(k, n)异或视觉密码的一般性研究

沈 刚 付正欣* 郁 滨
(信息工程大学 郑州 450004)

摘 要：通过研究(k, n)异或视觉密码像素扩展度最优的必要条件，该文提出一种由基矩阵生成(k, n)异或视觉密码的方法，并从理论上证明了该方法适合 $2<k\leq n$ 的(k, n)异或视觉密码，在此基础上构造了秘密分享和恢复算法。实验结果表明，该文方案可以有效地减小像素扩展度，且能够实现秘密图像的完全恢复。

关键词：异或视觉密码；(k, n)门限结构；像素扩展度最优的必要条件；完全恢复
中图分类号：TP309.7 **文献标识码**： A **文章编号**：1009-5896(2013)10-2294-07
DOI：10.3724/SP.J.1146.2012.01719

On the Generality of (k, n) XOR-based Visual Cryptography Scheme

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

Abstract: The necessary condition of the optimal pixel expansion is given and proved in (k, n) XOR-based Visual Cryptography Scheme (XVCS). A new method is designed for constructing (k, n)-XVCS by use of basis matrices. The method is proved to be suitable for (k, n)-XVCS with $2< k \leq n$. Based on the above results, the secret sharing and recovering algorithms are proposed. The experimental results show that the pixel expansion can be decreased efficiently. Furthermore, the secret images can be recovered perfectly.

Key words: XOR-based Visual Cryptography (XVC); (k, n) threshold structure; Necessary condition of optimal pixel expansion; Perfect recovery

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，其命名源于利用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。经过近二十年的发展，视觉密码在理论完善[4–6]、算法优化[7–9]和方案应用[10–12]方面取得了长足的进展。

视觉密码的设计初衷是解决恢复操作的简便性问题。受到当时计算设备不够普及的限制，视觉密码的共享份一般是以透明胶片为载体，解密图像则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运算(OR)，其代数结构为加法半群，致使白像素无法完全恢复，因此恢复图像存在形状和面积上的失真。

为了突破半群结构的限制，Biham 等人[13]提出了基于偏振光的视觉密码，恢复像素的颜色不再是共享份像素 OR 运算的结果，而是由共享份偏振方向的平行或正交来决定，实现了 XOR 运算的效果，但只适应于(2, 2)方案。这种基于偏振光的方案与基于透明胶片的视觉密码相比，大大改善了恢复图像的质量，能够完全恢复秘密图像。虽然秘密恢复所需的光学设备不利于推广实现，但由于其在秘密恢复时的代数结构发生了变化，使视觉密码突破以透明胶片为载体的限制成为可能。

此后，Hu 等人[14]将取反操作引入方案设计，提出了衡量视觉密码计算复杂性的因素：叠加和反转的次数，设计了一种只需要两次运算即可完全恢复的反转视觉密码，但图像按区域恢复，出现了位置失真。Yang 等人[15]引入反转算子(reversing)，将异或运算分解为简单的或、非运算，通过有限步的迭代可以完全恢复原图像的黑白像素。反转算子在具体实现时可借助于复印机，虽然脱离了计算设备，保持了视觉密码恢复简便的特点，但该方案恢复算法需要多次迭代，增加了计算复杂度。Wang 等人[16]结合或运算和异或运算设计了一种$(2, n)$方案，实现了共享份与秘密图像尺寸相同，但恢复图像的视觉效果是概率性的(probabilistic)。在 Wang 等人[16]方案的基础上，Chao 等人[17]设计了一种(k, n)方案，构造了 $n\times\binom{n}{k-1}$ 的共享份分配矩阵(shadows-

2012-12-27 收到，2013-03-15 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

assignment matrix)，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，然后进行异或运算，因此必须借助计算机上实现。

Tuyls 等人[18]给出(k, n)异或视觉密码方案(XOR-based Visual Cryptography Scheme, XVCS)的定义，并构造了完全恢复的(n, n)方案，证明了$(2, n)$方案与二值纠错码的等价关系，对于$2<k<n$的(k, n)方案，则通过基矩阵(basis matrices)予以实现。文献[18]在$k=2$和$k=n$时取得了较好的研究结果：$k=2$时像素扩展度为$\lceil \log_2 n \rceil$且相对差为$\lceil \log_2 n \rceil^{-1}$，$k=n$时像素扩展度和相对差均为 1。但$(2, n)$和$(n, n)$方案的设计方法并不适用于一般的$(k, n)$方案，且当$2<k<n$时$(k, n)$方案的恢复效果与 OR 运算相比优势不明显，因此关于(k, n)方案的一般特性有待进一步的研究。

本文首先给出了(k, n)-XVCS 像素扩展度最优的必要条件，揭示了(k, n)-XVCS 在设计时应遵循的基本原则。在满足必要条件的前提下，提出了一种由基矩阵生成(k, n)-XVCS 的方法，设计了完整的秘密分享和恢复算法，并在恢复算法中实现了秘密图像的完全恢复，且不增加恢复操作的计算复杂度。

2　基本概念

2.1 异或视觉密码定义

设 n 表示参与者的数量，k 表示恢复秘密图像的门限值，k, n 是非负整数，且$2 \le k \le n$。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。

定义 1[18]　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(k, n)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，在分享白(黑)像素时从 $C_0(C_1)$ 中随机选取一个矩阵，对应 n 个共享份各自的 m 个子像素。C_0, C_1 满足以下两个条件：

(1) 当 $|X|=k$ 时，设 $\boldsymbol{M}_0 \in C_0$，$\boldsymbol{M}_1 \in C_1$，则 $H(\mathrm{XOR}(\boldsymbol{M}_0[X])) \le h$，$H(\mathrm{XOR}(\boldsymbol{M}_1[X])) \ge l$。

(2) 当 $1 \le |X| < k$ 时，记 $D_0=\{\boldsymbol{M}[X] \mid \boldsymbol{M} \in C_0\}$，$D_1=\{\boldsymbol{M}[X] \mid \boldsymbol{M} \in C_1\}$，则 $D_0=D_1$。

其中，条件(1)是对比性条件，表明当参与者人数等于 k 个时，通过异或运算能够恢复秘密图像。条件(2)是安全性条件，表明当参与者人数小于 k 个时，得不到秘密图像的任何信息。h 表示恢复图像中原白像素对应子像素块的最大汉明重量，l 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。$\alpha=(l-h)/m$ 称为相对差，表示恢复图像与原图像在视觉上的差别，其越大越好。当 $m=1$ 且 $\alpha=1$ 时，恢复图像与秘密图像一致，即完全恢复。

关于定义 1 有两点补充说明：(1) 当 $|X| > k$ 时，Tuyls 等人认为取 X 中的 k 个参与者即可恢复秘密图像，因此不需要直接计算 X 中所有的共享份；(2) 相对差 α 的定义有多种，比如 $(l-h)/m$，$(l-h)/(l+h)$，$(l-h)/m(l+h)$ 等等，本文采用最常见的 $\alpha=(l-h)/m$。

m 和 α 是衡量视觉密码的两个重要指标，关于 m 和 α 的优化问题一直是视觉密码研究的热点和难点。对于定义 1 的(k, n)-XVCS，本文在恢复操作中增加阈值过滤环节即可实现秘密图像的完全恢复，具体流程见 3.2 节。考虑到相对差 α 的最优化实现简单，本文主要研究影响共享份尺寸的像素扩展度 m 的优化问题。

2.2 基于基矩阵的(k, n)-XVCS

当$2<k<n$时，(k, n)-XVCS 的构造与基于 OR 运算的(k, n)-VCS 类似，即首先设计满足定义 1 两个条件的基矩阵 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$，然后以列为单位对 $\boldsymbol{B}_0$ ($\boldsymbol{B}_1$) 进行全排列，排列得到的所有矩阵组成 $\boldsymbol{C}_0$ ($\boldsymbol{C}_1$)。设 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 的大小均为 $n \times m_b$，则 $|\boldsymbol{C}_0| = |\boldsymbol{C}_1| = m_b!$。

例 1　(3, 4)-XVCS 的构造

首先构造基矩阵 $\boldsymbol{B}_0=\begin{bmatrix}000111\\001011\\001101\\001110\end{bmatrix}$，$\boldsymbol{B}_1=\begin{bmatrix}000111\\001011\\010011\\100011\end{bmatrix}$，然后对 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 按列进行全排列，得到

$$\boldsymbol{C}_0=\left\{\begin{bmatrix}000111\\001011\\001101\\001110\end{bmatrix},\begin{bmatrix}001110\\010110\\011010\\011100\end{bmatrix},\cdots,\begin{bmatrix}111000\\110100\\101100\\011100\end{bmatrix}\right\}$$

$$\boldsymbol{C}_1=\left\{\begin{bmatrix}000111\\001011\\010011\\100011\end{bmatrix},\begin{bmatrix}001110\\010110\\100110\\000111\end{bmatrix},\cdots,\begin{bmatrix}111000\\110100\\110010\\110001\end{bmatrix}\right\}$$

通过研究(n, n)-XVCS 和$(2, n)$-XVCS 发现，$\boldsymbol{C}_0$ ($\boldsymbol{C}_1$)的元素之间不必存在列排序的关系。比如在

设计$(n,\ n)$-XVCS 时，$\boldsymbol{C}_0$由所有汉明重量为偶数的$1\times n$矩阵组成，$\boldsymbol{C}_1$由所有汉明重量为奇数的$1\times n$矩阵组成，具体见例 2；在设计$(2,\ n)$-XVCS 时，首先设计二值纠错码(binary error-correcting codes)，然后转换成矩阵集合$\boldsymbol{C}_0$和$\boldsymbol{C}_1$，具体见例 3。

例 2 (2, 2)-XVCS

$$\boldsymbol{C}_0=\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right\},\ \boldsymbol{C}_1=\left\{\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\right\}$$

例 3 (2, 4)-XVCS

首先构造(2, 4, 1)二值纠错码{[00], [10], [01], [11]}，$\boldsymbol{C}_0$中的矩阵元素每行均由同一个码元构成，$\boldsymbol{C}_1$中的矩阵元素包含所有的码元，且各矩阵是以行为单位的循环移动的关系，具体地，

$$\boldsymbol{C}_0=\left\{\begin{bmatrix}00\\00\\00\\00\end{bmatrix},\begin{bmatrix}01\\01\\01\\01\end{bmatrix},\begin{bmatrix}10\\10\\10\\10\end{bmatrix},\begin{bmatrix}11\\11\\11\\11\end{bmatrix}\right\},\ \boldsymbol{C}_1=\left\{\begin{bmatrix}00\\01\\10\\11\end{bmatrix},\begin{bmatrix}01\\10\\11\\00\end{bmatrix},\begin{bmatrix}10\\11\\00\\01\end{bmatrix},\begin{bmatrix}11\\00\\01\\10\end{bmatrix}\right\}$$

综上，研究$2<k<n$时由基矩阵$\boldsymbol{B}_0$和$\boldsymbol{B}_1$产生矩阵集合$\boldsymbol{C}_0$和$\boldsymbol{C}_1$时应遵循的基本原则及具体方法，是$(k,\ n)$-XVCS 的重要问题。

3 $(k,\ n)$-XVCS 设计

本节首先给出并证明了$(k,\ n)$-XVCS 像素扩展度最优的必要条件，提出了满足该必要条件的由基矩阵生成矩阵集合的方法。在此基础上，设计了秘密分享与恢复算法。

3.1 像素扩展度最优的必要条件

对于一般的$(k,\ n)$-XVCS，设其基矩阵为$\boldsymbol{B}_0$和$\boldsymbol{B}_1$，大小均为$n\times m_b$。由于矩阵集合$\boldsymbol{C}_0$和$\boldsymbol{C}_1$分别由$\boldsymbol{B}_0$和$\boldsymbol{B}_1$生成，根据定义 1，则 h 是$\boldsymbol{B}_0$中任意 k 行 XOR 运算得到向量的汉明重量最大值，l是$\boldsymbol{B}_1$中任意 k行 XOR 运算得到向量的汉明重量最小值，即

$$h=\max\left\{H\left(\mathrm{XOR}(\boldsymbol{B}_0[X])\right)\right\},X\subseteq\{1,2,\cdots,n\},|\,X\,|=k$$

$$l=\min\left\{H\left(\mathrm{XOR}(\boldsymbol{B}_1[X])\right)\right\},X\subseteq\{1,2,\cdots,n\},|\,X\,|=k$$

定理 1 设$(k,\ n)$-XVCS 的基矩阵为$\boldsymbol{B}_0$和$\boldsymbol{B}_1$，其像素扩展度为m_b。若$l-h\geq 2$，则一定存在另一个$(k,\ n)$-XVCS，其像素扩展度为 m，且$m<m_b$，$\alpha=1/m$。

证明 令$m=m_b+h-l+1$，$\boldsymbol{C}_0=P(\boldsymbol{B}_0,m)$，$\boldsymbol{C}_1=P(\boldsymbol{B}_1,m)$，其中$P(\boldsymbol{B},m)$表示从矩阵$\boldsymbol{B}$中任取 m 列组成的所有矩阵的集合，且$|\,\boldsymbol{C}_0\,|=|\,\boldsymbol{C}_1\,|=\prod_{i=0}^{m-1}(m_b-i)$。

(1)安全性证明 设参与者集合$X=\{i_1,i_2,\cdots,i_p\}$，$|\,X\,|=p$。当$1\leq p<k$时，记$D_0=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in\boldsymbol{C}_0\}$，$D_1=\{\boldsymbol{M}[X]\,|\,\boldsymbol{M}\in\boldsymbol{C}_1\}$，其中$\boldsymbol{M}[X]$表示矩阵$\boldsymbol{M}$中第$i_1,i_2,\cdots,i_p$行组成的子矩阵。

$\forall\boldsymbol{M}_0\in D_0$，由于$\boldsymbol{C}_0=P(\boldsymbol{B}_0,m)$，则$\boldsymbol{M}_0$由$\boldsymbol{B}_0[X]$中的 m 列组成。不妨设$\boldsymbol{M}_0$由$\boldsymbol{B}_0[X]$中的第$j_1,j_2,\cdots,j_m$列组成。由于$\boldsymbol{B}_0$和$\boldsymbol{B}_1$是 XVCS 的基矩阵，根据定义 1 的安全性，则$\boldsymbol{B}_0[X]$和$\boldsymbol{B}_1[X]$包含相同的列向量，仅排列顺序不同。设$\boldsymbol{B}_0[X]$中的第$j_1,j_2,\cdots,j_m$列在$\boldsymbol{B}_1[X]$中的列序号分别为$j_1',j_2',\cdots,j_m'$，记$\boldsymbol{M}_1$由$\boldsymbol{B}_1[X]$中的第$j_1',j_2',\cdots,j_m'$列组成，则$\boldsymbol{M}_1\in D_1$。由于$\boldsymbol{B}_0[X]$中的第$j_1,j_2,\cdots,j_m$列分别与$\boldsymbol{B}_1[X]$中的第$j_1',j_2',\cdots,j_m'$列相等，因此$\boldsymbol{M}_0=\boldsymbol{M}_1$。上述结果表明：对于$D_0$中的任意一个矩阵$\boldsymbol{M}_0$，总可以在$D_1$中找到一个矩阵$\boldsymbol{M}_1$与之相等，即$D_0\subseteq D_1$。

同理可证明对于D_1中的任意一个矩阵$\boldsymbol{M}_1$，总可以在D_0中找到一个矩阵$\boldsymbol{M}_0$与之相等，即$D_1\subseteq D_0$。因此$D_0=D_1$，即$\boldsymbol{C}_0$和$\boldsymbol{C}_1$满足$(k,\ n)$-XVCS 的安全性条件。

(2)对比性证明 当$|\,X\,|=k$时，$\forall\boldsymbol{M}_0\in\boldsymbol{C}_0$，$\boldsymbol{V}_0=\mathrm{XOR}(\boldsymbol{M}_0[X])$，由于$m-h=m_b-l+1\geq 1$，因此$\boldsymbol{V}_0$中最多有 h 个‘1’，即$H\left(\mathrm{XOR}(\boldsymbol{M}_0[X])\right)\leq h$。

$\forall\boldsymbol{M}_1\in\boldsymbol{C}_1,\boldsymbol{V}_1=\mathrm{XOR}(\boldsymbol{M}_1[X])$，由于$m-(m_b-l)=h+1\geq 1$，则$\boldsymbol{V}_1$最多有$(m_b-l)$个‘0’，因此$\boldsymbol{V}_1$中最少有$m-(m_b-l)$个‘1’，即$H\left(\mathrm{XOR}(\boldsymbol{M}_1[X])\right)\geq m-(m_b-l)=m-m_b+l=h+1$。由于$h+1>h$，故$\boldsymbol{C}_0$和$\boldsymbol{C}_1$满足定义 1 中的对比性条件。

综上，$\boldsymbol{C}_0$和$\boldsymbol{C}_1$组成了一个新的$(k,\ n)$-XVCS，其像素扩展度为$m=m_b+h-l+1<m_b$，$\alpha=(h+1-h)/m=1/m$。 证毕

定理 2 对于$(k,\ n)$-XVCS，$l-h=1$是像素扩展度 m 最优的必要条件。

证明 设$l-h\geq 2$时，$(k,\ n)$-XVCS 的像素扩展度是最优的，记为 m。根据定理 1，必然存在一个像素扩展度$m'<m$的$(k,\ n)$-XVCS，与 m 是$(k,\ n)$-XVCS 的最优像素扩展度矛盾，因此$l-h\leq 1$。又$l-h\geq 1$，因此$l-h=1$。 证毕

推论 1 在$(k,\ n)$-XVCS 中，$m=1$与$\alpha=1$是等价的。

证明 (1)当 $m=1$ 时，由于$0\leq h<l\leq m$，因此 $h=0$, $l=1$，故$\alpha=(l-h)/m=1$。

(2)当$\alpha=1$时，由于$\alpha=(l-h)/m$，因此$l-h=m$。若 $m>1$，根据定理 1，必然存在一个$m'=m+h-l+1=1$的视觉密码方案。若 $m=1$，则直接有$\alpha=1\Rightarrow m=1$。

综上，$m=1$与$\alpha=1$是等价的。 证毕

推论 2 当$1<k<n$时，不存在$\alpha=1$的$(k,\ n)$-XVCS。

证明 文献[18]的命题 6 指出，当$1<k<n$时，不存在 $m=1$ 的$(k,\ n)$-XVCS。根据推论 1，则不存

在$\alpha=1$的(k, n)-XVCS。　　证毕

推论 2 说明，当$1<k<n$时，对(k, n)-XVCS 的共享份进行 XOR 运算无法得到完全恢复的秘密图像。

推论 3　(n, n)-XVCS 的$m=1$且$\alpha=1$。

证明　首先构造(n, n)-XVCS 的基矩阵，令$\boldsymbol{B}_0$由所有汉明重量为偶数的$1\times n$向量组成，$\boldsymbol{B}_1$由所有汉明重量为奇数的$1\times n$向量组成，则$m_b=2^{n-1}$，$h=0$，$l=2^{n-1}$。根据定理 1，必然存在一个$m=m_b+h-l+1=2^{n-1}+0-2^{n-1}+1=1$，$\alpha=1/m=1$的$(n, n)$-XVCS。　　证毕

推论 3 说明(n, n)-XVCS 是(k, n)-XVCS 的特殊情况。

推论 4　存在像素扩展度为 $2n-5$ 的$(3, n)$-XVCS。

证明　由文献[18]可知，存在$m_b=2n-2$，$h=n-3$，$l=n+1$的$(3, n)$-XVCS。根据定理 1，必然存在$m=2n-2+n-3-(n+1)+1=2n-5$的$(3, n)$-XVCS。　　证毕

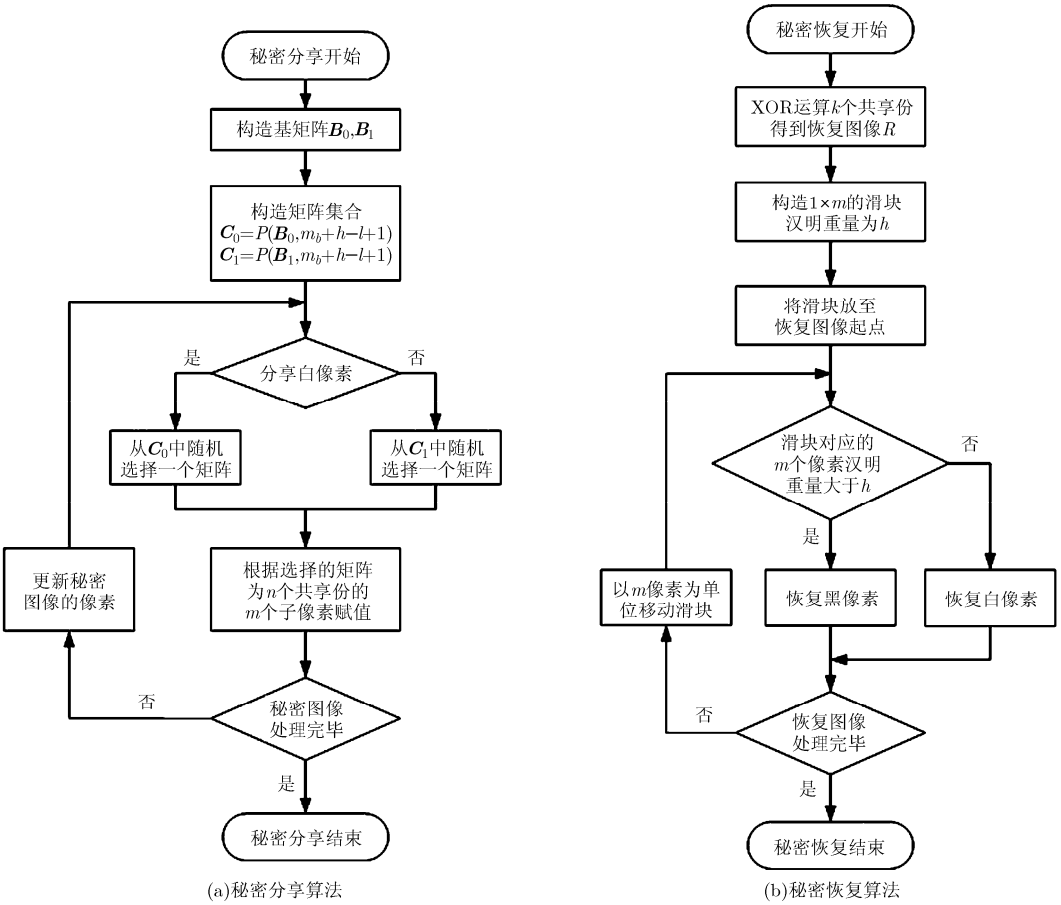
推论 5　存在像素扩展度为$2^{k-1}\binom{n}{k}-2^{k-1}+1$的$(k, n)$-XVCS。

证明　由文献[18]，存在$m_b=2^{k-1}\binom{n}{k}$，$h=2^{k-2}\left[\binom{n}{k}+\binom{n-k}{k}-1\right]$，$l=2^{k-2}\left[\binom{n}{k}+\binom{n-k}{k}+1\right]$的$(k, n)$-XVCS。根据定理 1，必然存在$m=m_b+h-l+1=2^{k-1}\binom{n}{k}-2^{k-1}+1$的$(k, n)$-XVCS。　　证毕

3.2 秘密分享与恢复算法

根据定理 2，设计秘密分享与恢复算法，具体流程如图 1 所示。

在(k, n)-XVCS 的算法流程图中，有两点需要说明。(1)在图 1(a)秘密分享算法中，基矩阵$\boldsymbol{B}_0, \boldsymbol{B}_1$构造是采用其它文献的结果，不是本文的研究重点。(2)在图 1(b)秘密恢复算法中，完全恢复操作会带来额外的计算开销，但不会增加恢复算法的计算复杂度的阶数。设秘密图像S的尺寸为$a\times b$，k个共享份通过光学仪器或可反转的复印机实现异或运算，得到尺寸为$a\times(m\cdot b)$的恢复图像R，计算量为$a\cdot b\cdot(k-1)$次运算。在此基础上，构造汉明重量为h的$1\times m$的滑块，增加$a\cdot b$次滑块移动操作和$a\cdot b$次阈值比较操作即可实现图像的完全恢复，而且恢复



(a)秘密分享算法　　(b)秘密恢复算法

图 1 (k, n)-XVCS 的算法流程图

表 1 本文方案与其它异或视觉密码方案的比较

算法	存取结构	像素扩展度		完全恢复	恢复算法的计算复杂度
文献[16]	$(2, n)$	1		N	$O(1)$
文献[17]	(k, n)	1		Y	$O\left(\begin{matrix} n \\ k-1 \end{matrix}\right)$
文献[18]	(k, n)	$(2, n)$	$\lceil \log_2 n \rceil$	N	$O(k)$
		$(3, n)$	$2n-2$		
		(k, n)	$2^{k-1}\left(\begin{matrix} n \\ k \end{matrix}\right)$		
		(n, n)	1		
本文算法	(k, n)	$(2, n)$	$\lceil \log_2 n \rceil$	Y	$O(k)$
		$(3, n)$	$2n-5$		
		(k, n)	$2^{k-1}\left(\begin{matrix} n \\ k \end{matrix}\right)-2^{k-1}+1$		
		(n, n)	1		

算法的计算复杂度仍然保持在 $O(k)$。其中，阈值比较操作是指当恢复图像 m 个像素的汉明重量大于 h 时恢复黑像素，否则恢复白像素。

4 实验分析

在评价异或视觉密码方案时，除了像素扩展度和恢复效果之外，方案所适用的存取结构以及恢复算法的计算复杂度也是重要的性能指标。本文方案与其它异或视觉密码方案的比较见表 1。从表中可以看出，文献[16]的像素扩展度和计算复杂度最小，但只适用于$(2, n)$的存取结构，而且方案无法实现完全恢复；文献[17]在存取结构，像素扩展度和恢复效果方面都是最优的，但其必须借助于计算机实现，而且计算复杂度最大；文献[18]的计算复杂度较小，且方案实现不依赖计算机，但其像素扩展度和恢复效果最差；本文方案适用于(k, n)门限存取结构，可以实现完全恢复，同时计算复杂度与文献[18]相同，而且当 $1<k<n$ 时像素扩展度与文献[18]相比有明显改进。

以$(3, 4)$视觉密码方案为例，对本文提出的方案进行实验仿真。

首先构造基矩阵 $\boldsymbol{B}_0=\begin{bmatrix}000111\\001011\\001101\\001110\end{bmatrix}$, $\boldsymbol{B}_1=\begin{bmatrix}000111\\001011\\010011\\100011\end{bmatrix}$，则 $m_b=6, h=1, l=5$。根据定理 1，令 $C_0=P(\boldsymbol{B}_0,3)$，表示从矩阵 $\boldsymbol{B}_0$ 中任取 3 列组成的所有矩阵的集合，且 $|\boldsymbol{C}_0|=A(6,3)=90$。同理，$\boldsymbol{C}_1=P(\boldsymbol{B}_1,3)$，具体有

$$\boldsymbol{C}_0=\left\{\begin{bmatrix}000\\001\\001\\001\end{bmatrix},\begin{bmatrix}001\\000\\001\\001\end{bmatrix},\cdots,\begin{bmatrix}111\\011\\101\\110\end{bmatrix}\right\}$$

$$\boldsymbol{C}_1=\left\{\begin{bmatrix}000\\001\\010\\100\end{bmatrix},\begin{bmatrix}001\\000\\010\\100\end{bmatrix},\cdots,\begin{bmatrix}111\\011\\011\\011\end{bmatrix}\right\}$$

按照第 3 节提出的秘密分享与恢复算法，得到实验结果如图 2 所示。

分析图 2 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信息。实验结果体现了本文方案满足定义 1 的对比性和安全性条件。

(2)通过秘密恢复算法的完全恢复流程，能够实现秘密图像的完全恢复。另外，若恢复图像时不具备实现滑块移动和阈值比较的计算环境，则只需对共享份进行 XOR 运算也可以恢复秘密图像(图 2(d))，但存在失真，即 $m=3, \alpha=1/3$。

(3)文献[16]只适用于$(2, n)$方案，无法用于$(3, 4)$方案。文献[17]的恢复效果如图 2(f)所示，与本文算法加入阈值计算的恢复图像图 2(e)相同，但计算复杂度却比本文算法更大。文献[18]的恢复效果如图 2(g)所示，与本文算法中 3 个共享份 XOR 运算的恢复效果 2(d)相比，显然存在更大的形状失真。

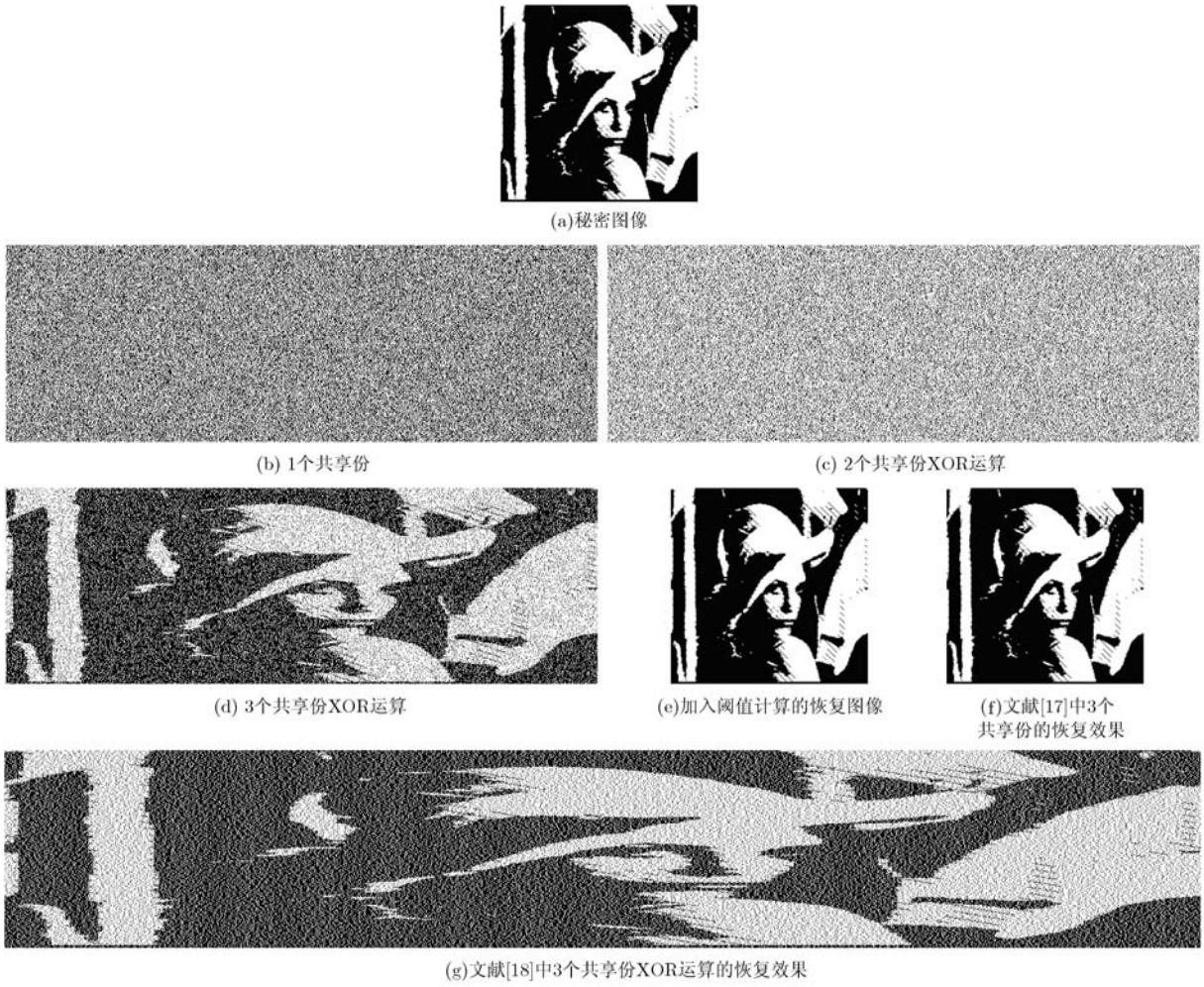


图 2　(3, 4)-XVCS 的实验效果图

5　结束语

本文对$(k,\ n)$-XVCS 的一般特性展开研究，给出并证明了像素扩展度最优的必要条件，提出了适用于$2 < k \le n$的$(k,\ n)$-XVCS 基矩阵产生视觉密码方案的方法，设计了分享算法和恢复流程。同时，秘密恢复算法实现了图像完全恢复，且计算复杂度仍为 $O(k)$。本文仅证明了像素扩展度最优的必要条件，关于其充分条件有待进一步的研究。

参 考 文 献

[1] Naor M and Shamir A. Visual cryptography[J]. *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, Santis A D, *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 B, Lu J Y, and Fang L G. 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(4): 261–289.

[8] 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.

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

[10] Guo J, Soo C, and Lee H. Watermarking in halftone images

with parity-matched error diffusion[J]. *Signal Processing*, 2011, 91(1): 126–135.

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

[12] 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.

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

[14] Hu C and Tzeng W. Compatible ideal contrast visual cryptography schemes with reversing[J]. *LNCS*, 2005, 3650: 300–313.

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

[16] 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.

[17] 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.

[18] 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.

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.

沈 刚： 男，1986年生，硕士生，研究方向为视觉密码.