Journal of System Simulation

Volume 32 | Issue 1 Article 3

1-17-2020

A XOR-based Visual Cryptography Scheme for (2, *n*) Access Structure with Ideal Structure Division

Yuqiao Cheng
Information Engineering University, Zhengzhou 450000, China;

Zhengxin Fu
Information Engineering University, Zhengzhou 450000, China;

Bin Yu
Information Engineering University, Zhengzhou 450000, China;

A XOR-based Visual Cryptography Scheme for (2, *n*) Access Structure with Ideal Structure Division

Abstract

Abstract: We propose a XOR-based visual cryptography scheme for (2, *n*) access structures. According to the definition of ideal access structure, the relationship of shares among the minimal qualified subsets is analyzed. *And based on it, a division algorithm of access structures is presented with the theory of graph. By this approach, we can obtain the least number of ideal access structures.* Additionally the processes of secret sharing and recovering are given. Experimental results show that this scheme can achieve a perfect secret recovery. Compared with existing schemes, the pixel expansion of our paper is the best.

Keywords

XOR-based visual cryptography scheme, perfect recovery, ideal structure division, (2, n) access structure, optimal pixel expansion

Recommended Citation

Cheng Yuqiao, Fu Zhengxin, Yu Bin. A XOR-based Visual Cryptography Scheme for (2, *n*) Access Structure with Ideal Structure Division[J]. Journal of System Simulation, 2020, 32(1): 20-26.

第 32 卷第 1 期
2020 年 1 月

系统仿真学报©
Journal of System Simulation

Vol. 32 No. 1
Jan., 2020

基于理想存取结构划分的(2, *n*)异或视觉密码

程羽乔，付正欣，郁滨
(信息工程大学，郑州 450000)

摘要：针对(2, *n*)异或视觉密码的完全恢复问题，依据理想存取结构定义，在分析最小授权子集之间特殊的共享份关系基础上，*借助图论思想设计了一种存取结构划分算法，并证明了该算法划分得到的理想存取结构数目最少*。设计并实现了秘密分享与恢复算法。实验结果表明，提出的(2, *n*)异或视觉密码方案可以实现秘密图像的完全恢复，且与现有方案相比，像素扩展度达到最优。

关键词：异或视觉密码；完全恢复；理想结构划分；(2, *n*)存取结构；最小像素扩展
中图分类号：TP309.1　　文献标识码：A　　文章编号：1004-731X (2020) 01-0020-07
DOI: 10.16182/j.issn1004731x.joss.17-CACIS010

A XOR-based Visual Cryptography Scheme for (2, *n*) Access Structure with Ideal Structure Division

Cheng Yuqiao, Fu Zhengxin, Yu Bin
(Information Engineering University, Zhengzhou 450000, China)

Abstract: We propose a XOR-based visual cryptography scheme for (2, *n*) access structures. According to the definition of ideal access structure, the relationship of shares among the minimal qualified subsets is analyzed. *And based on it, a division algorithm of access structures is presented with the theory of graph. By this approach, we can obtain the least number of ideal access structures.* Additionally the processes of secret sharing and recovering are given. Experimental results show that this scheme can achieve a perfect secret recovery. Compared with existing schemes, the pixel expansion of our paper is the best.

Keywords: XOR-based visual cryptography scheme; perfect recovery; ideal structure division; (2, *n*) access structure; optimal pixel expansion

引言

视觉密码[1]是一项结合数字图像处理的秘密共享技术，该技术基于人眼视觉特性将秘密图像加密成若干个共享份并分发给对应的参与者，解密时只有授权集合才能恢复出秘密图像。相比于传统秘密共享技术[2]，视觉密码具有解密简单的特点，其秘密恢复过程无需复杂的计算，能够有效解决计算能力受限环境下的秘密共享问题，因而引起了国内外学者们的广泛关注和研究。

在最初方案基础上，视觉密码的研究从存取结构[3-5]、参数优化[6-11]、恢复方式[12-17]、秘密数量[18-19]和图像色彩[20-21]等方面不断完善。Ateniese 等[3]对通用存取结构下的方案设计进行了研究，通过定义授权子集和禁止子集，使秘密恢复时参与者的授权组合方式更为随意。Arumugam 等[4]定义了一种(*k*, *n*)*存取结构，其最小授权子集由一个必要参与者与其余任意 *k*–1 个参与者构成。之后，Dutta 等[5]进一步研究了 *t*-(*k*, *n*)*存取结构，将必要参与者的

收稿日期：2017-07-18　　修回日期：2017-08-28;
基金项目：国家自然科学基金(61602513), 信息工程大学优秀青年基金(2016611303);
作者简介：程羽乔(1994-)，女，江西丰城，硕士生，研究方向为视觉密码、信息安全；付正欣(通讯作者 1986-)，男，山东曹县，博士，讲师，研究方向为视觉密码、信息安全。

数量由一个扩展为 t 个。在任意存取结构下，一个授权子集规模越大，意味着实现一次秘密恢复需要的参与者更多。而在实际应用时，大多情况只要求同时有 2 个合法用户在场即可，例如群身份认证等。因此，部分学者针对(2, n)这一特定存取结构进行相关研究。在提高相对差方面，Blundo 等[6]给出并证明了(2, n)方案的最大相对差。Hofmeister 等[7]通过建立线性规划模型，研究了基矩阵的最小规模，进而得到了与文献[6]相同的结果。为减小像素扩展，Shyu 等[9]提出了求解最小像素扩展的整数线性规划模型，该模型需要穷举搜索求解，随着 n 增大，计算复杂度以指数形式急剧增大。

上述方案虽在像素扩展度和相对差方面有所改进，但都是基于或运算设计的，其代数结构为加法半群，无法实现秘密图像的完全恢复。Biham 等[12]利用偏振光设计了一种群结构的视觉密码方案，为秘密恢复算法和共享份载体提供了更多的选择。Tuyls 等[13]明确提出了异或视觉密码(XOR-based visual cryptography scheme, XVCS)的概念，并证明了(2, n)-XVCS 与二值纠错码两者之间的等价性。Liu 等[15]对(2, n)-XVCS 的参数最优问题进行了研究，方案构造了(2, n)-XVCS 分享矩阵，得到最小像素扩展度$\lceil \log_2 n \rceil$，但恢复图像存在失真。付等[16]给出了理想存取结构的定义，通过将任意存取结构划分为若干个理想存取结构，实现了秘密图像的完全恢复。此时，划分的理想存取结构数目即为方案的像素扩展度。文献[17]在该算法下划分得到(2, n)方案的像素扩展度为$\lceil n/2 \rceil$，与文献[15]相比，该方案像素扩展度较大。

因此，本文依据理想存取结构的定义，深入研究(2, n)异或视觉密码的完全恢复。通过分析最小授权子集之间共享份的关系，基于图论提出一种新的存取结构划分算法。在此基础上，设计(2, n)异或视觉密码方案，并对方案有效性进行理论证明和实验验证。实验分析表明，该方案在秘密图像完全恢复的前提下，能够保证最小像素扩展。

1 存取结构划分

本节针对(2, n)存取结构的最小授权集合展开研究，通过分析子集之间共享份的关系，设计一种(2, n)存取结构划分算法。

1.1 共享份关系

定义 1[3] 假设参与者集合 $P = \{1, 2, \cdots, n\}$，幂集为 2^P。令Γ_Q表示所有授权子集集合，Γ_F表示所有禁止子集集合。若$\Gamma_Q \subseteq 2^P$，$\Gamma_F \subseteq 2^P$且$\Gamma_Q \cap \Gamma_F = \varnothing$，则称$(\Gamma_Q, \Gamma_F)$为 P 的一个存取结构。记最小授权集合$\Gamma_0 = \{Q \in \Gamma_Q: \forall B \subset Q \Rightarrow B \notin \Gamma_Q\}$，其中各个元素称为最小授权子集。

定义 2[16] 对于存取结构$\Gamma = (\Gamma_Q, \Gamma_F)$，记最小授权集合$\Gamma_0 = \{Q_1, Q_2, \cdots, Q_t\}$。设秘密图像为 S，$\mathrm{R}(Q)$表示对 Q 中参与者的共享份进行异或运算，若$\forall Q \in \Gamma_0$，均有 $\mathrm{R}(Q) = S$ 成立，则称Γ是一个理想存取结构。

根据定义 2，在(2, n)-XVCS 中，若Γ_0是一个理想存取结构的最小授权集合（以下简称理想授权集合），则对于$\forall Q_a, Q_b \in \Gamma_0$，有 $\mathrm{R}(Q_a) = \mathrm{R}(Q_b) = S$。令 T_i 表示参与者 i 的共享份，设 $Q_a = \{i_1, i_2\}$, $Q_b = \{i_3, i_4\}(Q_a \neq Q_b)$，若 $Q_a \cap Q_b \neq \varnothing$，不妨设 $i_1 = i_3$，则有 $T_{i_1} = T_{i_3}$，$T_{i_2} = S \oplus T_{i_1} = S \oplus T_{i_3} = T_{i_4}$；若 $Q_a \cap Q_b = \varnothing$，有$\{T_{i_1}, T_{i_2}\} = \{T_{i_3}, T_{i_4}\}$或$\{T_{i_1}, T_{i_2}\} \cap \{T_{i_3}, T_{i_4}\} = \varnothing$。

定义 3 在(2, n)-XVCS 中，设Γ_0是一个理想授权集合，对于其中任意 2 个元素 $Q_a = \{i_1, i_2\}$，$Q_b = \{i_3, i_4\}(Q_a \neq Q_b)$，定义 2 类关系如下：

(1) 若$\{T_{i_1}, T_{i_2}\} = \{T_{i_3}, T_{i_4}\}$，则称 Q_a 和 Q_b 的共享份是相同关系，记作 $T_{Q_a} = T_{Q_b}$。

(2) 若$\{T_{i_1}, T_{i_2}\} \cap \{T_{i_3}, T_{i_4}\} = \varnothing$，则称 Q_a 和 Q_b 的共享份是等价关系，记作 $T_{Q_a} \sim T_{Q_b}$。

显然，Γ_0 中任意 2 个最小授权子集的共享份只可能存在相同关系或等价关系。

实际上，(2, n)-XVCS 中的任意一个存取结构都是一个基于图的存取结构[3]。其中，顶点表示各个参与者，边代表一个最小授权子集。设图 $G = (V,$

https://dc-china-simulation.researchcommons.org/journal/vol32/iss1/3
DOI: 10.16182/j.issn1004731x.joss.17-CACIS010

第 32 卷第 1 期 系统仿真学报 Vol. 32 No. 1
2020 年 1 月 Journal of System Simulation Jan., 2020

$E(G)$)是一个理想授权集合，V 是图 G 中顶点的集合，$E(G)$是图 G 中边的集合，$E(V_i, V_j)$表示两个顶点分别属于 V_i 和 V_j 的边的集合。根据上述分析，G 可以被划分为若干个完全二分图，如图 1 所示。一个虚线框对应一个完全二分图，图 G 的边集合和顶点集合分别满足：

$$E(G) = E(V_{11}, V_{12}) \cup E(V_{21}, V_{22}) \cup \cdots \cup E(V_{s1}, V_{s2})$$

$$V = V_{11} \cup V_{12} \cup V_{21} \cup V_{22} \cup \cdots \cup V_{s1} \cup V_{s2}$$

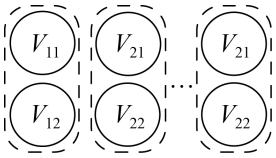

图 1 基于图的理想授权集合表示

Fig. 1 Graph-based denotation of an ideal access structure

对于 $1 \leqslant i \neq j \leqslant s$，$\forall Q_1, Q_2 \in E(V_{i1}, V_{i2})$，$\forall Q_3 \in E(V_{j1}, V_{j2})$，有 $T_{Q_1} = T_{Q_2} \sim T_{Q_3}$。

1.2 划分算法

本小节以分层递归划分子图的方式，将(2, n)结构划分为若干个理想存取结构，具体步骤为：设 $V(s)$表示 V 中任意 s 个顶点形成的一个子集，V_i^j 表示第 i 层第 j 个顶点子集。

输入：全体参与者集合 $V_0^1 = \{1, 2, \cdots, n\}$。

输出：理想授权集合$\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$。

step 1：令 $i = 0$，$s = n$。

step 2：若 $s > 1$，令 $i = i + 1$，$\Gamma_i = \varnothing$，$s = \lfloor s/2 \rfloor$，$j = 0$，$\Gamma_0^i = \varnothing$，转 step 3；否则，转 step 5。

step 3：令 $j = j + 2$，若 $j \leqslant 2^i$，转 step 4；否则，转 step 5。

step 4：令 $m = \lceil |V_{i-1}^{j/2}|/2 \rceil$，$V_i^{j-1} = V_{i-1}^{j/2}(m)$，$V_i^j = V_{i-1}^{j/2} - V_i^{j-1}$，$\Gamma_0^i = \Gamma_0^i + E(V_i^{j-1}, V_i^j)$，转 step 3。

step 5：若 $n > 2^i$，令 $d = i + 1$，$\Gamma_0^d = \{E(V_{d-1}^j, V_{d-1}^j) \mid |V_{d-1}^j| = 2, 1 \leqslant j \leqslant 2^{d-1}\}$；否则，$d = i$。转 step 6。

step 6：算法结束，输出$\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$。

图 2 是划分算法示意图。由图可知，该算法划分的理想存取结构数目为 $d = \lceil \log_2 n \rceil$。

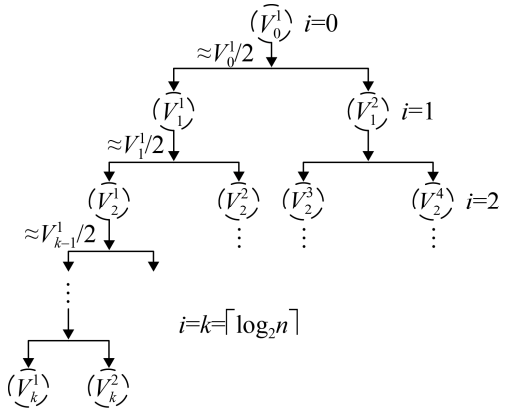

图 2 (2, n)结构划分示意图

Fig. 2 Division of the (2, n) access structure

2 方案设计

在(2, n)存取结构划分基础上，本节将给出一种(2, n)-XVCS 的构造流程，并对方案的有效性进行证明。

2.1 秘密分享与恢复

2.1.1 秘密分享流程

设 T_i^j 表示共享份 T_i 的第 j 部分($1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant d$)，rand($S$)表示生成一幅与 S 大小相同的随机噪声图像，具体分享步骤如下。

输入：(2,n)结构划分的理想授权集合$\Gamma_0^1, \Gamma_0^2, \cdots, \Gamma_0^d$，秘密图像 S。

输出：n 个共享份 $T_1, T_2, \cdots, T_n$。

step 1：令 $j = 1$，$P' = \varnothing$。

step 2：任取 $Q = \{a, b\} \in \Gamma_0^j$，令 $T_a^j = \text{rand}(S)$，$T_b^j = S \oplus T_a^j$，$a, b \in P'$，$\Gamma_0^j = \Gamma_0^j - Q$，转 step 3。

step 3：遍历Γ_0^j，寻找所有包含元素 a(或 b)的 $Q' = \{a, c\}$(或 $Q' = \{b, d\}$)，令 $T_c^j = T_b^j$，$c \in P'$(或 $T_d^j = T_a^j$，$d \in P'$)。从Γ_0^j中删除所有包含 P'中元素的最小授权子集，转 step 4。

step 4：若$\Gamma_0^j \neq \varnothing$，转 step 2；否则，转 step 5。

step 5：若 $P' \neq \{1, 2, \cdots, n\}$，则利用 rand($S$)对剩下未赋值共享份的第 j 部分进行赋值。令 $j = j + 1$，若 $j \leqslant d$，转 step 2；否则，转 step 6。

step 6：连接共享份的各个部分，生成最终共享份 $T_k = T_k^1 \circ T_k^2 \circ \cdots \circ T_k^d$($1 \leqslant k \leqslant n$)，算法结束。其

中“∘”表示图像的拼接，拼接方式不受限制，既可以是横向拼接，也可以是纵向拼接，或者按矩形拼接，如图 3 所示。

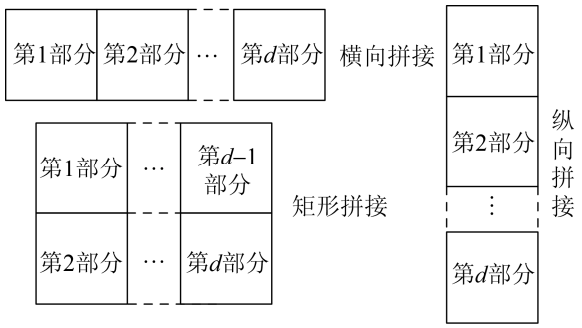

图 3 子共享份拼接方式示意图
Fig. 3 Combination modes of sub-shares

2.1.2 秘密恢复流程

对最小授权子集 $Q = \{i, j\}$，将其中的参与者共享份进行异或运算，即可得到秘密恢复图像 S'，即：

$$S' = T_i \oplus T_j$$

2.2 有效性分析

定理 1 对于(2, n)-XVCS 中的任意一个理想授权集合Γ_0，必然存在一个完全二分图 $G=(V, E(G))$，V 由Γ_0中包含的全体参与者组成，且 $E(G)$ 包含了Γ_0中所有最小授权子集。

证明：由 2.1 节分析可知，任意一个理想授权集合Γ_0都能由图 1 表示。

因而存在一个完全二分图 G，顶点集合 $V = V_1 \cup V_2$，其中 $V_1 = V_{11} \cup V_{21} \cup \cdots \cup V_{s1}$，$V_2 = V_{12} \cup V_{22} \cup \cdots \cup V_{s2}$，边集合 $E(G) = E(V_1, V_2)$。

显然，$E(V_{11}, V_{12}) \cup E(V_{21}, V_{22}) \cup \cdots \cup E(V_{s1}, V_{s2}) \subseteq E(G)$，即 $E(G)$包含Γ_0中所有元素。

证毕。

推论 1 设(2, n)-XVCS 的最小授权集合构成一个完全图 G，Γ_0 是包含子集最多的理想授权集合且构成图 G'，则 G'是 G 的一个完全二分图。

证明：设Γ_0 是包含子集最多的理想授权集合，且 G'不是 G 的一个完全二分图。根据定理 1，必然存在一个完全二分图 G''，对应于另一个理想存取结构Γ_0'，有$\Gamma_0 \subseteq \Gamma_0'$，与$\Gamma_0$包含子集最多相矛盾。

因此，G'一定是 G 的一个完全二分图。

证毕。

任意一个完全图 G 可以由 2 个完全子图 G_1，G_2 和一个完全二分图 G'组成。因此，(2, n)-XVCS 的最小授权集合可以划分为Γ_0 以及 2 个互不相交的(2, s)-XVCS 最小授权集合和(2, n–s)-XVCS 最小授权集合。Γ_0 是(2, n)-XVCS 中包含子集最多的理想授权集合。

推论 2 设(2, s)-XVCS 和(2, $n-s$)-XVCS 的最小授权集合分别构成完全子图 G_1 和 G_2。若 $G = G_1+G_2$，且Γ_0，Γ_0^1和Γ_0^2分别是(2, n)-XVCS，(2, s)-XVCS 和(2, n–s)-XVCS 中包含子集最多的理想授权集合，则$\Gamma_0 = \Gamma_0^1 \cup \Gamma_0^2$。

证明：对于$\forall Q_1 \in \Gamma_0^1$，$\forall Q_2 \in \Gamma_0^2$，令 $T_{Q_1} \sim T_{Q_2}$，则 Q_1 和 Q_2 属于同一个理想存取结构。因此，$\Gamma_0 = \Gamma_0^1 \cup \Gamma_0^2$是一个理想授权集合。

假设存在另一个理想授权集合Γ_0'，$|\Gamma_0'| > |\Gamma_0|$且$|\Gamma_0'| = m_1 + m_2$（m_1, m_2 分别表示Γ_0'包含 G_1, G_2 中的子集的数目）。根据推论 1，有 $m_1 \leqslant |\Gamma_0^1|$，$m_2 \leqslant |\Gamma_0^2|$，故$|\Gamma_0'| \leqslant |\Gamma_0^1| + |\Gamma_0^2| \leqslant |\Gamma_0|$，与假设相矛盾。因此，$\Gamma_0$ 是包含子集最多的理想授权集合。

证毕。

定理 2 (2, n)存取结构划分得到的理想存取结构数目最少为$\lceil \log_2 n \rceil$。

证明：根据推论 1 和 2，只有将每个完全图都划分为两个完全子图和一个完全二分图时，划分数目最少。设(2, n)-XVCS 的最小授权集合对应完全图 G_n，划分得到两个完全子图 G_s 和 G_{n-s}。记 G_n，G_s 和 G_{n-s} 的划分数目分别为 d_n，d_s 和 d_{n-s}，有 $d_n = \max\{d_s, d_{n-s}\} + 1$。由于 d_n 是一个单调递增函数，则对于 $1 \leqslant s \leqslant k \leqslant n$，有：

(1) 当 $s \geqslant \lceil k/2 \rceil$时，有 $d_s \geqslant d_{k-s}$，$\max\{d_s, d_{k-s}\} = d_s \geqslant d_{\lceil k/2 \rceil}$。

(2) 当 $s \leqslant \lceil k/2 \rceil$时，有 $d_s \leqslant d_{k-s}$，$\max\{d_s, d_{k-s}\} = d_{k-s} \geqslant d_{\lceil k/2 \rceil}$。

第 32 卷第 1 期 系统仿真学报 Vol. 32 No. 1
2020 年 1 月 Journal of System Simulation Jan., 2020

显然，$\max\{d_s, d_{k-s}\} \geqslant d_{\lceil k/2 \rceil}$。故当 $s = \lceil k/2 \rceil$，即完全图 G_k 划分为 2 个完全子图 $G_{\lceil k/2 \rceil}$和 $G_{\lfloor k/2 \rfloor}$时，d_k 取最小值。

假设存在 p(p 是大于 1 的正整数)满足条件 $2^p + 1 \leqslant n \leqslant 2^{p+1}$。已知 $d_2 = 1$，根据递归关系，有：

$d_n \geqslant d_{\lceil n/2 \rceil} + 1 \geqslant d_{2^p} + 1 \geqslant \cdots \geqslant d_2 + p = p+1$

故 $\min d_n = p + 1$，又根据 p 的取值范围，可得 $d_n = \lceil \log_2 n \rceil$。

证毕。

定理 3 任意单个共享份无法推断出秘密图像的相关信息。

证明：设 S 和 S'分别表示秘密图像和恢复图像，$P(S|S')$表示条件概率。根据 3.1.1 节，单个共享份赋值满足 $T = \mathrm{rand}(S)$或者 $T = S \oplus \mathrm{rand}(S)$。显然，$P(S = 0|T = 0) = P(S = 1|T = 0)$且 $P(S = 0|T = 1) = P(S = 1|T = 1)$。

因此，任意单个共享份无法推断出秘密图像的相关信息。

证毕。

定理 4 任意一个最小授权子集的恢复图像中，有且仅有某一部分区域能完全恢复出秘密图像。

证明：根据 3.1.1 节，若 $Q = \{i, j\} \in \Gamma_k$，有 $S' = T_i \oplus T_j = \mathrm{rand}(S) \oplus \mathrm{rand}(S) \oplus S = S$ 成立。

若 $Q \notin \Gamma_k$，有以下 3 种情况：

(1) $S' = T_i \oplus T_j = 0$；

(2) $S' = T_i \oplus T_j = \mathrm{rand}(S)^1 \oplus \mathrm{rand}(S)^2$ ($\mathrm{rand}(S)^1$，$\mathrm{rand}(S)^2$ 表示由 $\mathrm{rand}(S)$产生的 2 幅不同的随机噪声图像)；

(3) $S' = T_i \oplus T_j = \mathrm{rand}(S)^1 \oplus \mathrm{rand}(S)^2 \oplus S$。

不难发现，从 Q 恢复图像的第 k 部分区域不能推断出任何与秘密图像有关的信息。又根据 2.2 节划分算法，一个最小授权子集只属于一个理想授权集合。因此，任意一个最小授权子集的恢复图像中有且仅有某一部分能完全恢复出秘密图像。

证毕。

3 实验与分析

为验证本文设计方案的有效性，本节以 $n = 9$ 为例对方案进行实验验证，并分析给出本方案与其他分享方案的参数综合对比。

首先，根据 2.2 节划分算法，得到(2, 9)存取结构划分结果如图 2 所示。。

由图 4 可得，Γ_0^1={{1,6},{2,6},{3,6},{4,6}, {5,6}, {1,7},{2,7},{3,7},{4,7},{5,7},{1,8},{2,8},{3,8}, {4,8}, {5,8},{1,9},{2,9},{3,9},{4,9},{5,9}}；Γ_0^2={{1,4}, {2,4}, {3,4},{1,5},{2,5},{3,5},{6,8},{6,9},{7,8},{7,9}}；Γ_0^3= {{1,3},{2,3},{4,5},{6,7},{8,9}}；Γ_0^4 = {{1,2}}。

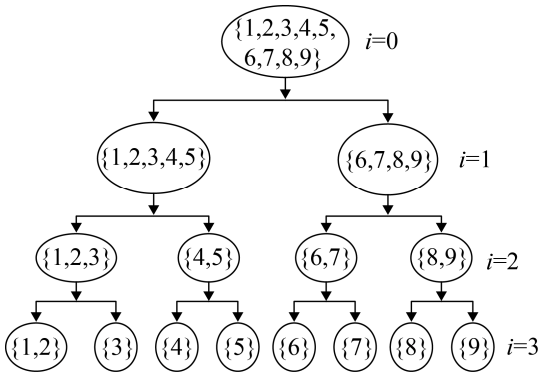

图 4 (2, 9)存取结构顶点集合递归划分
Fig. 4 Recursive division of (2,9) access structure

利用 3.1 节秘密分享与恢复流程对秘密图像进行分享，并按照 2×2 的矩形形式排列拼接共享份各个部分，实验结果见图 5。设 K_i^j 表示对共享份第 j 部分赋值时由 $\mathrm{rand}(S)$生成的第 i 个随机噪声图像。

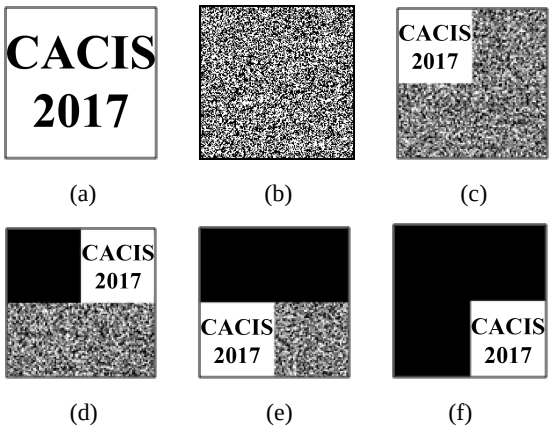

图 5 (2, 9)方案实验结果
Fig. 5 Experimental result of (2,9)-XVCS

考虑共享份第 1 部分，可得 $T_1^1= T_2^1= T_3^1= T_4^1= T_5^1= K_1^1$，$T_6^1= T_7^1= T_8^1= T_9^1= S \oplus K_1^1$；同理，对于第 2 部分，有 $T_1^2= T_2^2= T_3^2= K_1^2$，$T_4^2= T_5^2= S \oplus K_1^2$，$T_6^2= T_7^2= K_2^2$，$T_8^2= T_9^2= S \oplus K_2^2$；对于第 3 部分，有 $T_1^3= T_2^3= K_1^3$，$T_3^3= S \oplus K_1^3$，$T_4^3= K_2^3$，$T_5^3= S \oplus K_2^3$，$T_6^3= K_3^3$，$T_7^3= S \oplus K_3^3$，$T_8^3= K_4^3$，$T_9^3= S \oplus K_4^3$；对于第 4 部分，有 $T_1^4= K_1^4$，$T_2^4= S \oplus K_1^4$，$T_3^4= K_2^4$，$T_4^4= K_3^4$，$T_5^4= K_4^4$，$T_6^4= K_5^4$，$T_7^4= K_6^4$，$T_8^4= K_7^4$，$T_9^4= K_8^4$。

图 5(a)是秘密图像，图 5(b)是单个共享份图像。值得说明的是，所有共享份都呈现的是类似图 5(b)所示的随机噪声图像，为节省空间只列出了其中的一个共享份。此外，所有图片边框均为了方便观察，并不参与秘密分享和恢复过程。

图 5(c)是理想授权集合Γ_0^1中任意一个最小授权子集的共享份叠加结果。如图 5(c)所示，恢复图像的第 1 部分区域能够完全恢复出秘密图像。由于Γ_0^1中的最小授权子集都不属于Γ_0^2，Γ_0^3，Γ_0^4，因此，恢复图像的第 2~4 部分区域都是随机噪声图像，无法从中推断出秘密图像的相关信息。图 5(d)是Γ_0^2中任意最小授权子集的共享份叠加结果。显然，恢复图像的第 2 部分区域能够完全恢复出秘密图像。对于Γ_0^2中任意一个最小授权子集，其中两个参与者共享份的第 1 部分区域赋值相同，而第 3~4 部分区域赋值不同。因此，恢复结果图像中第 1 部分区域呈现全黑，第 3~4 部分区域无任何有意义信息。同理，图 5(e)和(f)分别是Γ_0^3和Γ_0^4中最小授权子集的共享份的叠加结果。

恢复计算复杂度低是视觉密码相比于其他秘密共享技术的一个突出优势。对视觉密码而言，像素扩展度和秘密图像恢复效果是两个能够用来评判方案优劣的重要参数。表 1 是本方案与其他分享方案的一个综合对比结果。

通过分析，可得如下结论：

(1) 在秘密恢复效果方面，只有本文和文献[2,14,17]能实现完全恢复。

(2) 在像素扩展方面，本文与文献[13-15]的像素扩展度相同，文献[3,6-8,17]较大，文献[2]较小。文献[9]建立的线性规划模型包含 $O(2^n)$个变量和约束条件，随着 n 增大，该模型求解所需计算复杂度过大，因此，文献[9]未给出具体数学表达式。

(3) 在恢复计算复杂度方面，文献[2]需要借助于计算机实现恢复，计算复杂度较大。文献[14]需要对 XOR 运算得到的恢复图像作进一步阈值比较，才能实现完全恢复。文献[3,6-9]通过 OR 运算直接恢复，本文和文献[13,15,17]通过 XOR 运算直接恢复。

表 1 本文与其他分享方案的比较

Tab. 1 Comparisons between this paper and related works

文献	完全恢复	像素扩展度	恢复计算复杂度
[2]	是	1	$O\left(\binom{n}{k-1}\right)$
[3]	否	$\lceil n/2 \rceil$	$O(1)$
[6]	否	$\binom{n}{\lfloor n/2 \rfloor}$	$O(1)$
[7]	否	$\binom{n}{\lfloor n/2 \rfloor}$	$O(1)$
[8]	否	n	$O(1)$
[9]	否	—	$O(1)$
[13]	否	$\lceil \log_2 n \rceil$	$O(1)$
[14]	是	$\lceil \log_2 n \rceil$	$O(k)$
[15]	否	$\lceil \log_2 n \rceil$	$O(1)$
[17]	是	$\lceil n/2 \rceil$	$O(1)$
本文	是	$\lceil \log_2 n \rceil$	$O(1)$

4 结论

本文基于理想存取结构划分设计了一种可完全恢复的(2, n)异或视觉密码方案，定义了(2, n)门限结构最小授权子集共享份的两类关系，提出了一种基于图的存取结构划分算法，使方案像素扩展度达到最小值$\lceil \log 2n \rceil$。本文为进一步研究完全恢复的(k, n)异或视觉密码方案奠定了基础。

参考文献：

[1] Naor M, Shamir A. Visual cryptography[J]. Lecture Notes in Computer Science (S0302-9743), 1995, 950(9): 1-12.

[2] Chao K Y, Lin J C. Secret Image Sharing: A Boolean Operations Based Approach Combining Benefits of

https://dc-china-simulation.researchcommons.org/journal/vol32/iss1/3
DOI: 10.16182/j.issn1004731x.joss.17-CACIS010

Polynomial Based and Fast Approaches[J]. International Journal of Pattern Recognition and Artificial Intelligence (S0218-0014), 2009, 23(2): 263-285.

[3] Ateniese G, Blundo C, Santis A D, et al. Visual Cryptography for General Access Structures[J]. Information and Computation (S0890-5401), 1996, 129(2): 86-106.

[4] Arumugam S, Lakshmanan R, Nagar AK. On (k,n)*-Visual Cryptography Scheme[J]. Designs, Codes and Cryptography (S1573-7586), 2014, 71(1): 153-162.

[5] Dutta S, Rohit R S, Adhikari A. Constructions and Analysis of Some Efficient, \(t\), -, \((k,n)^*\), -Visual Cryptographic Schemes Using Linear Algebraic Techniques[J]. Designs, Codes and Cryptography (S1573-7586), 2016, 80(1): 165-196.

[6] Blundo C, Santis A D, Stinson D R. On the Contrast in Visual Cryptography Schemes[J]. Journal of Cryptology (S0933-2790), 1999, 12(4): 261-289.

[7] Hofmeister T, Krause M, Simon H U. Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography [J]. Theoretical Computer Science (S0304-3975), 2000, 240(2): 471-485.

[8] Lakshmanan R, Arumugam S. Construction of A (k, n)-Visual Cryptography Scheme[J]. Designs Codes & Cryptography (S1573-7586), 2017, 82(3): 629-645.

[9] Shyu S J, Chiang C M. Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes[J]. IEEE Transactions on Information Forensics & Security (S1556-6013), 2011, 6(3): 960-969.

[10] Shyu S J, Chen M C. Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures[J]. IEEE Transactions on Circuits & Systems for Video Technology (S1558-2205), 2015, 25(9): 1557-1561.

[11] 侯永昌, 官振宇, 蔡志丰, 等. 没有形变的(3,n)-视觉秘密分享方案[J]. 计算机学报, 2016, 39(3): 441-453.
Hou Yongchang, Guan Zhenyu, Cai Zhifeng, et al. (3,n)-Visual Secret Sharing Scheme with Unexpanded Shares[J]. Chinese Journal of Computers, 2016, 39(3): 441-453.

[12] Biham E, Itzkovitz A. Visual Cryptography with Polarization [EB/OL]. [2017-04-10]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.9.6412.

[13] Tuyls P, Hollmann H D L, Lint J H V, et al. XOR-based Visual Cryptography Schemes[J]. Designs, Codes and Cryptography (S1573-7586), 2005, 37(1): 169-186.

[14] 沈刚, 付正欣, 郁滨. (*k*, *n*)异或视觉密码的一般性研究[J]. 电子与信息学报, 2013, 35(10): 2294-2300.
Shen Gang, Fu Zhengxin, Yu Bin. On the Generality of (*k*, *n*) XOR-based Visual Cryptography Scheme[J]. Journal of Electronics & Information Technology, 2013, 35(10): 2294-2300.

[15] Liu F, Wu C K. Optimal XOR Based (2,n)-Visual Cryptography Schemes[M]. Digital-Forensics and Watermarking. Springer International Publishing, 2014: 333-349.

[16] 付正欣, 沈刚, 孔志印, 等. 异或视觉密码的理想存取结构研究[J]. 电子与信息学报, 2014, 36(7): 1642-1647.
Fu Zhengxin, Shen Gang, Kong Zhiyin, et al. Investigation on Ideal Access Structure of XOR-based Visual Cryptography[J]. Journal of Electronics & Information Technology, 2014, 36(7): 1642-1647.

[17] 付正欣. 视觉密码的一般模型及关键问题研究[D]. 郑州: 中国人民解放军信息工程大学, 2014.
Fu Zhengxin. Research on General Model of Visual Cryptography and Its Key Problems[D]. Zhengzhou: Information Engineering University, 2014.

[18] Li Shundong, Li Jiliang, Wang Daoshun. Region Incrementing Visual Cryptography Scheme with Same Contrast[J]. Chinese Journal of Electronics (S2075-5597), 2016, 25(4): 621-624.

[19] 付正欣, 沈刚, 李斌, 等. 一种可完全恢复的门限多秘密视觉密码方案[J]. 软件学报, 2015, 26(7): 1757-1771.
Fu Zhengxin, Shen Gang, Li Bin, et al. Threshold Multi-Secret Visual Cryptography Scheme with Perfect Recovery[J]. Journal of Software, 2015, 26(7): 1757-1771.

[20] Yan X, Wang S, Niu X, et al. Halftone Visual Cryptography with Minimum Auxiliary Black Pixels and Uniform Image Quality[J]. Digital Signal Processing (S1051-2004), 2015, 38(C): 53-65.

[21] Sridhar S, Sathishkumar R, Sudha G F. Adaptive Halftoned Visual Cryptography with Improved Quality and Security[J]. Multimedia Tools & Applications (S1573-7721), 2017, 76(1): 815-834.