第 34 卷第 3 期 通 信 学 报 Vol.34 No. 3
2013 年 3 月 Journal on Communications March 2013
doi:10.3969/j.issn.1000-436x.2013.03.021

无损分享视觉密码研究

郁滨，付正欣
(信息工程大学 电子技术学院，河南 郑州 450004)

摘 要：根据秘密图像分享过程中的信息损失，给出了无损分享视觉密码的概念，从而将视觉密码 2 个参数的优化问题简化为一个，并提出了矩阵转化算法和整数规划模型，实现了一种像素扩展度的优化算法。实验结果表明，该算法能够实现无损分享下的像素扩展度最优化，且适用于通用存取结构。

关键词：视觉密码；无损分享；像素扩展度；优化算法
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000-436X(2013)03-0165-06

Lossless sharing visual cryptography

YU Bin, FU Zheng-xin
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract: According to the information loss during the secret image sharing process, the lossless sharing visual cryptography was proposed. The optimizations of two parameters were simplified into one parameter. The matrices translation algorithm and the integer programming model were designed. Furthermore, the pixel expansion optimization algorithm was realized. The experimental results show that the algorithm achieves the optimal pixel expansion under lossless sharing, and can be used in general access structure.

Key words: visual cryptography; lossless sharing; pixel expansion; optimization algorithm

1 引言

视觉密码[1](visual cryptography)是一种新的图像分存技术，它将秘密共享和数字图像相结合，经过 10 多年的不断丰富和发展，已经成为密码学的一个新的研究方向，并从最初的(2, 2)方案发展成为一个相对完善的理论体系。

视觉密码通过秘密分享算法将秘密图像编码成为若干个共享份，并分发给每个参与者。当参与者集合满足约定的恢复条件时，只需将参与者的共享份直接叠加即可恢复出秘密图像。由于视觉密码的秘密恢复过程简单，因此视觉密码的研究重点主要集中于秘密分享算法。

以基矩阵为核心的秘密分享算法由 Naor 和 Shamir 最先提出，由于其能够保证视觉密码方案的安全性和对比性条件，因而基矩阵的设计是视觉密码方案的关键。Naor 和 Shamir[1]证明了(n, n)方案的最小像素扩展度为 2^{n-1}，并给出了基矩阵的构造方法，即 $\boldsymbol{B}_0$（分享白像素的基矩阵）由所有汉明重量为偶数的列向量组成，$\boldsymbol{B}_1$（分享黑像素的基矩阵）由所有汉明重量为奇数的列向量组成。Bludno 等[2]证明了$(2, n)$门限方案的最小像素扩展度为满足 $C(m,\lceil m/2\rceil)\geq n$ 的最小 m 值，在基矩阵设计时，$\boldsymbol{B}_0$ 由 n 个相同的汉明重量为 $\lceil m/2\rceil$ 的行向量组成，而 $\boldsymbol{B}_1$ 由 n 个不同的汉明重量为 $\lceil m/2\rceil$ 的行向量组成。Droste[3]提出了 ADD 算子，用以在(n, n)方案基础上动态增加列向量，可以有效地减小(k, n)门限方案的像素扩展度，同时还提出利用线性规划的方法设计基矩阵，但由于规划模型的解不是整数，因此并不具有实际的意义。Ateniese 等[4]通过定义授权

收稿日期：2011-08-22；修回日期：2012-05-07
基金项目：国家自然科学基金资助项目(61070086)；河南省杰出人才创新基金资助项目(094100510002)
Foundation Items: The National Natural Science Foundation of China(61070086); The Excellent Youth Foundation of Henan Scientific Committee(094100510002)

集合 G_{Qual} 和禁止集合 G_{Forb}，将视觉密码由门限结构扩展到通用存取结构，并提出了2种经典的基矩阵构造方法，即基于累积矩阵方法和小方案扩展方法，广泛地应用于通用存取结构的方案。Hajiabolhassan[5]研究了几种特殊的通用存取结构，讨论了其像素扩展度的界限，并提出了相应的基矩阵设计方法。研究表明，基矩阵的列数代表图像面积上扩大的倍数，而以基矩阵为核心的视觉密码方案无法达到像素扩展度的理想值“1”。

为了使像素扩展度达到理想值，部分学者提出了与基矩阵不同的秘密分享算法。Yang[6] 以整幅图像的安全性代替每个像素点的安全性，在分享像素点时随机从基矩阵中选取一列，实现了像素的不扩展。白璟霖[7]利用随机乱数率表示图像的对比度，提出了一种基于随机数的秘密分享算法，实现了像素的不扩展。Hou 等[8]利用人类视觉系统的空间均衡及局部统计等特性，提出了一种多点加密法，该方法可以一次分享 m 个像素，使像素扩展度达到了理想值。Hsu 等[9]从概率的角度研究视觉密码方案，认为原图像的识别可以通过黑白区域的不同灰度来实现，设计了以加密规则矩阵和概率矩阵为核心的秘密分享算法，得到了像素扩展度为1的视觉密码方案。上述方案达到了像素扩展度的理想值，但均以原图像的信息损失为代价，即恢复图像不再包含原图像的所有信息。目前尚无像素扩展度与信息损失之间关系的研究。

针对像素扩展与信息损失的问题，本文给出了无损分享的定义，指出无损分享视觉密码的最优像素扩展度是区分无损分享与有损分享的关键，并设计了矩阵转化算法和整数规划模型，实现了一种像素优化算法，可以在保持恢复计算复杂度的条件下实现完全恢复。

2 无损分享

设 $P=\{1,\cdots,n\}$ 表示 n 个参与者的集合，2^p 表示 P 的所有子集组成的集合。记 G_{Qual} 为授权集合，G_{Forb} 为禁止集合，其中，$G_{\mathrm{Qual}}\subseteq 2^p$，$G_{\mathrm{Forb}}\subseteq 2^p$，且 $G_{\mathrm{Qual}}\cap G_{\mathrm{Forb}}=\varnothing$，则 $(G_{\mathrm{Qual}},G_{\mathrm{Forb}})$ 表示一个视觉密码方案的通用存取结构。下面是以基矩阵为核心的视觉密码方案定义。

定义 1[4] $(G_{\mathrm{Qual}},G_{\mathrm{Forb}})$ 为参与者集合 $P=\{1,\cdots,n\}$ 的通用存取结构，称 $(G_{\mathrm{Qual}},G_{\mathrm{Forb}},m)-\mathrm{VCS}$ 表示一个视觉密码方案，其基矩阵为 $n\times m$ 的布尔矩阵 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$。当分享白(黑)像素时，选择 $\boldsymbol{B}_0(\boldsymbol{B}_1)$ 进行随机的列排序，以确定 n 个共享份中 m 个子像素的颜色。$\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 满足以下2个条件。

1) 对比性条件：对于授权子集 $X=\{i_1,i_2,\cdots,i_p\}\in G_{\mathrm{Qual}}$，$\boldsymbol{B}_0$ 的 $i_1,i_2,\cdots,i_p$ 行“或”运算得到的向量 V 满足 $H(V)\le t_X-a\,m$；$\boldsymbol{B}_1$ 的 $i_1,i_2,\cdots,i_p$ 行“或”运算得到的向量 V 满足 $H(V)\ge t_X$，其中，$H(V)$ 表示 V 的汉明重量。

2) 安全性条件：对于禁止子集 $X=\{i_1,i_2,\cdots,i_f\}\in G_{\mathrm{Forb}}$，设 $\boldsymbol{D}_0(\boldsymbol{D}_1)$ 为 $\boldsymbol{B}_0(\boldsymbol{B}_1)$ 的 $i_1,i_2,\cdots,i_f$ 行构成的子矩阵，则 $\boldsymbol{D}_0=\boldsymbol{D}_1$。

定义 2 设一个视觉密码方案的原图像为 S，经过秘密分享算法后得到共享份集合 T，直接叠加授权子集的共享份，得到恢复图像 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分享的。

定理 1 满足定义1的视觉密码方案是无损分享的。

证明 通过计算恢复图像 S' 中 m 个子像素的汉明重量并分类，可以实现原图像 S 的完全恢复。设原图像 S 的大小为 $a\times b$，$S(i,j)$ 对应恢复图像中 $S'(mi-m+1,j)$ 到 $S'(mi,j)$ 的 m 个像素，设 $W(i,j)=\sum_{k=1}^{m}S'(mi-m+k,j)$ 表示 S' 中 m 个像素的汉明重量，$\overline{W}=\sum\sum_{i=1,j=1}^{i=a,j=b}W(i,j)/(ab)$ 表示像素块的平均汉明重量，W_0 表示原白像素对应像素块的汉明重量，W_1 表示原黑像素对应像素块的汉明重量，由定义1可知 $W_0<\overline{W}<W_1$。因此 $S(x,y)=\left\lfloor W(i,j)/\overline{W}\right\rfloor$，即存在函数 R 满足 $S=R(S')$，定理1证毕。

实际上对于一个已知基矩阵的方案而言，函数 R 更容易设计。例如对(2, 2)方案而言，其基矩阵为 $\boldsymbol{B}_0=\begin{bmatrix}1&0\\1&0\end{bmatrix}$ 和 $\boldsymbol{B}_1=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，叠加2个共享份 T_1 和 T_2 得到 S'。S' 中的'01'汉明重量为1，对应 S 的'0'；S' 中的'11'汉明重量为2，对应 S 的'1'。令 $S(i,j)=\left\lfloor\left(S'(2i-1,j)+S'(2i,j)\right)/2\right\rfloor$（$i$ 和 j 表示 S 的像素坐标），即可完全恢复出原图像。

由定理1的证明和(2, 2)方案的示例可知，无损分享的视觉密码方案在完全恢复原图像时，需要进行 abm 次加法和 ab 次取整，其计算复杂度与传统的

直接叠加相同，均为 $O(1)$。因此无损分享视觉密码既继承了恢复简单的特点，又可以实现完全恢复，待解决的问题是如何减小像素扩展度。

定理 2（判别定理） 设 $(G_{\text{Qual}}, G_{\text{Forb}})$ 为通用存取结构，若 $m<m_0$，则以 m 为像素扩展度的视觉密码方案是有损分享的，其中，m_0 为该存取结构下无损分享方案的最小像素扩展度。

证明 若以 m 为像素扩展度的方案是无损分享的，则 m_0 不是无损分享方案的最小像素扩展度，与已知条件矛盾，定理 2 证毕。

推论 1 对于像素扩展度为 1 的视觉密码方案而言，若恢复操作为或运算，则该方案是有损分享的。

证明 对于恢复操作为或运算的视觉密码而言，(2, 2)方案的 m_0 最小，且 m_0=2。因此对所有视觉密码方案均有 $m_0>1$。根据定理 2，若 m=1，则 $m<m_0$，因此像素扩展度为 1 的视觉密码方案是有损分享的。

由此可见，无损分享视觉密码是一类重要的方案，而且 m_0 是衡量秘密信息能否完全恢复的关键。

3　像素扩展度的优化算法

一般而言，直接计算 m_0 难度较大，而 m_0 表示的是基矩阵的列数，所以可以将复杂的基矩阵设计问题简化为概率矩阵的最大公约数问题。根据像素扩展度 m 与最大公约数 d 的数学关系，建立以 d 最大化为目标、安全性和对比性为约束条件的整数规划模型，然后利用基矩阵与概率矩阵之间的转化算法，得到最优的像素扩展度及相应的基矩阵。本文设计的优化算法流程如图 1 所示。

3.1　加密规则矩阵和概率矩阵

加密规则矩阵和概率矩阵是 Hsu 等[9]为了避开基矩阵而提出的概念。

定义 3　记 $\boldsymbol{E}=[e_{ij}]$ 为加密规则矩阵，$i\in\{1, 2, \text{L}, 2^n\}$，$j\in\{1,2,\text{L},n\}$，$e_{ij}\in\{0,1\}$。$E$ 中各行向量均不相同，行向量 $e_i=(e_{i1}, e_{i2}, \text{L}, e_{in})$ 表示第 i 种加密规则，即原图像的 1 个像素按照 e_i 加密，生成第 j 共享份中对应的像素为 e_{ij}。

定义 4　记 $\boldsymbol{C}=[c_{ij}]$ 为概率矩阵，$i\in\{0,1\}$，$j\in\{1, 2, \text{L}, 2^n\}$，$c_{ij}\in[0,1]$。其中，$c_{0j}$ 表示白像素选择第 j 条加密规则的概率，c_{1j} 表示黑像素选择第 j 条加密规则的概率，且 $\sum_{j=1}^{2^n} c_{0j}=\sum_{j=1}^{2^n} c_{1j}=1$。

对(2, 2)门限方案，$G_{\text{Qual}}=\{\{1,2\}\}$，$G_{\text{Forb}}=\{\{1\},\{2\}\}$，2 个矩阵的使用方法如表 1 所示。

生成共享份时，根据概率矩阵选择加密规则。根据表 1 可知，当原像素为 0（白像素）时，以 c_{01}=0.5 的概率选择 e_1=(e_{11}, e_{12})，以 c_{04}=0.5 的概率选择 e_4=(e_{41}, e_{42})，而 e_2 和 e_3 则不选择；当原像素为 1（黑像素）时，以 c_{02}=0.5 的概率选择 e_2=(e_{21}, e_{22})，以 c_{03}=0.5 的概率选择 e_3=(e_{31}, e_{32})，而 e_1 和 e_4 则不在选择之列。通过上述步骤生成的共享份，其大小与原秘密图像相等，故像素扩展度为 1。在衡量方案安全性和对比性时，则根据一个像素为黑色的概率来判断。

在安全性方面，禁止子集{1}和{2}无法得到原图像的信息。T_1 中原白像素的加密效果为 FC_{01} =

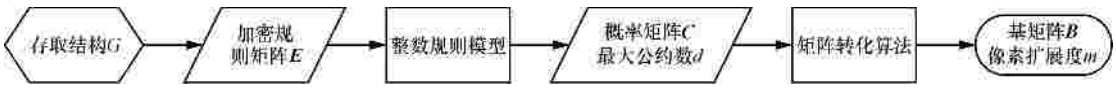


图 1　优化算法流程

表 1　基于加密规则矩阵和概率矩阵的(2, 2)门限视觉密码

原像素	共享份 T_1	共享份 T_2	T_1+T_2	概率	显示黑色的概率		
					T_1	T_2	T_1+T_2
0	e_{11}=0	e_{12}=0	0	c_{01}=0.5	FC_{01}=0.5	FC_{02}=0.5	QC_{01}=0.5
	e_{21}=0	e_{22}=1	1	c_{02}=0.0			
	e_{31}=1	e_{32}=0	1	c_{03}=0.0			
	e_{41}=1	e_{42}=1	1	c_{04}=0.5			
1	e_{11}=0	e_{12}=0	0	c_{11}=0.0	FC_{11}=0.5	FC_{12}=0.5	QC_{11}=1.0
	e_{21}=0	e_{22}=1	1	c_{12}=0.5			
	e_{31}=1	e_{32}=0	1	c_{13}=0.5			
	e_{41}=1	e_{42}=1	1	c_{14}=0.0			

$\sum_{i=1}^{4} e_{i1}c_{0i} = 0.5$，原黑像素的加密效果为 $FC_{11} = \sum_{i=1}^{4} e_{i1}c_{1i} = 0.5$。由于 $FC_{01} = FC_{11}$，因此从 T_1 中无法分辨出原图像的像素颜色。对 T_2 的分析同理。

在对比性方面，需要确定授权子集{1,2}能够恢复出原图像。对 T_1+T_2 而言，原白像素对应的恢复效果为 $QC_{01} = \sum_{i=1}^{4}(e_{i1} + e_{i2})c_{0i} = 0.5$，原黑像素对应的恢复效果为 $QC_{11} = \sum_{i=1}^{4}(e_{i1} + e_{i2})c_{1i} = 1.0$，由于 $QC_{11} > QC_{01}$，因此从 T_1+T_2 中可以分辨出原图像的像素颜色。

3.2 矩阵转化算法

为了便于描述 m 与 d 之间的数学关系，本节首先介绍矩阵转化算法。

定义 5 记能被概率矩阵 $\boldsymbol{C}$ 中所有元素整除的有理数组成集合 D，若 d 是 D 中的最大值，则称 d 为 $\boldsymbol{C}$ 的最大公约数。

注：由于概率矩阵 $\boldsymbol{C}$ 中的元素为[0, 1]的有理数，因此本文是在有理数范围内讨论最大公约数，与通常的自然数范围不同。

矩阵转化算法以加密规则矩阵 $\boldsymbol{E}$ 和概率矩阵 $\boldsymbol{C}$ 为算法输入，以基矩阵 $\boldsymbol{B}_0$ 和 $\boldsymbol{B}_1$ 为算法输出，具体步骤如下。

step1 找到 $\boldsymbol{C}$ 的最大公约数 d。

step2 计算修正后的概率矩阵 $\boldsymbol{C}' = \boldsymbol{C}/d$。

step3 将加密规则 $e_i(1 \le i \le 2^n)$ 的转置重复 c'_{0i} 次，并依次连接组成新的矩阵 $\boldsymbol{B}_0$。

step4 将加密规则 $e_i(1 \le i \le 2^n)$ 的转置重复 c'_{1i} 次，并依次连接组成新的矩阵 $\boldsymbol{B}_1$。

由矩阵转化算法可知，若 $(\boldsymbol{E}_1, \boldsymbol{C}_1) \ne (\boldsymbol{E}_2, \boldsymbol{C}_2)$，则得到的基矩阵是不同的。由于根据基矩阵 $\boldsymbol{B}_0$ 和 B_1 也可以计算出相应的 $\boldsymbol{E}$ 和 $\boldsymbol{C}$，因此可以设计以基矩阵为算法输出，以 $\boldsymbol{E}$ 和 $\boldsymbol{C}$ 为算法输出的逆算法，具体步骤如下。

step1 根据参与者人数 n 确定加密规则矩阵 $\boldsymbol{E}$。

step2 统计 $\boldsymbol{B}_0$ 中加密规则 $e_i(1 \le i \le 2^n)$ 出现的次数 c'_{0i}。

step3 统计 $\boldsymbol{B}_1$ 中加密规则 $e_i(1 \le i \le 2^n)$ 出现的次数 c'_{1i}。

step4 计算概率矩阵 $\boldsymbol{C} = \boldsymbol{C}'/m$。

定理 3 对一个视觉密码方案而言，其基矩阵的像素扩展度 m 与概率矩阵的最大公约数 d 满足 $m = 1/d$。

证明 从矩阵转换算法及其逆算法可知，$\boldsymbol{C}' = \boldsymbol{C}/d$ 且 $\boldsymbol{C} = \boldsymbol{C}'/m$，故定理 3 得证。

下面以(3, 3)门限方案为例，对矩阵转化算法进行说明。加密规则矩阵 $\boldsymbol{E} = \begin{matrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \end{matrix}\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$，概率矩阵 $\boldsymbol{C} = \begin{bmatrix} 1/4 & 0 & 0 & 1/4 & 0 & 1/4 & 1/4 & 0 \\ 0 & 1/4 & 1/4 & 0 & 1/4 & 0 & 0 & 1/4 \end{bmatrix}$，则 $\boldsymbol{C}$ 的最大公约数 $d = 1/4$，修正后的概率矩阵 $\boldsymbol{C}' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$。将 e_i 的转置重复 c'_{0i} 次，并依次连接组成新的矩阵 $\boldsymbol{B}_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$，将 e_i 的转置重复 c'_{1i} 次，并依次连接组成新的矩阵 $\boldsymbol{B}_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$，基矩阵的像素扩展度 $m = 4$。

3.3 整数规划模型

设 $G = (G_{\text{Qual}}, G_{\text{Forb}})$，且 $|G_{\text{Qual}}| = q$，$|G_{\text{Forb}}| = f$。对于以 G 为存取结构的视觉密码方案，其最优像素扩展度是以下整数规划模型的解。

$$\max \quad d$$
$$\text{s.t.} \begin{cases} QC_{1h} - QC_{0h} > 0, (h \in \{1, 2, \text{L}, q\}) \\ FC_{1k} - FC_{0k} = 0, (k \in \{1, 2, \text{L}, f\}) \\ c_{ij} = n_{ij} d \\ \sum_{j=1}^{2^n} c_{ij} = 1 \\ c_{ij} \in [0,1] \\ n_{ij} \in ?, (i \in \{0,1\}, j \in \{1, 2, \text{L}, 2^n\}) \end{cases} \tag{1}$$

1) 规划目标

由于像素扩展度 $m = 1/d$，因此求 m 的最小值等价于 d 的最大值。在视觉密码方案设计过程中，d 只随概率矩阵 $\boldsymbol{C}$ 的变化而取不同的值，因此本模型的规划目标是寻找到一个 d 最大的概率矩阵 $\boldsymbol{C}$。

2) 对比性约束条件

设 $QC_{0h}(QC_{1h})$ 表示授权子集 $Q_h \in G_{\text{Qual}}$ ($h \in \{1,$

$2, \text{L}, q\}$) 的所有共享份叠加后，原白（黑）像素呈现黑像素的概率。定义 $OR(\boldsymbol{E}, X)$ ($X = \{x_1, x_2, \text{L}, x_t\} \in 2^p$) 表示加密规则矩阵 $\boldsymbol{E}$ 中第 x_1, x_2, L, x_t 列在或运算后得到的列向量，则 $(QC_{0h}, QC_{1h})^{\text{T}} = \boldsymbol{C} \times OR(\boldsymbol{E}, Q_h)$。对比性约束条件指授权子集能够恢复秘密图像，故 $QC_{1h} - QC_{0h} > 0$。

3) 安全性约束条件

设 FC_{0k} (FC_{1k}) 表示禁止子集 $F_k \in G_{\text{Forb}}$ ($k \in \{1, 2, \text{L}, f\}$) 的所有共享份叠加后，原白（黑）像素呈现黑像素的概率，则 $(FC_{0k}, FC_{1k})^{\text{T}} = \boldsymbol{C} \times OR(\boldsymbol{E}, F_k)$。安全性条件表示禁止子集无法获取秘密图像的任何信息，故 $FC_{1k} - FC_{0k} = 0$。

4) 其他约束条件

由于 d 是概率矩阵 $\boldsymbol{C}$ 的最大公约数，因此 $c_{ij} = n_{ij} d$ 且 $n_{ij} \in N$ ($i \in \{0,1\}, j \in \{1, 2, \text{L}, 2^n\}$)。另外由根据概率矩阵的定义，可知 $\sum_{j=1}^{2^n} c_{ij} = 1$ 和 $c_{ij} \in [0,1]$。

4　实验结果与分析

本文设计的像素扩展度优化算法适用于通用存取结构，下面从门限结构和通用存取结构 2 个方面进行实验与分析，以说明本文算法的有效性。

1) 门限结构

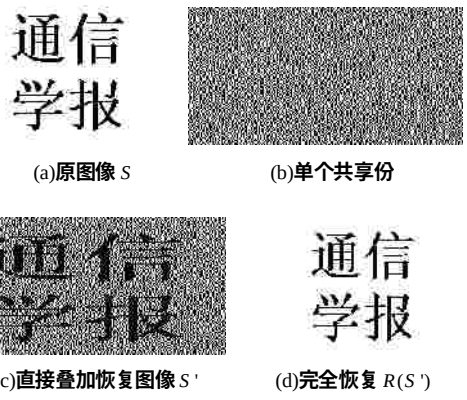
按照像素扩展度的优化算法，计算 (k, n) ($2 \le k \le n \le 10$) 门限结构视觉密码方案的最优像素扩展度，如表 2 所示。从计算结果可以看出：对于(n, n)门限结构，表 2 的结果与文献[1]相同；对于(2, n)门限结构，表 2 的结果与文献[2]相同；对于(k, n) ($2 < k < n \le 10$) 门限结构，表 2 的结果与文献[3]相同。因此本文提出的优化算法对于(k, n)门限结构是有效的。

表 2　(k, n)门限结构方案的像素扩展度

k	n								
	2	3	4	5	6	7	8	9	10
2	2	3	4	4	4	5	5	5	5
3		4	6	8	10	12	14	16	18
4			8	15	24	35	48	63	80
5				16	30	48	70	96	126
6					32	70	128	210	320
7						64	140	256	420
8							128	315	640
9								256	630
10									512

2) 通用存取结构

设 $P = \{1,2,3,4\}$，$G_{\text{Qual}} = \{\{1,2\},\{2,3\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$，$G_{\text{Forb}} = \{\{1,3\}, \{1,4\}, \{2,4\},\{3,4\},\{1\},\{2\},\{3\},\{4\}\}$，则 $(G_{\text{Qual}}, G_{\text{Forb}})$ 是通用存取结构。根据文献[4]的累积矩阵方法，计算得到的基矩阵为 $\boldsymbol{B}_0 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$，$\boldsymbol{B}_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$，$m$=5。根据本文方法，计算的基矩阵为 $\boldsymbol{B}_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$，$\boldsymbol{B}_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$，$m$=4，比文献[4]的方法更优，因此本文方法对于通用存取结构是有效的。本方案对应的原图像、共享份和恢复图像如图 2 所示。



(a)原图像 S　(b)单个共享份　(c)直接叠加恢复图像 S'　(d)完全恢复 $R(S')$

图 2　本文方案的实验效果

从图 2 分析可知，直接叠加共享份得到的 S' 能够完全恢复出原图像 S。需要说明的是，对于不同的授权子集，函数 R 是不同的。比如对于{1, 2}，$R(S') = \left\lfloor \sum_{k=1}^{4} S'(4i - 4 + k, j) / 3 \right\rfloor$；对于{1, 2, 3}，则 $R(S') = \left\lfloor \sum_{k=1}^{4} S'(4i - 4 + k, j) / 4 \right\rfloor$。

最后从通用存取结构、像素扩展度、相对差、信息损失和恢复计算复杂度等 5 个方面将本文方案与前人方案进行对比，具体结果如表 3 所示。其中，$m_0 \le m_1, m_2$，$0 < QC_{1h} - QC_{0h} < 1$。分析表 3 可知：

表 3 方案综合比较

方案	通用存取结构	像素扩展度	相对差	信息损失	恢复计算复杂度
Droste 方案[3]	不适用	m_1	$1/m_1$	无	$O(1)$
Ateniese 方案[4]	适用	m_2	$1/m_2$	无	$O(1)$
Hsu 方案[9]	适用	1	$QC_{1h}-QC_{0h}$	有	$O(1)$
本文方案	适用	m_0	1	无	$O(1)$

本文方案在保证原图像完全恢复的情况下，能够有效减小像素扩展度，且不增加恢复过程的计算复杂度。

5 结束语

在研究秘密图像恢复质量的基础上，本文给出了无损分享视觉密码的定义，保持了恢复简单优点，同时实现了原图像的完全恢复。针对无损分享方案中的像素扩展问题，将像素扩展度 m_0 的求解问题转化为计算概率矩阵的最大公约数 d，进而设计了像素扩展度的优化算法，包括整数规划模型和矩阵转化算法 2 部分。本文取得的计算结果只考虑了或运算的情况，对于其他的算子如 XOR 等，尚有待进一步的研究。

参考文献：

[1] NAOR M, SHAMIR A. Visual cryptography[A]. Cryptology-Eurocrypt' 94[C]. 1994. 1-12.

[2] BLUDNO C, SANTIS A D, STINSON D R, *et al*. Graph decomposition and secret sharing schemes[J]. Journal of Cryptology, 1995, (8): 39-64.

[3] DROSTE S. New results on visual cryptography[A]. Cryptography-CRYPTO' 96[C]. 1996. 401-415.

[4] ATENIESE G, CARLO B, SANTIS A D, *et al*. Visual cryptography for general access structures[J]. Information and Computation, 1996, (12): 86-106.

[5] HAJIABOLHASSAN H, CHERAGHI A. Bounds for visual cryptography schemes[J]. Discrete Applied Mathematics, 2010, (158): 659-665.

[6] YANG C. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, (25):481-494.

[7] 白璟霖. 以随机乱数为基础的影像机密分享[D]. 铭传大学, 2005.
BAI J L. Image Secret Sharing based Upon Random Numbers[D]. Ming Chuan University, 2005.

[8] HOU Y C, TU S F. A visual cryptographic technique for chromatic images using multi-pixel encoding method[J]. Journal of Research and Practice in Information Technology, 2005, 37(2):179-191.

[9] HSU C S, TU S F, HOU Y C. An optimization model for visual cryptography schemes with unexpanded shares[A]. ISMIS[C]. Springer-Verlag Berlin Heidelberg, 2006. 58-67.

作者简介：

郁滨（1964-），男，河南郑州人，信息工程大学教授、博士生导师，主要研究方向为视觉密码和网络安全。

付正欣[通信作者]（1986-），男，山东曹县人，信息工程大学博士生，主要研究方向为视觉密码。E-mail:13503452712@163.com