 5　若 $\Gamma_0 \neq \varnothing$，转步骤 2；若 $\Gamma_0 = \varnothing$ 且 $F \neq \varnothing$，则令 $\Gamma_0^i = Q$, $\Gamma_0 = F$, $Q = F = \varnothing$, i=i+1 转步骤 1；若 $\Gamma_0 = \varnothing$ 且 $F = \varnothing$, d=i，算法结束，输出 $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$。

4.2 秘密分享算法

设通用存取结构划分为 d 个理想存取结构的最小授权集合 $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$，$T_1, T_2, \cdots, T_n$ 表示 n 个共享份。令每个共享份的规模是秘密图像的 d 倍，将每个共享份划分为规模相等的 d 个部分，其中 T_k^i 表示第 k 个共享份的第 i 部分$(1 \le k \le n, 1 \le i \le d)$，则秘密分享算法如表 2 所示。

4.3 秘密恢复算法

对于最小授权子集 $Q = \{q_1, q_2, \cdots, q_h\}$，取其中所有参与者共享份进行异或叠加即可恢复秘密图像，即

$$R = T_{q1} \oplus T_{q2} \oplus \cdots \oplus T_{qh}$$

表 2 秘密分享算法

输入：通用存取结构的划分 $\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$，秘密图像 S, i=1
输出：n 个共享份 $T_1, T_2, \cdots, T_n$
步骤 1　取未处理的 Γ_0^i=$\{Q_1, Q_2, \cdots, Q_t\}$，令 Q=$\bigcup_{j=1}^{t} Q_j$，$P = \{1, 2, \cdots, n\}$, $F = P - Q$；
步骤 2　对于第 k 个共享份的第 i 部分 $T_k^i (1 \le k \le n)$，Q 中参与者的共享份按算法 1 赋值，F 中参与者的共享份随机取值；
步骤 3　令 i=i+1，若 i>d 则转步骤 4，否则转步骤 1；
步骤 4　连接子共享份，生成最终共享份 $T_k = T_k^1 \circ T_k^2 \circ \cdots \circ T_k^d (1 \le k \le n)$，算法结束。其中“$\circ$”表示图像的拼接，拼接的方式不受限制，既可以是行向拼接，也可以是纵向拼接，或者按矩形拼接。

5 实验与分析

本文方案与其他异或视觉密码方案的比较见表3，可得如下结论：(1)在存取结构方面，只有文献[14]和本文方案适用于通用存取结构。(2)在恢复效果方面，只有文献[13, 14]和本文方案可以实现完全恢复。(3)在恢复算法方面，仅文献[13]需要借助于计算机实现，而其余方案均可以通过 XOR 运算直接恢复。(4)在每个参与者持有的共享份数量上，文献[14]可能持有多个共享份，而且各参与者的共享份数量不同，在恢复秘密图像时需要根据授权子集而选择相应的共享份。(5)在像素扩展度方面，文献[11]较大，文献[12,13]较小，但文献[12]不能实现完全恢复，文献[13]则需要借助于计算机实现，文献[14]由于各参与者的共享份数量不同，因此采用平均像素扩展度(Average Pixel Expansion, APE)作为衡量指标，本文的像素扩展度则等于划分理想存取结构的个数 d。表 4 列出了本文方案与文献[11]像素扩展度的比较，括号里面表示文献[11]的结果。

以(3,6)视觉密码方案为例，对本文提出的方案进行实验仿真。首先根据理想存取结构的划分算法可以得到：Γ_0^1={ {123}, {124}, {125}, {136}, {146}, {156}}, Γ_0^2 ={{134}, {234}, {345}, {346}}, Γ_0^3 = { {126}, {246}, {256},{236} }, Γ_0^4 ={{135}, {145}, {235}, {245}, {456} , {356}}，然后按照第 4 节提出的秘密分享与恢复算法有：

对于 Γ_0^1，有 $T_1^1 = K_1^1$, $T_2^1 = T_6^1 = K_2^1$, $T_3^1 = T_4^1 = T_5^1 = S \oplus K_1^1 \oplus K_2^1$。

对于 Γ_0^2，有 $T_1^2 = T_2^2 = T_5^2 = T_6^2 = K_1^2$, $T_3^2 = K_2^2$, $T_4^2 = S \oplus K_1^2 \oplus K_2^2$。

对于 Γ_0^3，有 $T_1^3 = T_3^3 = T_4^3 = T_5^3 = K_1^3$, $T_2^3 = K_2^3$, $T_6^3 = S \oplus K_1^3 \oplus K_2^3$。

对于 Γ_0^4，有 $T_1^4 = T_2^4 = T_6^4 = K_1^4$, $T_3^4 = T_4^4 = K_2^4$, $T_5^4 = S \oplus K_1^4 \oplus K_2^4$。

其中 $K_i^j (1 \le i \le 2, 1 \le j \le 4)$ 表示与秘密图像 S 规模相同的随机数序列。

将各子共享份拼接可以得到最终的共享份，即 $T_k = T_k^1 \circ T_k^2 \circ T_k^3 \circ T_k^4 (1 \le k \le 6)$，实验结果如图 3 所示。为节省空间将视觉效果相近的恢复图像进行了约简，比如单个共享份都是杂乱无章的，故用一幅图像表示，但不表示各共享份是相同的。又如 $T_{1\oplus 3}$ 与 $T_{1\oplus 4}$ 均在左下角呈现空白，但 $T_{1\oplus 3}$ 与 $T_{1\oplus 4}$ 其它部分的图像仅是相似，而非相同。

分析图 3 的实验结果可知：(1)1 个共享份和 2 个共享份 XOR 运算的结果是杂乱无章的，与预计的结果相同。3 个共享份 XOR 运算后，能够利用视觉系统分辨出秘密图像的全部信息。而文献[11]的 3 个共享份 XOR 结果显然存在严重的失真，其像素扩展度为 10，相对差为 2/5。(2)2 个共享份 XOR 运算后有一部分是全白，原因是在相应的理想结构里共享份的赋值相同；3 个共享份 XOR 运算后，根据参与者集合所属的理想存取结构，秘密图像出现在对应的区域。

表3 本文方案与其他异或视觉密码方案的比较

	文献[11]	文献[12]	文献[13]	文献[14]	本文方案
存取结构	(k, n)门限结构	$(2, n)$门限结构	(k, n)门限结构	通用存取结构	通用存取结构
完全恢复	否	否	是	是	是
恢复算法	XOR 运算	XOR 运算	借助计算机	XOR 运算	XOR 运算
每个参与者的共享份数量	1 个	1 个	1 个	多个	1 个
像素扩展度	$2^{k-1}\binom{n}{k}$	1	$\frac{2(n-k+1)}{n}$	APE	d

表4 本文方案与文献[11]像素扩展度的比较

k	n				
	2	3	4	5	6
2	1(1)	2(2)	2(2)	3(3)	3(3)
3		1(1)	2(6)	3(8)	4(10)
4			1(1)	3(15)	5(24)
5				1(1)	3(30)
6					1(1)

6 结束语

本文给出了理想存取结构的必要条件，提出了将通用存取结构划分为若干理想存取结构的算法，设计了通用存取结构下的异或方案的秘密分享算法和恢复流程。研究如何将通用存取结构划分为数量最少的理想存取结构，以及(k, n)门限结构划分的一般规律，是本文进一步的研究方向。

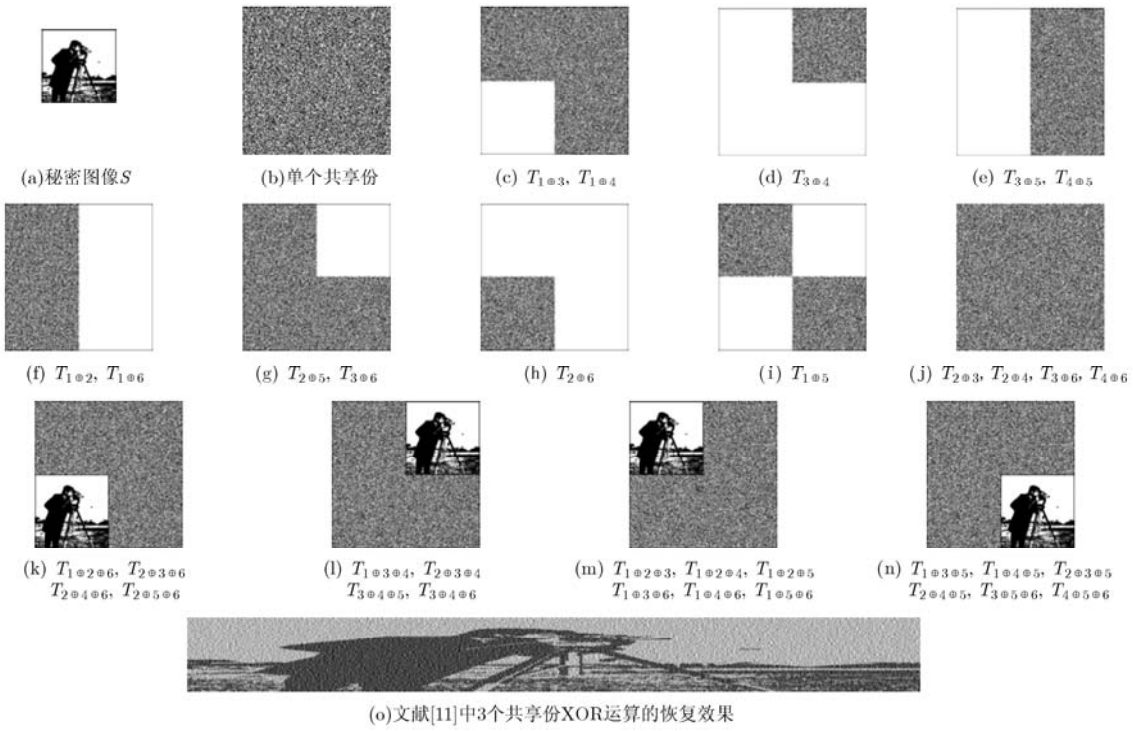

图3　(3,6)异或视觉密码方案的实验效果

参 考 文 献

[1] Naor M and Shamir A. Visual cryptography[J]. *LNCS*, 1995, 950: 1–12.

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

[3] Fu Z X, Yu B, and Fang L G. The access-based multi-secret visual cryptography with compression algorithm[J]. *Journal of Electronics & Information Technology*, 2013, 35(5): 1055–1062.

[4] Chen T H and Li K C. Multi-image encryption by circular random grids[J]. *Information Sciences*, 2012, 189(1): 255–265.

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

[6] Li P, Ma P J, Su X H, *et al.*. Multi-threshold image secret sharing scheme[J]. *Acta Electronica Sinica*, 2012, 40(3): 518–524.

[7] Yang C N, Shih H W, Wu C C, *et al.*. k out of n region incrementing scheme in visual cryptography[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2012, 22(5): 799–810.

[8] Biham E and Itzkovitz A. Visual cryptography with polarization[EB/OL]. http: //www.cs.technion.ac.il/biham/reports/visual.ps.gz, 1997.

[9] Viet D Q and Kurosawa K. Almost ideal contrast visual cryptography with reversing[J]. *LNCS*, 2004, 2964: 353–365.

[10] Yang C N, Wang C, and Chen T. Visual cryptography schemes with reversing[J]. *The Computer Journal*, 2008, 51(6): 710–722.

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

[12] Wang D S, Zhang L, Ma N, *et al.*. Two secret sharing schemes based on Boolean operations[J]. *Pattern Recognition*, 2007, 40(10): 2776–2785.

[13] Chao K Y and Lin J C. Secret image sharing: a Boolean operations based approach combining benefits of polynomial-based and fast approaches[J]. *International Journal of Pattern Recognition and Artificial Intelligence*, 2009, 23(2): 263–285.

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

付正欣：　男，1986 年生，博士生，研究方向为视觉密码.

沈　刚：　男，1986 年生，博士生，研究方向为视觉密码.

孔志印：　男，1964 年生，高级工程师，主要研究方向为信息安全.

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.