一种二值图像的阈值可视密码方案

徐永平,胡予濮,王 明,刘书盼
XU Yong-ping,HU Yu-pu,WANG Ming,LIU Shu-pan

西安电子科技大学 计算机网络与信息安全教育部重点实验室,西安 710071
Key Laboratory of Computer Network and Information Security,Xidian University,Xi'an 710071,China
E-mail:xyplh@sohu.com

XU Yong-ping,HU Yu-pu,WANG Ming,et al.Threshold scheme for binary image visual cryptography.Computer Engineering and Applications,2009,45(31):77-80.

Abstract: Most recent papers about binary visual cryptography schemes are dedicated to study a higher contrast of recovered images or a smaller share size in visual secret sharing schemes.This paper proposes a new binary (k,n)-VCS based on the secret sharing schemes.A strong access structure is given which uses the feature of the solution of a system of linear equations over the binary field and hierarchical method for constructing basis binary matrices $\boldsymbol{S}^0,\boldsymbol{S}^1$,and the (k,n)-VCS is obtained and in almost all the case a much smaller pixel expansion is gained from this method.

Key words: visual cryptography;visual secret sharing scheme;general access structure;threshold scheme

摘 要: 目前提出的许多关于二值可视密码方案的论文都致力于研究在可视秘密共享方案里如何使像素扩展比较小或恢复图像的对比度比较高的问题。基于 Shamir 的秘密共享方案的思想,提出一种新的二值图像(k,n)-VCS可视密码方案。该方案利用二元域上线性方程组解的特征及多层(k,k)-VCS构造基础矩阵 $\boldsymbol{S}^0,\boldsymbol{S}^1$,给出一个强的访问结构,从而获得$(k,n)$-VCS 可视密码方案更小的像素扩展。

关键词:可视密码;可视秘密共享方案;一般访问结构;阈值方案
DOI:10.3778/j.issn.1002-8331.2009.31.024 **文章编号**:1002-8331(2009)31-0077-04 **文献标识码**:A **中图分类号**:TP391

1 引言

目前提出的大多数二值可视密码方案都是致力于解决子图像素扩展比较大和恢复图像的对比度低的问题。在阈值可视密码方案中有三个重要的参数:对比度 $\alpha(m)$、像素扩展 m 和阈值 t。假设秘密图像由黑白像素组成,每个像素被分割共享于 n 个参与者,且每个像素扩展为 m 个子像素,造成子秘密图像要比原始秘密图像大。同时也造成恢复图像失真问题,为了能够清晰地恢复秘密图像,要求黑色像素的灰度要比白色像素的灰度深,通常这两个像素的灰度比称为对比度,当然对比度越强,恢复的图像就越清晰。阈值 t 的大小决定对比度的强弱。

一个(k,n)阈值 VCS 秘密共享方案对于任意的访问结构$(\Gamma_{Qual},\Gamma_{Forb})$,具有 $\Gamma_0=\{B\subseteq P:|B|=k\}$,且 $\Gamma_{Forb}=\{B\subseteq P:|B|\leqslant k-1\}$,也就是说对于任意的$(k,n)$阈值 VCS 秘密共享方案,通过重叠任意 k 个或 k 个以上的子秘密图像可以恢复秘密图像,而任意少于 k 个子秘密图像无论用什么方法也不可恢复秘密图像。

在文献[2]中提出了利用线性方程组在二元域上所有解的集合形成一个在基础域上的向量空间来构造基础矩阵 $\boldsymbol{S}^0,\boldsymbol{S}^1$ 所构成的在一般访问结构上的黑白可视密码方案,在二元域上齐次线性方程组的解构成向量空间构造基础矩阵 $\boldsymbol{S}^0$,而非齐次线性方程组的解构成的向量空间构造基础矩阵 $\boldsymbol{S}^1$。该构造方法有极大的利用价值,在提出的方案中,构造基础矩阵时利用了线性方程组解的特征,同时利用 Shamir 提出的方案的(k,k)-VCS 基本结构,联合较小的方案构造的多层(k,k)-VCS 方案,极大地减小了子图像素扩展。

2 多层(k,k)-VCS 方案

结论 1[1] 对于一般的(k,k)-VCS 方案,$m=2^{k-1}$,$\alpha=1/2^{k-1}$。

多层(k,k)-VCS 方案的基本原则是,利用 Naor-Shamir 的最优(k,k)-VCS 方案的基本结构,联合较小的方案构造而成。基础(k_1,k_1)-VCS 方案,有 k_1 个子图,重叠即可获得原图像。如果利用 k_1 的每个子图作为(k_2,k_2)-VCS 方案的原始图像,那么可以得到 $k_1\times k_2$ 个子图。这就构成了两层(k_1k_2,k_1k_2)-VCS 方案且像素扩展为 $2^{k_1-1}\times 2^{k_2-1}$。

下面描述(k,k)-VCS 多层方案:

构造 1 $k=p_1^{a_1}p_2^{a_2}\cdots p_j^{a_j}$,$k>1$ 且 $p_1,p_2,\cdots,p_j$ 为不同的素数,a_1,

基金项目:国家重点基础研究发展规划(973)(the National Grand Fundamental Research 973 Program of China under Grant No.2007CB311201);国家自然科学基金(the National Natural Science Foundation of China under Grant No.60673072,No.60803149)。

作者简介:徐永平(1980-),男,硕士研究生,主要研究方向:信息安全,可视密码;胡予濮,男,教授,博士生导师;王明(1984-),男,硕士研究生;刘书盼,男,高级工程师。

收稿日期:2009-05-22 **修回日期**:2009-06-29

$a_2,\cdots,a_j$ 为正整数，则构成一个$(a_1+a_2+\cdots+a_j)$层(k,k)–VCS 方案，该方案包含$(1+p_1+p_1^2+\cdots+p_1^{a-1})$个$(p_1,p_1)$方案，$(p_1^{a_1}\times(1+p_2+p_2^2+\cdots+p_2^{a-1}))$个$(p_2,p_2)$方案，…，和$\prod_{i=1}^{j=1}p_i^{a_i}\times(\sum_{s=1}^{a_j}p_j^{(s-1)})$个$(p_j,p_j)$方案。当 $k=p_1^{a_1}p_2^{a_2}\cdots p_j^{a_j}$，共享子图大小为 $2^{a_1(p_1-1)}\times\cdots\times2^{a_j(p_j-1)}$。

定理 1[3] 对于(k,k)–VCS 方案，可以通过在(k,k)–VCS 方案里添加任意 $h(h<k)$个子图到另外 $k–h$ 个子图里来构造$(k–h,k–h)$–VCS 方案。

证明 设 $S_1,S_2,\cdots,S_k$ 为(k,k)–VCS 方案里的 k 个子图，当添加 $Si_1,Si_2,\cdots,Si_h$ 到另外 $k–h$ 个子图 $Sj_1,Sj_2,\cdots,Sj_{k-h}$ 形成新的 $k–h$ 个子图 $S'1=Sj_1+Si_1+Si_2+\cdots+Si_h$，$S'2=Sj_2+Si_1+Si_2+\cdots+Si_h$，$\cdots$，$S'k–h=Sj_{k-h}+Si_1+Si_2+\cdots+Si_h$ 这些新的 $k–h$ 个子图仅仅是在(k,k)–VCS 里的(h,k)中情况。因此，它们也满足方案条件。

构造 2 让 k 为一个范围$[2^{(b-1)}+1,2^b]$，那么可以利用$(2^b,2^b)$方案构造 b 层(k,k)–VCS 方案。该方案由 $2^b–1=(1+2+2^2+\cdots+2^{(b-1)})$个$(2,2)$–VCS 方案构成。

Shamir 的$(2,2)$–VCS 方案的基础矩阵为 $\boldsymbol{S}^0=\begin{bmatrix}1&0\\1&0\end{bmatrix}$，$\boldsymbol{S}^1=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，由构造 2 知，$(k,k)$–VCS 方案是由 $2^b–1=(1+2+2^2+\cdots+2^{(b-1)})$个$(2,2)$–VCS 方案构成，故$(k,k)$–VCS 方案的基础矩阵是由$(2,2)$–VCS 方案的基础矩阵对应的元素[1 0]，[0 1]再次进行$(2,2)$–VCS 方案的扩展构成，其基础矩阵集合 C_0,C_1 通过置换相应的基础矩阵获得，且大小为 2^{2^b-1}，用 r 表示。下面举例说明。

例 1 构造$(4,4)$–VCS 方案，需要两个$(2,2)$–VCS 方案。其黑白像素被分解成 4 个子像素，且两两成对。其基础矩阵如下：

$$\boldsymbol{S}^0=\begin{bmatrix}1&0&1&0\\0&1&1&0\\1&0&1&0\\0&1&1&0\end{bmatrix},\boldsymbol{S}^1=\begin{bmatrix}1&0&1&0\\1&0&0&1\\1&0&1&0\\0&1&1&0\end{bmatrix}$$

其基础矩阵集合 C_0,C_1 通过置换相应的基础矩阵获得，且大小为 8。注意这里基础矩阵集合与一般访问结构的矩阵集合的置换规则不同，以基础矩阵 S^0 的构造为例，其构造是对$(2,2)$–VCS 方案的基础矩阵对应的元素[1 0]，[0 1]再次进行$(2,2)$–VCS 方案的扩展。例如 [1 0] 扩展为两行四列$\begin{bmatrix}1&0&1&0\\0&1&1&0\end{bmatrix}$，$\begin{bmatrix}1&0&0&1\\0&1&0&1\end{bmatrix}$，$\begin{bmatrix}0&1&1&0\\1&0&1&0\end{bmatrix}$，$\begin{bmatrix}0&1&0&1\\1&0&0&1\end{bmatrix}$，与文献[3]不同，如此限定基础矩阵的构造克服了子像素恢复原像素时由白像素变为黑像素的错误，并且有利于编程实现。由文献[3]分析知，该方案满足安全性条件，即当参与者小于 k 个时，相同的矩阵以相同的概率出现。

由多层(k,k)–VCS 阈值方案构造的$(4,4)$–VCS 方案（图像按比例缩放 20%）。

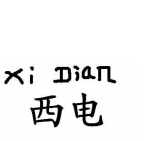

图 1　原始秘密图像

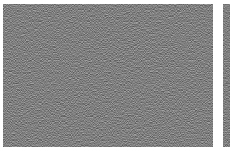

图 2　子秘密图 s1

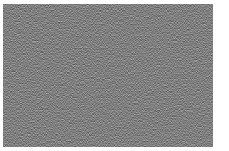

图 3　子秘密图 s2

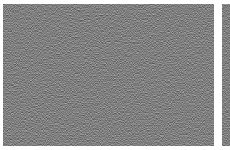

图 4　子秘密图 s3

图 5　子秘密图 s4

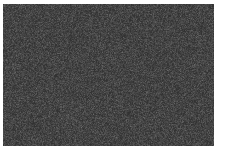

图 6　由子秘密图 s1、s2、s3 恢复的图像

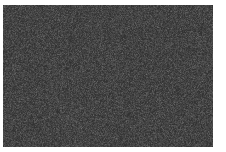

图 7　s2、s3、s4 恢复的图像

图 8　s1、s2、s3、s4 恢复的图像

例 2 由构造 1 构造$(15,15)$–VCS 方案，因为 $15=3\times5$，所以该方案需要一个$(3,3)$–VCS 方案和 5 个$(5,5)$–VCS 方案，且像素扩展为 $2^{(3-1)}\times2^{(5-1)}=64$，因为 $15<2^4$，所以利用 $2^4–1=15$ 个$(2,2)$–VCS 方案构造一个$(16,16)$–VCS 方案，且像素扩展为 $2^4=16$，利用定理可以得到$(15,15)$–VCS 方案具有像素扩展为 $2^4=16$。

最优像素扩展：Naor–Shamir 的(k,k)–VCS 方案像素扩展为 2^{k-1}；

构造 1 的像素扩展为：$2^{a_1(p_1-1)}\times\cdots\times2^{a_j(p_j-1)}$；

构造 2 的像素扩展为：2^b。

由此可知，构造 2 的像素扩展明显优于构造 1，故在二值图像(k,n)–VCS 可视密码方案中选用构造 2 的方法。

3　二值图像的阈值可视密码方案

3.1　二元域上特定线性方程组的解

未知数为 $x_1,x_2,\cdots,x_k,x_{k+1},\cdots,x_n,x_i\in\{0,1\},1\leqslant i\leqslant n$，考虑如下方程组：

$$\begin{cases}f_1=x_1+x_2+\cdots+x_{k-1}+x_k=0\\f_2=x_1+x_2+\cdots+x_{k-1}+x_{k+1}=0\\\cdots\\f_{n-k}=x_1+x_2+\cdots+x_{k-1}+x_n=0\end{cases}\text{和}\begin{cases}f_1=x_1+x_2+\cdots+x_{k-1}+x_k=1\\f_2=x_1+x_2+\cdots+x_{k-1}+x_{k+1}=1\\\cdots\\f_{n-k}=x_1+x_2+\cdots+x_{k-1}+x_n=1\end{cases}$$

容易看出 $x_k=x_{k+1}=\cdots=x_n=x_1+\cdots+x_{k-1}$。

3.2　强的访问结构

在文献[5]$(\Gamma_{Qual},\Gamma_{Forb})$为 n 个参与者的访问结构，构成一个$(\Gamma_{Qual},\Gamma_{Forb},m)$–VCS 的基础上定义一个具有强访问结构的$(k,n)$阈值 VCS 如下：

定义 2 $(\Gamma_{Qual},\Gamma_{Forb})$为 n 个参与者的访问结构。两个 $n\times m$

表 1　三种不同方案的像素扩展比较

k	2	3	4	5	6	7	8	9	10	15	20	30	40	50
最优像素扩展	2	4	8	16	32	64	128	256	1 024	2^{14}	2^{19}	2^{29}	2^{39}	2^{49}
k 的因式分解	1×2	1×3	2^2	1×5	2×3	1×7	2^3	3^2	2×5	3×5	2^2×5	2×3×5	2^3×5	2×5^2
构造 1 的像素扩展	2	4	4	16	8	64	8	16	32	64	64	128	128	1 024
$2^b\geqslant k$	2	2^2	2^2	2^3	2^3	2^3	2^3	2^4	2^4	2^4	2^5	2^5	2^6	2^6
构造 2 的像素扩展	2	4	4	8	8	8	8	16	16	16	32	32	64	64

的矩阵 C_0,C_1 集(多子集)构成一个$(\Gamma_{Qual},\Gamma_{Forb},m)$-VCS,如果存在 $\alpha(m)$和集合$\{(X,t_X)\}_{X\in\Gamma_{Qual}}$满足如下条件:

(1)对于任意子集 $X=\{i_1,i_2,\cdots,i_p\}\in\Gamma_{Qual}$ 通过重叠分存图像(透明胶片)恢复原始秘密图像。通常,$\forall M\in C_0$,对其 $i_1,i_2,\cdots,i_p$ 行进行或运算所得的向量 $\boldsymbol{V}$ 满足 $w(\boldsymbol{V})\leqslant t_X-\alpha(m)\cdot m$;而 $\forall M\in C_1$ 的结果为 $w(\boldsymbol{V})\geqslant t_X$。

(2)对于任意子集 $X=\{i_1,i_2,\cdots,i_p\}\in\Gamma_{Forb}$ 得不到任何信息。当 $t=0,1$,对由限定 C_t 中的每个 $n\times m$ 矩阵的第 $i_1,i_2,\cdots,i_p$,所得到的 2 个 $p\times m$ 矩阵的集合 $D_t,t\in\{0,1\}$ 相互之间是不可区分的,因为 D_0,D_1 中的所包含的矩阵是相同的,而且每一个矩阵出现的频率相同。

引理 3 设$(\Gamma_{Qual},\Gamma_{Forb})$在 p 个参与者的集合 $P=\{1,2,\cdots,p\}$ 上为一强的访问结构,且 $\Gamma_0=\{A_i,A_j\},A_i,A_j\subseteq P,|A_i\cup A_j|=p,|A_i|=|A_j|=p-1,p>2$,那么在 P 上存在一个强的$(\Gamma_{Qual},\Gamma_{Forb},m)$-VCS,且 $m=2^b,2^{b-1}<p-1\leqslant 2^b,t_X=m,\forall X\in\Gamma_{Qual}$。

证明 $A_i=\{i_1,i_2,\cdots,i_{p-1}\},A_j=\{j_1,j_2,\cdots,j_{p-1}\}$对于 $i\in\{i_1,i_2,\cdots,i_{p-1}\}$ 与变量 x_i 关联,$j\in\{j_1,j_2,\cdots,j_{p-1}\}$与变量 x_j 关联,A_i,A_j 分别与方程f_{A_i},f_{A_j}关联,方程如下:

$$f_{A_i}=x_{i_1}+x_{i_2}+\cdots+x_{i_{p-1}}\quad f_{A_j}=x_{j_1}+x_{j_2}+\cdots+x_{j_{p-1}}$$

在二元域上考虑如下方程组:

$$\begin{cases}f_{A_i}=0\\f_{A_j}=0\end{cases}\text{和}\begin{cases}f_{A_i}=1\\f_{A_j}=1\end{cases}$$

由第 3.1 节知,解上述方程式有 $p-2$ 个变量与其他两个变量值相等。假设前 $p-2$ 个变量为 $x_1,x_2,\cdots,x_{p-2}$,剩余的两个变量分别为 x_{p-1},x_p,则有 $x_1+x_2+\cdots+x_{p-2}=x_{p-1}=x_p$。

再由多层(k,k)-VCS 方案构造知,$m=2^b,2^{b-1}<p-1\leqslant 2^b,t_X=m,\forall X\in\Gamma_{Qual}$ 构造的基础矩阵 $\boldsymbol{S}^0,\boldsymbol{S}^1$ 为 $p\times 2^b$ 的布尔矩阵。将矩阵每行对应向量分配给变量 $x_1,x_2,\cdots,x_p$,又每个变量对应一个参与者,所以由 $x_1,x_2,\cdots,x_{p-2},x_{p-1}$ 和 $x_1,x_2,\cdots,x_{p-2},x_p$ 所对应的行向量重叠能够恢复秘密图像。

由上述引理得出如下结论:

结论 2 设 $P=\{1,2,\cdots,p,p+1,\cdots,n\}$。那么引理构造的矩阵 $\boldsymbol{S}^0,\boldsymbol{S}^1$ 可以扩展成 $n\times 2^b$ 布尔矩阵,且$(n-p)\times 2^b$ 空矩阵对应非必要参与者 $p+1,p+2,\cdots,n$,由此得到一个强的$(\Gamma_{Qual},\Gamma_{Forb},m)$-VCS,且 $m=2^b,2^{b-1}<p-1\leqslant 2^b,t_X=m,\forall X\in\Gamma_{Qual}$。

3.3　由较小的方案构造 VCS

设$(\Gamma'_{Qual},\Gamma'_{Forb})$$(\Gamma''_{Qual},\Gamma''_{Forb})$为两个在 n 个参与者集合 P 里的方案。假设 $i\in P$ 是$(\Gamma'_{Qual}\Gamma'_{Forb})$非有效参与者,类似情况在$(\Gamma''_{Qual}\Gamma''_{Forb})$。存在$(\Gamma'_{Qual},\Gamma'_{Forb},m)$-VCS,$(\Gamma''_{Qual},\Gamma''_{Forb},m)$-VCS 基础矩阵为 $\boldsymbol{R}^0,\boldsymbol{R}^1$ 和 $\boldsymbol{T}^0,\boldsymbol{T}^1$。构造 VCS 的访问结构$(\Gamma_{Qual},\Gamma_{Forb})=(\Gamma'_{Qual}\cup\Gamma''_{Qual},\Gamma'_{Forb}\cap\Gamma''_{Forb})$,通过 $\boldsymbol{R}^0,\boldsymbol{R}^1$ 和 $\boldsymbol{T}^0,\boldsymbol{T}^1$ 构造两对矩阵,$(\hat{\boldsymbol{R}}^0,\hat{\boldsymbol{R}}^1)$和$(\hat{\boldsymbol{T}}^0,\hat{\boldsymbol{T}}^1)$,每个包含 n 行。构造一个$\hat{\boldsymbol{R}}^0$,对于 $i=1,\cdots,n$,如果 i 是非有效参与者,那么$\hat{\boldsymbol{R}}^0$ 的第 i 行全为 0;否则,为相应的参与者的$\hat{\boldsymbol{R}}^0$ 的第 i 行。其他类似构造。最后,对于$(\Gamma_{Qual},\Gamma_{Forb})$的基础矩阵 $\boldsymbol{S}^0$ 通过级连矩阵$\hat{\boldsymbol{R}}^0$ 和$\hat{\boldsymbol{T}}^0$ 实现。

定理 4[5] $(\Gamma'_{Qual},\Gamma'_{Forb})$,$(\Gamma''_{Qual},\Gamma''_{Forb})$为两个在 n 个参与者 P 上的访问结构。存在 $(\Gamma'_{Qual},\Gamma'_{Forb},m)$-VCS,$(\Gamma_{Qual},\Gamma_{Forb},m)$-VCS 具有基础矩阵 $\boldsymbol{R}^0,\boldsymbol{R}^1$ 和 $\boldsymbol{T}^0,\boldsymbol{T}^1$。那么由前面构造产生的$(\Gamma'_{Qual}\cup\Gamma''_{Qual},\Gamma'_{Forb}\cap\Gamma''_{Forb},m'+m'')$-VCS。如果原来的两个矩阵是强的访问结构。

3.4　二值图像的阈值可视密码方案

定理 5 设$(\Gamma_{Qual},\Gamma_{Forb})$为强的访问结构在 n 个参与者的集合 $P=\{1,2,\cdots,n\}$,且 $\Gamma_0=\{A\subseteq P:|A|=k\},2\leqslant k\leqslant n$,那么存在一个强的$(k,n)$-VCS,$m_1=l\cdot 2^b,l=C_n^k,2^{b-1}<k<2^b,\alpha(m)=1/m_1$。

证明 由题设 $\Gamma_0=\{A\subseteq P:|A|=k\},2\leqslant k\leqslant n=\{A_1,A_2,\cdots,A_l:|A_i|=k,i=1,2,\cdots,l\}$,设集合 A_i 的访问结构为$(\Gamma^i_{Qual},\Gamma^i_{Forb})$,由定义 2、定理 3、定理 4 及第 2 章的构造 2,很容易证明存在一个强的(k,n)-VCS,$m_1=l\cdot 2^b,l=\binom{n}{k},2^{b-1}<k<2^b,\alpha(m)=1/m_1$。

引理 6 设 $P=\{1,2,\cdots,n\}$,考虑 P 的所有可能的 k 个元素的子集 $B_1,B_2,\cdots,B_l,l=C_n^k$,如果 l 是偶数,那么存在置换 σ 在 $\{1,2,\cdots,l\}$上使得$|B_{\sigma(2i-1)}\cap B_{\sigma(2i)}|=k-1$,对于所有的 $i=1,2,\cdots,l/2$,如果 l 是奇数,那么也存在置换 σ 在$\{1,2,\cdots,l\}$上使得$|B_{\sigma(2i-1)}\cap B_{\sigma(2i)}|=k-1$,对于所有的 $i=1,2,\cdots,\lfloor l/2\rfloor$。

证明 直接由参考文献[4]可得。

定理 7 设$(\Gamma_{Qual},\Gamma_{Forb})$为强的访问结构在 n 个参与者的集合 $P=\{1,2,\cdots,n\}$,且 $\Gamma_0=\{A\subseteq P:|A|=k\},2\leqslant k\leqslant n$,那么存在一个强的$(k,n)$-VCS,$m_2=\lceil C_n^k/2\rceil\cdot 2^b,2^{b-1}<k<2^b,\alpha(m)=1/m_2$。

证明 令 $l=C_n^k$,设 l 为偶数。由引理 6,定理 4 和构造 2 可得 $m_2=\dfrac{l}{2}\cdot 2^b$。

设 l 为奇数。仍由引理 6,定理 4 和构造 2 可得 $m_2=\dfrac{l-1}{2}\cdot 2^b+2^b$。

即 $m_2=\lceil\dfrac{C_n^k}{2}\rceil\cdot 2^b$。最后,由$(k,n)$-VCS 的基础矩阵的构造得到 $\alpha(m)=1/m_2$。因此得证。

引理 8 设 $P=\{1,2,\cdots,n\}$,考虑 P 的所有可能的 k 个元素的子集 $B_1,B_2,\cdots,B_l,l=C_n^k$,如果将其子集中有 $k-1$ 个元素相同的子集归类,那么可以归为:当 $k=2$ 时,为 $n-1$ 类,$(n-1)\leqslant C_n^2=n(n-1)/2$,当 $k>2$ 时,为$\lfloor n/(k-1)\rfloor+\lceil[C_n^k-\lfloor n/(k-1)\rfloor\times(n-k+1)]/2\rceil$类,且当 $2<k<n-1$ 时,下式成立:

$$\lfloor\frac{n}{k-1}\rfloor+\lceil\frac{C_n^k-\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}\rceil<\lceil\frac{C_n^k}{2}\rceil\qquad(1)$$

证明 当 $k=2$ 时,很显然。

当 $k>2$ 时,分四种情况讨论:

情况 1 若 $C_n^k\equiv 0(\bmod 2)\lfloor n/(k-1)\rfloor\times(n-k+1)\equiv 0(\bmod 2)$,那么式(1)等价于$\lfloor\dfrac{n}{k-1}\rfloor-\dfrac{\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}<0\Leftrightarrow 1<\dfrac{n-k+1}{2}\Leftrightarrow 2<k<n-1$;

情况 2 $C_n^k\equiv 0(\bmod 2),\lfloor\dfrac{n}{k-1}\rfloor\times(n-k+1)\equiv 0(\bmod 2)$,那么式(1)等价于$\lfloor\dfrac{n}{k-1}\rfloor<\dfrac{\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}-\dfrac{1}{2}\Leftrightarrow 1<\dfrac{n-k+1}{2}+\dfrac{1}{2\lfloor\frac{n}{k-1}\rfloor}\Leftrightarrow 1<\dfrac{n-k+1}{2}\Leftrightarrow 2<k<n-1$;

情况 3 $C_n^k\equiv1(\mathrm{mod}\ 2)$,$\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)\equiv0(\mathrm{mod}\ 2)$,那么式(1)等价于$\lfloor\frac{n}{k-1}\rfloor<\frac{\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}\Leftrightarrow2<k<n-1$;

情况 4 $C_n^k\equiv1(\mathrm{mod}\ 2)$,$\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)\equiv1(\mathrm{mod}\ 2)$,那么式(1)等价于$\lfloor\frac{n}{k-1}\rfloor<\frac{\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}\Leftrightarrow1<\frac{n-k+1}{2}\Leftrightarrow2<k<n-1$,所以得证。

例 3 设 $P=\{1,2,3,4,5,6\}$,则其中 4 个元素的所有可能子集共有 $C_6^4=15$ 个,具体分类如下:{1,2,3,4},{1,2,3,5},{1,2,3,6};{1,2,4,5},{1,2,4,6};{1,2,5,6},{1,3,5,6};{1,5,3,4},{1,6,3,4};{1,4,5,6},{2,4,5,6},{3,4,5,6};{2,3,4,5},{2,3,4,6};{2,3,5,6},共计 7 类。

定理 9 设$(\Gamma_{Quad},\Gamma_{Forb})$为强的访问结构在 n 个参与者的集合 $P=\{1,2,\cdots,n\}$,且 $\Gamma_0=\{A\subseteq P:|A|=k\}$,$2\leqslant k\leqslant n$ 那么存在一个强的(k,n)-VCS。

$$m_3=\begin{cases}(n-1)\cdot2^b & k=2,b=1\\ (\lfloor\frac{n}{k-1}\rfloor+\lceil\frac{C_n^k-\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}\rceil)\cdot2^b & k>2,2^{b-1}<k<2^b\end{cases}$$

$$\alpha(m)=\frac{1}{m_3}$$

证明 由第 2 章构造 2,第 3.1 节线性方程组解的特征,引理 3、结论 2、定理 4 及引理 8 可以得出结论:$m_3=\begin{cases}(n-1)\cdot2^b & k=2,b=1\\ (\lfloor\frac{n}{k-1}\rfloor+\lceil\frac{C_n^k-\lfloor\frac{n}{k-1}\rfloor\times(n-k+1)}{2}\rceil)\cdot2^b & k>2,2^{b-1}<k<2^b\end{cases}$,同时由定义 2 及$(k,n)$-VCS 方案结构得到 $\alpha(m)=\frac{1}{m_3}$,得证。

例 4 由定理 9 构造的一个强访问结构(4,6)-VCS。利用例 1,例 3 结果得到第一类子集为{1,2,3,4},{1,2,3,5},{1,2,3,6},则其基础矩阵为:$\boldsymbol{S}_1^0=\begin{bmatrix}1&0&1&0\\0&1&1&0\\1&0&1&0\\0&1&1&0\\0&1&1&0\\0&1&1&0\end{bmatrix}$,$\boldsymbol{S}_1^1=\begin{bmatrix}1&0&1&0\\1&0&0&1\\1&0&1&0\\0&1&1&0\\0&1&1&0\\0&1&1&0\end{bmatrix}$,其余类依次,构造基础矩阵如下:

$\boldsymbol{S}^0=$

$$\begin{bmatrix}\overbrace{1\ 0\ 1\ 0}^{s_1^0}&\overbrace{1\ 0\ 0\ 1}^{s_2^0}&\overbrace{0\ 1\ 1\ 0}^{s_3^0}&\overbrace{0\ 1\ 0\ 1}^{s_4^0}&\overbrace{1\ 0\ 1\ 0}^{s_5^0}&\overbrace{0\ 0\ 0\ 0}^{s_6^0}&\overbrace{0\ 0\ 0\ 0}^{s_7^0}\\0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&1\ 0\ 1\ 0\\1\ 0\ 1\ 0&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&0\ 1\ 1\ 0&0\ 1\ 0\ 1&0\ 1\ 1\ 0\\0\ 1\ 1\ 0&1\ 0\ 0\ 1&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&0\ 0\ 0\ 0\\0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0&0\ 1\ 1\ 0&1\ 0\ 0\ 1&0\ 1\ 0\ 1&1\ 0\ 1\ 0\\0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0&0\ 1\ 1\ 0&0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0\end{bmatrix}$$

$\boldsymbol{S}^0=$

$$\begin{bmatrix}\overbrace{1\ 0\ 1\ 0}^{s_1^1}&\overbrace{1\ 0\ 0\ 1}^{s_2^1}&\overbrace{0\ 1\ 1\ 0}^{s_3^1}&\overbrace{0\ 1\ 0\ 1}^{s_4^1}&\overbrace{1\ 0\ 1\ 0}^{s_5^1}&\overbrace{0\ 0\ 0\ 0}^{s_6^1}&\overbrace{0\ 0\ 0\ 0}^{s_7^1}\\1\ 0\ 0\ 1&1\ 0\ 1\ 0&0\ 1\ 0\ 1&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&1\ 0\ 1\ 0\\1\ 0\ 1\ 0&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&0\ 1\ 1\ 0&0\ 1\ 0\ 1&0\ 1\ 1\ 0\\0\ 1\ 1\ 0&1\ 0\ 0\ 1&0\ 0\ 0\ 0&1\ 0\ 1\ 0&1\ 0\ 1\ 0&1\ 0\ 0\ 1&0\ 0\ 0\ 0\\0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0&0\ 1\ 1\ 0&1\ 0\ 0\ 1&0\ 1\ 0\ 1&1\ 0\ 1\ 0\\0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0&0\ 1\ 1\ 0&0\ 1\ 1\ 0&0\ 1\ 0\ 1&1\ 0\ 1\ 0\end{bmatrix}$$

其像素扩展为 28,利用文献[2]定理 3 的方法像素扩展为 64,利用定理 3.5 和定理 3.7 的像素扩展分别为 64 和 32。且其基础矩阵的置换的集合 C_0,C_1 为 $7!\cdot8^7$ 种。

例 5 由定理 9 构造一个强的访问结构(2,3)-VCS。

其基础矩阵为 $\boldsymbol{S}^0=\begin{bmatrix}1&0&0&1\\1&0&0&0\\1&0&0&1\end{bmatrix}$,$\boldsymbol{S}^1=\begin{bmatrix}1&0&1&0\\0&1&0&0\\1&0&0&1\end{bmatrix}$,其像素扩展为 4,对比度为 1/4,且基础矩阵的置换的集合 C_0,C_1 为 8 种。

由定理 9 构造的(2,3)-VCS 方案(按比例缩放 20%):

图 9 原始秘密图像

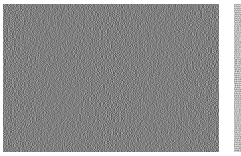

图 10 子秘密图像 $t1$

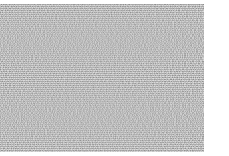

图 11 子秘密图像 $t2$

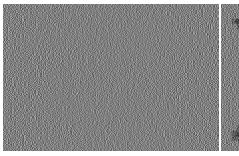

图 12 子秘密图像 $t3$

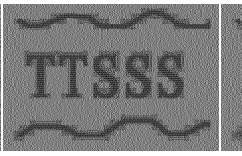

图 13 $t1,t2$ 恢复的图像

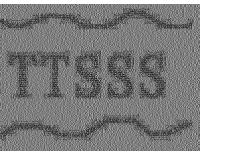

图 14 $t2,t3$ 恢复的图像

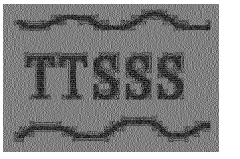

图 15 $t1,t3$ 恢复的图像

结论 3 由多层(k,k)-VCS 构造方案的基础矩阵的置换的集合容易知道定理 3.8 构造的基础矩阵的集合 C_0,C_1 为 $k!\cdot(2^{2^k-1})^k$,$k=\lfloor\frac{n}{m-1}\rfloor+\lceil\frac{C_n^m-\lfloor\frac{n}{m-1}\rfloor\times(n-k+1)}{2}\rceil$,$2<k<n-1$。

3.5 一些(k,n)-VCS 方案的像素扩展的比较

由上面结论得到不同方案像素扩展部分 k 值如表 2($n\geqslant k$)。

$l=C_n^k$,$k=\lfloor\frac{n}{m-1}\rfloor+\lceil\frac{C_n^m-\lfloor\frac{n}{m-1}\rfloor\times(n-k+1)}{2}\rceil$,$2<k<n-1$。$m_{our}$ 为文献[2]定理 3 的像素扩展,m_1,m_2,m_3 分别为该文定理 5、定理 7、定理 9 的像素扩展。

由表可以看出定理 9 方案的像素扩展明显优于其他方案的像素扩展。

比较如下:

$$\begin{cases}m_{our}<m_1 & k=2,3\\ m_{our}\geqslant m_1 & k=4,5\\ m_{our}>m_1 & k>5\end{cases}\quad\begin{cases}m_{our}=m_2 & k=2,3\\ m_{our}>m_2 & k>3\end{cases}\quad\begin{cases}m_1=m_2 & n=2\\ m_1>m_2 & n>2\end{cases}$$

$$\begin{cases}m_2=m_3 & k=2,n=2\\ m_2>m_3 & 2\leqslant k<n-1,n>3\end{cases}$$

(下转 88 页)