# 一种新的(k,n)阈值可视密钥分存方案

黄东平,王道顺,黄连生,戴一奇
(清华大学计算机科学与技术系 北京 100084)

**摘 要:** 本文提出(k,n)阈值可视秘密分存的一种新的分析和实现方案.该方案从可视分存的对比度条件和安全性条件入手,建立起一个方程组,最后得到其近似最优解和基本矩阵的构造方案.该方案将(k,n)和(n,n)方案统一起来分析,使之和谐统一;同时,通过理论分析代替了以往算法的部分工作;本文给出的算法可达到以往方案的安全强度而具备更高的实现效率.

**关键词:** 阈值; 秘密分存; 可视密码
**中图分类号:** TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2006) 03-0503-05

# A Novel (k,n) Threshold Scheme for Visual Secret Sharing

HUANG Dong-ping, Wang Dao-shun, Huang Lian-sheng, Dai Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

**Abstract:** A novel k-out-of-n threshold scheme for visual secret sharing is proposed. The construction scheme of basic matrix is brought forward from the approximate best optimized solution of the equation set which is established on the basis of contrast condition and security condition of the visual secret sharing. The proposed method analyses the (k, n) and (n,n) schemes uniformly and brings them into an integral framework. Furthermore, a fraction of algorithm operations were replaced by theoretical analysis in the new scheme. Consequently, it achieves higher efficiency with same security intensity compared with the previous schemes.

**Key words:** threshold; secrest sharing; visual cryptography

## 1 背景介绍

秘密共享方案用于在一组参与者中分享秘密.每个参与者获取一部分秘密信息(称为一个共享).参与者集合的一些子集(称为授权子集)联合可以恢复共享的秘密,而其他子集(称为禁止集)得不到秘密的任何信息.(n,k)阈值方案是一种特殊的秘密共享方案,当至少 $k$ 个参与者联合时能得到秘密,而少于 $k$ 个则不能.传统的实现方案见Blakley, Shamir 和 Ito 等人[1~3]的研究.

1994年,Naor 和 Shamir 提出可视分存的概念,它利用人的视觉系统完成解码运算[4].在一个(k,n)可视分存方案中,将有 $n$ 份透明片,将其中任意 $k$ 份叠加,秘密图像将显示出来.而从至多 $k-1$ 份透明片将无法得到秘密图像的任何信息.可视分存的优势在于它的解码方式.传统的阈值方案的解码通常需要借助计算机在有限域里进行计算,而可视分存方案的解码用人的视觉系统完成.因此,人们对可视分存产生了极大的研究兴趣,并且在多个领域里尝试,如网络安全,版权保护等[15,16].

文献[4]的(k,n)可视秘存方案造成巨大的象素膨胀,不便于实际使用.文[5]对此做了改进,提出一种新方案,象素膨胀度小得多,可以被实际操作所接受.众多的研究者在此基础上进行了大量的研究,如[7,8]等研究了如何得到最优的对比度,以使得更利于视觉系统的分辨;文[9~11]等研究如何提高恢复的秘密图像的黑白象素的效果;文[12~14]等研究了基于彩色图的秘密分存;文[15,16]等研究了可视秘密分存的应用.

尽管人们把很多精力投入到了灰度图和彩色图的分存上,黑白图的可视分存仍然有研究的价值.尽管优化对比度有利于视觉系统恢复秘密,彩色图分存能丰富分存图的内容,但都是以牺牲信息率为代价的,而信息率也是秘密分存系统最重要的指标之一.更进一步,黑白图分存的研究对彩色图的分存有重要的指导意义,甚至一些彩色图分存算法直接以黑白图分存为基础[12].迄今也仍只有个别方案在极个别情形下膨胀度优于文[5],因此它在可视分存里占有重要地位.文[6]从可视分存的定义出发,用数学方程描述可视分存的安全性条件和对比度条件,得到了一种实现(k,n)方案的新方法.该方法与文[5]有相同的效果,而实现效率更高.

然而,他们的工作的一个共同点是先构造(n,n)方案,然后将其扩展到一般的(k,n)方案.也就是说,他们将(n,n)和(k,n)方案分别分析,而不是作为一个整体.本文提出一种实现(k,n)可视秘存阈值方案的新方法.不同于已有实现方式的是,该方法采用不同的分析和实现步骤,将(k,

收稿日期:2005-03-25;修回日期:2005-10-21
基金项目:国家自然科学基金(No.90304014);国家863高技术研究发展计划(No.2005AA114160)

$n$)和($n$,$n$)方案纳入到一个统一的框架里;另一方面,得到的结果具有相同的安全性,而实现效率更高. 本文的工作也采用了数学方程的方式,但相比文[6],本文提出的方程组物理意义更清晰,形式更简单,分析也更简单、直接. 本文第 2 节介绍基本模型并完成分析,第 3 节给出实现算法,第 4 节是结论部分. 理解可视分存思想最简单的途径是考察一个具体的例子,附录部分给了一个(2,3)方案,要解码消息,只需要将任意两个共享对齐并叠在一起,秘密信息将显示出来.

## 2 基本模型

本文考虑的是最简单的情形. 假设秘密图像由黑白两种象素构成,$n$ 个处理过的共享对原始图像进行分存. 原始图像中的单个象素在每个共享里膨胀为 $m$ 个黑白子象素,它们的位置彼此很靠近,这样人的视觉系统看到的是这些子象素整体的平均效果. 分存可以被描述为一个 $n\times m$ 的布尔矩阵 $\boldsymbol{S}_{n\times m}=[S_{ij}]$,其中 $S_{ij}=1$ 当且仅当第 $i$ 张透明片的第 $j$ 个子象素为黑色. 当第 $i_1,\cdots,i_r(1\leqslant r\leqslant n)$ 张透明片对齐叠加在一起,我们得到一个共享的组合,记为向量 $\boldsymbol{V}$,它的每个分量(子象素)是矩阵 $\boldsymbol{S}_{n\times m}$ 的第 $i_1,i_2,\cdots,i_r$ 行的布尔或. $\boldsymbol{V}$ 的灰度正比于它的海明重(记做 $H(V)$),任意交换 $\boldsymbol{S}_{n\times m}$ 的列的顺序(称为列置换)不影响 $H(V)$ 的值. 为了保证安全性,少于 $k$ 个共享时不能分辨原始象素是黑或白,也即少于 $k$ 个共享叠加时黑白原始象素对应的布尔向量的海明重一致. 在以往的研究中,人们往往采用的是一个直观上更强的条件:从 $\boldsymbol{S}^t_{n\times m}$,$t\in\{0,1\}$,任选少于 $k$ 行得到的子矩阵经有限次列置换后相等(文中称能够通过有限次列置换变成相等矩阵的两个矩阵不可区分). 下面我们证明这两个定义是等价的.

**命题 1** 从 $\boldsymbol{S}^t_{n\times m}$ 里任取 $0<r<k$ 行得到子矩阵 $\boldsymbol{S}^t_{r\times m}$,以下两个条件等价:(1)$\boldsymbol{S}^t_{r\times m}$ 的海明重一致,(2)$\boldsymbol{S}^t_{r\times m}$ 不可区分.

证明 (2)⇒(1)显然成立.

下面证明:(1)⇒(2). 我们用数学归纳法进行证明.

$r=1$ 时显然成立. 假设 $r<q$ 时上述结论都成立. 则当 $r=q$ 时,设列置换后两个矩阵的不同部分为两个 $r\times c$ 的子矩阵 $\boldsymbol{S}^0_{r\times c}$ 和 $\boldsymbol{S}^1_{r\times c}$,其中 $0<c\leqslant m$. 由归纳假设,从 $\boldsymbol{S}^t_{r\times c}$ 中去掉任意一行后的子矩阵不可区分,那么从 $\boldsymbol{S}^0_{r\times c}$ 中任取第 $i$ 列 $\boldsymbol{v}_i$,在 $\boldsymbol{S}^1_{r\times c}$ 中必有列向量 $\boldsymbol{v}_{i,1},\boldsymbol{v}_{i,2},\cdots,\boldsymbol{v}_{i,l}$ 与 $\boldsymbol{v}_i$ 分别仅在第 $1,2,\cdots,r$ 行不同. 同样,$\boldsymbol{S}^1_{r\times c}$ 中的任何列向量也有这样的性质. $\boldsymbol{S}^0_{r\times c}$、$\boldsymbol{S}^1_{r\times c}$ 必然包含了所有的 $2^r$ 种列向量,并且两个矩阵分别包括了含有奇(偶)数个“1”的列向量. 二者有且只有一个包括全部为“0”的列. 这样,这 $r$ 个分存叠加后的海明重不一致,这与已知条件矛盾! $c=0$,结论成立.

通常情况下,一个($k$,$n$)可视分存方案包括两个由 $n\times m$ 的布尔矩阵构成的集合. 两个矩阵集合可以通过将布尔矩阵 $\boldsymbol{S}^0_{n\times m}$ 和 $\boldsymbol{S}^1_{n\times m}$ 列置换得到,因此实现一个($k$,$n$)方案的关键步骤是构造合适的 $\boldsymbol{S}^0_{n\times m}$ 和 $\boldsymbol{S}^1_{n\times m}$.

**定义 2**[4] 两个布尔矩阵 $\boldsymbol{S}^0_{n\times m}$ 和 $\boldsymbol{S}^1_{n\times m}$ 是($k$,$n$)可视分存方案的一个解,如果对于给定的常数 $\alpha\geqslant 1$ 和 $d\in\{1,\cdots,m\}$,它们满足下面三个条件:

(1)$\boldsymbol{S}^1_{n\times m}$ 的任意 $k$ 行做布尔或得到的向量 $\boldsymbol{V}$ 满足 $H(V)\geqslant d$.

(2)$\boldsymbol{S}^0_{n\times m}$ 的任意 $k$ 行做布尔或得到的向量 $\boldsymbol{V}$ 满足 $H(V)\leqslant d-\alpha\times m$.

(3)对 $\{1,\cdots,n\}$ 的任意子集 $\{i_1,\cdots,i_q\}$,其中 $q<k$,取出 $\boldsymbol{S}^0_{n\times m}$ 和 $\boldsymbol{S}^1_{n\times m}$ 的第 $i_1,\cdots,i_q$ 行得到的两个子矩阵在列变换下无法区分,即它们以不同的顺序包含相同的列,两个子矩阵的海明重一致.

其中 $m$ 是子象素的膨胀度,$\alpha\geqslant 1/m$ 代表对比度,而 是 $k\in\{1,\cdots,m\}$ 一个表示灰度的阈值.

条件 1 和 2 保证了当 $k$ 个共享叠加在一起时能够得到秘密图像. 条件 3 表示即使有无穷的计算资源,通过分析少于 $k$ 个共享,仍然无法得到分存图像象素是黑还是白的任何信息. 前两个称为对比度条件,而第三个称为安全性条件.

例如,一个(2,2)方案可以用两个 $\boldsymbol{S}_{2\times 2}$ 矩阵,如 $\begin{bmatrix}0&1\\0&1\end{bmatrix}$(表示白象素 0)和 $\begin{bmatrix}1&0\\0&1\end{bmatrix}$(表示黑色象素 1). 第 1 个共享根据原始秘密图像选择相应矩阵的第 1 行,第 2 个共享选取第 2 行. 白色象素对应的两个共享叠加的海明重为 1,而黑色象素的两个共享叠加后为 2,看起来颜色更深一些. 出于安全性的考虑,我们将上面两个矩阵的列做置换,得到两个矩阵集合(分别对应黑白象素). 对原始图像的象素分存时,根据象素从相应的矩阵集合里随机取出一个矩阵.

**定理 3** 设 $\boldsymbol{S}^t_{n\times m}(t\in\{0,1\})$ 是一个($k$,$n$)可视分存方案,$\boldsymbol{S}^t_{k\times m}$ 是从 $\boldsymbol{S}^t_{n\times m}$ 中任意选取的 $k$ 行组成的子矩阵. $\forall r\in\{1,\cdots,k-1\}$,$\{i_1,\cdots,i_r\}\subseteq\{1,\cdots,k\}$,设 $N^t_{|i_1,\cdots,i_r|}$ 是 $\boldsymbol{S}^t_{k\times m}$ 中在第 $i_1,\cdots,i_r$ 行为“1”,而在其他行为“0”的列的数目. 那么:

$$N^0_{|i_1,\cdots,i_r|}-N^1_{|i_1,\cdots,i_r|}=(-1)^r\delta$$

其中 $\delta=H(\boldsymbol{S}^1_{k\times m})-H(\boldsymbol{S}^0_{k\times m})$.

证明 对每个 $\{i_1,\cdots,i_r\}\subseteq\{1,\cdots,k\}$,选取 $\boldsymbol{S}^t_{k\times m}$ 的第 $i_1,\cdots,i_r$ 行形成两个子矩阵 $\boldsymbol{S}^t_{r\times m}(t\in\{0,1\})$,剩下的 $k-r$ 行组成另外两个子矩阵 $\boldsymbol{S}^t_{(k-r)\times m}(t\in\{0,1\})$. 我们不妨设选中的是前 $r$ 行(如图 1($a$)示). 根据定义 2 的条件 3,$H(\boldsymbol{S}^0_{(k-r)\times m})=H(\boldsymbol{S}^1_{(k-r)\times m})$,那么 $\boldsymbol{S}^0_{(k-r)\times m}$ 和 $\boldsymbol{S}^1_{(k-r)\times m}$ 中,海明重为 0 的列的数目相等,记作 $l$. 矩阵的列可以交换,不失一般性,设 $\boldsymbol{S}^t_{(k-r)\times m}$ 最后 $l$ 列海明重为 0. 这样,$\boldsymbol{S}^t_{k\times m}$ 可以被分成如图 1($a$)所示的四个部分.

我们定义 $R^t_i\subseteq\{1,2,\cdots,l\}$,$i\in\{1,\cdots,r\}$,当且仅当 $\boldsymbol{S}^t_{r\times l}[i,j]=1$ 时 $j\in R^t_i$. $R^t_i$ 中的元素为 $\boldsymbol{S}^t_{r\times l}$ 中第 $i$ 行的含有“1”的列号,显然,$|R^t_1\cap\cdots\cap R^t_r|$ 表示 $N^t_{|i_1,\cdots,i_r|}$. 我们分析 $\boldsymbol{S}^t_{k\times m}$ 的海明重.

$$H(\boldsymbol{S}^t_{k\times m})=H(\boldsymbol{S}^t_{(k-r)\times(m-l)})+H(\boldsymbol{S}^t_{r\times l})$$

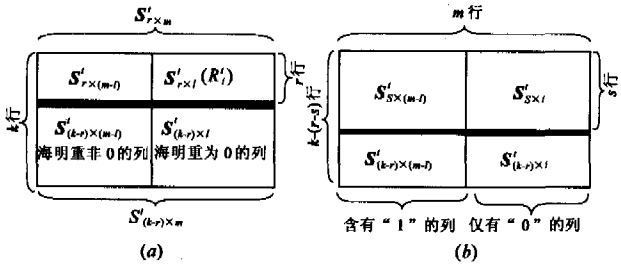



图1　$S^t_{k\times m}$和$S^t_{k-(r-s)\times m}$

$$=(m-l)+H(S^t_{kr\times l})$$
$$=(m-l)+|R^t_1\cup\cdots\cup R^t_r| \tag{1}$$

根据容斥原理：

$$|R^t_1\cup\cdots\cup R^t_r|=\sum_{i=1}^{r}|R^t_i|-\sum_{i<j}|R^t_i\cap R^t_j|+\cdots+(-1)^{r+1}|R^t_1\cap\cdots\cap R^t_r| \tag{2}$$

考虑到定义2的条件3，$\forall s(<r)$，从图1(a)中删除$r-s$行后，余下的$(k-(r-s))\times m$的布尔矩阵(图1(b))是不可区分的，也即它们含有相同的列(列顺序可能不一致)．根据划分的规则，图1(b)中前$m-l$列不可能与后$l$列一致，那么，这两个$(k-(r-s)\times m)$布尔矩阵的后$l$列不可区分(图1(b))．而$S^t_{(k-r)\times l}$是零矩阵，这样$S^t_{s\times l}$不可区分．由此可得到如下关系：

$$|R^0_{i1}\cap\cdots\cap R^0_{is}|=|R^1_{i1}\cap\cdots\cap R^1_{is}|$$

其中$\{i1,\cdots,is\}\subseteq\{1,\cdots,r\}(s<r)$．再结合式(1)和(2)，有：

$$|R^0_1\cap\cdots\cap R^0_r|-|R^1_1\cap\cdots\cap R^1_r|=(-1)^r(H(S^0_{k\times m})-H(S^1_{k\times m}))=(-1)^r\delta$$

另外，我们注意到$r=k$时该结论仍然成立，这可以直接从式(2)得到．　　证毕．

**定理4**　设$T_{n,p}(p<n)$是一个包括所有海明重为$p$的$n$维向量一次且仅一次的$n\times C^p_n$布尔矩阵．那么$T_{n,p}$将$C^{p-q}_{n-k}$次包括它的每个$k\times C^p_n$子矩阵$T_{k,q}$，其中$\max(0,p-(n-k))\leqslant q\leqslant\min(k,p)$．

这个定理可以很容易的从文[5]的结论得到，这里略去证明过程．

假设$S^t_{n\times m}$包含$\alpha^t_p(\geqslant 0)$个$T_{n,p}$，$S^t_{k\times m}$包括$\beta^t_r(\geqslant 0)$个$T_{k,r}$．可以通过各个不同$T_{n,p}$里面的$T_{k,r}$的数目计算$\beta^t_r$：

$$\sum_{p=0}^{n}\alpha^t_p C^{p-r}_{n-k}=\beta^t_r$$

为了叙述方便，我们令$y<0$或$y>x$时$C^y_x=0$．考虑$t=0$和$t=1$两种情形，容易得到

$$\sum_{p=0}^{n}(\alpha^0_p-\alpha^1_p)C^{p-r}_{n-k}=\beta^0_r-\beta^1_r$$

由定理3，　$\sum_{p=0}^{n}\gamma_p C^{p-r}_{n-k}=\beta^0_r-\beta^1_r=(-1)^r\delta$

其中$\gamma_p=\alpha^0_p-\alpha^1_p$．通常，我们希望膨胀度$m$比较小，便于视觉系统分辨，因此令$\delta=1$．这样，我们得到的如下方程组：

$$\sum_{p=0}^{n}\gamma_p C^{p-r}_{n-k}=(-1)^r,r=0,\cdots,k \tag{3}$$

这是本文最重要的方程组，我们将其写做矩阵形式：

$$\boldsymbol{C}\times\boldsymbol{\gamma}=\boldsymbol{W}$$

其中$\boldsymbol{C},\boldsymbol{\gamma}$和$\boldsymbol{W}$定义为：

$$\boldsymbol{C}=\begin{bmatrix}C^0_{n-k}&C^1_{n-k}&C^2_{n-k}&\cdots&C^{n-k}_{n-k}&0&0&\cdots&0&0\\0&C^0_{n-k}&C^1_{n-k}&\cdots&C^{n-k-1}_{n-k}&C^{n-k}_{n-k}&0&\cdots&0&0\\\vdots&\vdots&\vdots&&&&&&\vdots&\vdots\\0&0&0&\cdots&\cdots&\cdots&\cdots&\cdots&C^{n-k}_{n-k}&0\\0&0&0&\cdots&\cdots&\cdots&\cdots&\cdots&C^{n-k-1}_{n-k}&C^{n-k}_{n-k}\end{bmatrix}$$

$$\boldsymbol{\gamma}=(\gamma_0\ \ \gamma_1\ \ \gamma_2\ \ \cdots\ \gamma_{n-2}\ \ \gamma_{n-1}\ \ \gamma_n\ \ )^T$$

$$\boldsymbol{W}=((-1)^0,(-1)^1,(-1)^2,(-1)^3,\cdots,(-1)^k)^T$$

当未知数数目大于方程数目时，方程组的解不唯一．然而，方程组(3)的任何解都可以用于构造一个$(k,n)$方案．注意到将一个$(k,n)$方案的$S^0_{n\times m}$和$S^1_{n\times m}$中的相同列删去将不影响$S^0_{n\times m}$和$S^1_{n\times m}$的有效性，并且象素的膨胀度$m$会相应的降低．这更便于视觉系统分辨，正是我们希望得结果．因而，我们假设$\alpha^0_p$和$\alpha^1_p$中仅有一个非零．

我们希望$m$的值尽可能的小．最优的$m$在$\sum_{p=1}^{n}|\gamma_p|$取得最小值时取得，这个最优化是一个整数规划问题．下面我们找方程组(3)的近似最优解．

## 3　近似求解算法

为了找到近似解，我们从$(k+1)\times(n+1)$矩阵$\boldsymbol{C}$中删除中间的$(n-k)$列得到一个$(k+1)\times(k+1)$的矩阵．

为什么要删除中间的列？如果我们将基本矩阵$S^t_{n\times m}$看作一系列$T^t_p(p=0,\cdots,n)$拼接而成的，$S^t_{n\times m}$的列数可以通过各个$T^t_p$的列数相加得到，即$m=\sum_{p=0}^{n}\alpha^t_p C^p_n$．为了减小$m$，最好除去那些$C^p_n$比较大的项．$C^p_n$在$p\leqslant\lceil n/2\rceil$时随$p$增大而增大，$p\geqslant\lceil n/2\rceil$时随$p$增大而减小．因此，矩阵$\boldsymbol{C}$中间的列含有相对较大的$C^p_n$．现在，我们得到了一个简化过的方程组：

$$\boldsymbol{C}_2\times\boldsymbol{\gamma}=\boldsymbol{W}_2$$

其中$\boldsymbol{C}_2,\boldsymbol{\gamma}_2$和$\boldsymbol{W}_2$定义如下：

$$\boldsymbol{C}_2=\begin{bmatrix}1&C^1_{n-k}&\cdots&C^{\lfloor k/2\rfloor-1}_{n-k}&C^{\lfloor k/2\rfloor}_{n-k}&0&0&\cdots&0&0\\0&1&\cdots&C^{\lfloor k/2\rfloor-2}_{n-k}&C^{\lfloor k/2\rfloor-1}_{n-k}&0&0&\cdots&0&0\\\cdots&&&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&1&C^1_{n-k}&0&0&\cdots&0&0\\0&0&\cdots&0&1&0&0&\cdots&0&0\\0&0&\cdots&0&0&1&0&\cdots&0&0\\0&0&\cdots&0&0&C^1_{n-k}&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&0&0&C^{k-\lfloor k/2\rfloor-1}_{n-k}&C^{k-\lfloor k/2\rfloor-2}_{n-k}&\cdots&C^1_{n-k}&1\end{bmatrix}$$

$$\boldsymbol{\gamma}_2=(\gamma_0\ \ \gamma_1\ \ \cdots\ \gamma_{\lfloor k/2\rfloor-1}\ \gamma_{\lfloor k/2\rfloor}\ \gamma_{n-k+\lfloor k/2\rfloor+1}\ \gamma_{n-k+\lfloor k/2\rfloor+2}\ \cdots\ \gamma_n)^T$$

$$\boldsymbol{W}_2=((-1)^0(-1)^1\cdots(-1)^k)^T$$

矩阵 $\boldsymbol{C}_2$ 有 $\begin{bmatrix}A & 0\\ 0 & B\end{bmatrix}$ 的形式，其逆矩阵是 $\begin{bmatrix}A^{-1} & 0\\ 0 & B^{-1}\end{bmatrix}$. 为了求它的逆矩阵，从下面的矩阵(对任意 $s\geqslant r>0$)入手：

$$\begin{bmatrix}1 & C_s^1 & C_s^2 & \cdots & & C_s^{r-1}\\ 0 & 1 & C_s^1 & \cdots & & C_s^{r-2}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & 1 & C_s^1\\ 0 & 0 & 0 & \cdots & 0 & 1\end{bmatrix}$$

该矩阵是一个上三角阵，而上三角部分也有一定规律，其逆矩阵也应该是上三角阵. 我们从对角线开始试算其逆矩阵的元素，发觉它的元素为 $(-1)^qC_{s+q-1}^q$，其中 $q$ 是元素所在位置离对角线的距离. 下面证明该设想：

**命题 5** 对任意给定的 $p>0$，

有 $$\sum_{q=0}^{p}(-1)^qC_s^{p-q}C_{s+(q-1)}^q=0$$ 成立.

证明 将 $(1-x)^s$ 展开，得：

$$(1-x)^s=1-C_s^1x+C_s^2x^2+\cdots+(-1)^{s-1}C_s^{s-1}x^{s-1}+(-1)^sx^s$$

1 将 $(1-x)^{-s}$ 展开得到：

$$(1-x)^{-s}=1+C_s^1x+C_{s+1}^2x^2+C_{s+2}^3x^3+\cdots+C_{s+(q-1)}^qx^q+\cdots$$

那么 $(1-x)^s\cdot(1-x)^{-s}$ 的 $p$ 次项系数为：

$$\sum_{q=0}^{p}(-1)^{p-q}C_s^{p-q}C_{s+(q-1)}^q$$

$p>0$ 时 $(1-x)^s\cdot(1-x)^{-s}$ 的 $p$ 次项系数显然为 0，那么

$$\begin{aligned}&\sum_{q=0}^{p}(-1)^qC_s^{p-q}C_{s+(q-1)}^q\\&=\sum_{q=0}^{p}(-1)^{-q}C_s^{p-q}C_{s+(q-1)}^q\\&=(-1)^p\sum_{q=0}^{p}(-1)^{p-q}C_s^{p-q}C_{s+(q-1)}^q=0\end{aligned}$$

证毕.

通过命题 5 容易得到：

$$\begin{bmatrix}1 & C_s^1 & C_s^2 & \cdots & C_s^{r-1} & C_s^r\\ 0 & 1 & C_s^1 & \cdots & C_s^{r-2} & C_s^{r-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & 1 & C_s^1\\ 0 & 0 & 0 & \cdots & 0 & 1\end{bmatrix}\begin{bmatrix}1 & (-1)C_s^1 & (-1)^2C_{s+1}^2 & \cdots & (-1)^{r-1}C_{(s-1)+(r-1)}^{r-1} & (-1)^rC_{(s-1)+r}^r\\ 0 & 1 & (-1)C_s^1 & \cdots & (-1)^{r-2}C_{(s-1)+(r-2)}^{r-2} & (-1)^{r-1}C_{(s-1)+r-1}^{r-1}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & 1 & (-1)C_s^1\\ 0 & 0 & 0 & \cdots & 0 & 1\end{bmatrix}=\boldsymbol{I}$$

这个结论有助于找方程组(3)的解. 经过这些工作，我们得到了方程组(3)的一组近似最优解：

对 $0\leqslant p\leqslant\lfloor k/2\rfloor$：

$$\begin{aligned}\gamma_p&=(-1)^p(1+C_{n-k}^1+C_{n-k+1}^2+\cdots+C_{n-k+\lfloor k/2\rfloor-1-p}^{\lfloor k/2\rfloor-p})\\&=(-1)^pC_{n-k+\lfloor k/2\rfloor-p}^{\lfloor k/2\rfloor-p}\end{aligned}$$

对 $(n-k)+\lfloor k/2\rfloor+1\leqslant p\leqslant n$

$$\begin{aligned}\gamma_p&=(-1)^p(1+C_{n-k}^1+C_{n-k+1}^2+\cdots\\&\quad+C_{(n-k)-1+(p-(n-k)-\lfloor k/2\rfloor-1)}^{p-(n-k)-\lfloor k/2\rfloor-1})\\&=(-1)^pC_{p-\lfloor k/2\rfloor-1}^{p-(n-k)-\lfloor k/2\rfloor-1}\end{aligned}$$

在本节的最后，给出近似解的算法：

**算法 6 (构造方案基本矩阵)**

(1) $P\leftarrow0$；将 $\boldsymbol{S}_{n\times m}^0$ 和 $\boldsymbol{S}_{n\times m}^1$ 置空.

(2) 如果 $p$ 是偶数，$\alpha_p^0\leftarrow C_{n-k+\lfloor k/2\rfloor-p}^{\lfloor k/2\rfloor-p}$，$\alpha_p^1\leftarrow0$；否则，$\alpha_p^0\leftarrow0$；$\alpha_p^1\leftarrow C_{n-k+\lfloor k/2\rfloor+p}^{\lfloor k/2\rfloor-p}$；$p\leftarrow p+1$；如果 $p\leqslant\lfloor k/2\rfloor$，重复(2).

(3) $\alpha_p^0\leftarrow0$，$\alpha_p^1\leftarrow0$；$p\leftarrow p+1$；如果 $p\leqslant(n-k)+\lfloor k/2\rfloor$，重复(3).

(4) 如果 $p-n+k$ 是偶数，$\alpha_p^0\leftarrow C_{p-\lfloor k/2\rfloor-1}^{p-(n-k)-\lfloor k/2\rfloor-1}$，$\alpha_p^1\leftarrow0$；否则 $\alpha_p^1\leftarrow0$，$\alpha_p^1\leftarrow C_{p-\lfloor k/2\rfloor-1}^{p-(n-k)-\lfloor k/2\rfloor-1}$；$p\leftarrow p+1$；如果 $p\leqslant n$，重复(4).

(5) $p\leftarrow0$.

(6) 将所有含有 $p$ 个 1 的列 $\alpha_p^0$ 次并入 $S_{n\times m}^0$，$\alpha_p^1$ 次并入 $S_{n\times m}^1$；$p\leftarrow p+1$；如果 $p\leqslant n$，重复 6.

## 4 结论

本文提出一种实现文献[4]定义的可视分存的方案的新方法. 与以往方法不同的是，我们通过分析该定义，以方程的形式描述可视分存的模型，最后以解析形式给出了问题的一个近似最优解. 该方案的结果与文[5]的方案一致，但因为处理方式的不同，我们的算法相当于其算法的前两步，而省去了其算法中用以尝试和平衡的第三步循环比较过程(最坏情况下该循环的时间复杂度为 $O(k^2)$)，代之以理论分析得到的解析解直接进行赋值，实现效率明显提高. 同时，我们的分析可以视为对文[5]所提算法的一个更深入的分析，揭示了其算法背后的数学机理. 我们将 $(k,n)$ 分存和 $(n,n)$ 分存纳到一起，形成一个有机的整体，体系更和谐统一.

## 5 附录

本部分用本文的算法得到一个(2,3)可视分存方案的例子，以帮助读者理解可视秘密分存的思想. 容易得到，(2,3)方案的基本矩阵为：

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

膨胀度 $m$ 为 3. 为了便于构图，我们拟用 $2\times2$ 的子象素块表示秘密图像里的一个象素，那么，我们在基本矩阵 $\boldsymbol{S}^0$ 和

$S^1$ 上分别加上一个全'1'的列,这不影响秘密的恢复. 这样,采用的基本矩阵为:

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

原始秘密图像

图2　原始秘密图像

这样,分存和叠加后的效果如图3所示:

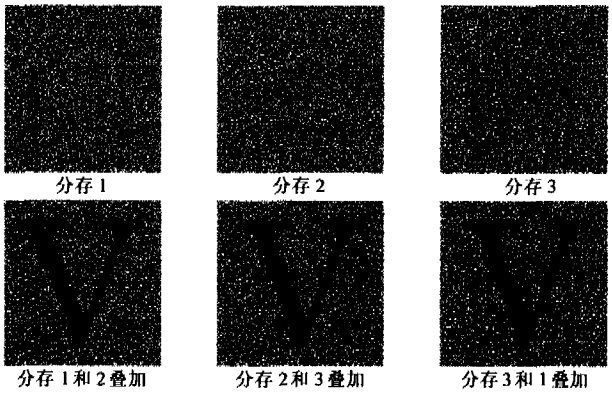



图3　一个(2,3)可视分存方案

**参考文献:**


[1] Blakley G R. Safeguarding cryptographic keys[A]. Proceedings of National Computer Conference [C]. Montvale, NJ: AFIPS Press, 1979, 48. 313 -317.

[2] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612 -613.

[3] Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure [A]. Proceedings IEEE Globecom'87[C]. Tokyo, Japan: IEEE, 1987. 99 -102.

[4] Naor M, Shamir A. Visual cryptography[A]. Advances in Cryptology-Eurocrypt'94, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1995, 950, 1 -12.

[5] Droste S. New result on visual cryptography[A]. Advances in Cryptology-CRYPTO'96, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1996. 1109: 401 -415.

[6] Zheng H. Linear threshold schemes, visual cryptography, and parasite-host cryptosystems[D]. Texas, USA: Texas A&M university, 1998.

[7] Krause M, Simon H. Determining the optimal contrast for secret sharing schemes in visual cryptography[J]. Combinatorics Probability and computing, 2003, 12 (3): 285 -299.

[8] Blundo C, D'Arco P, et al. Contrast optimal threshold visual cryptography schemes[J]. SIAM Journal on Discrete Mathematics, 2003, 16(2): 224 -261.

[9] Blundo C, De Santis A. Visual cryptography schemes with perfect reconstruction of black pixels[J]. Computers & Graphics, 1998, 22(4): 449 -455.

[10] Eisen P A, Stinson D R, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels[J]. Designs, Codes and Cryptography, 2002, 25 (1): 15 -61.

[11] Cimato S, De Santis A, et al. Ideal contrast visual cryptography schemes with reversing[J]. Information Processing Letters, 2005, 93(4): 199 -206.

[12] Yang C N, Laih C S. New colored visual secret sharing schemes[J]. Designs, Codes, and Cryptography, 2000, 20(3): 325 -335.

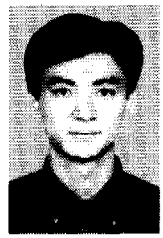
[13] Chang C C, Tsai C S, et al. A new scheme for sharing secret color images in computer network[A]. Proceedings of Seventh International Conference on Parallel and Distributed Systems[C]. Iwate, Japan: IEEE, 2000. 21 -27.

[14] Lukac R, Plataniotis KN. Color image secret sharing [J]. Electronics Letters, 2004, 40(9): 529 -531.

[15] Hou Y C, Chen P M. An asymmetric watermarking scheme based on visual cryptography[A]. Proceedings of 5th International Conference on Signal Processing (WCCC-ICSP 2000)[C]. Beijing, China: IEEE, 2000, 2: 992 -995.

[16] Chang C C, Wu H C. A copyright protection scheme of images based on visual cryptography[J]. Imaging SCI J, 2001, 49(3): 141 -150.


**作者简介:**



**黄东平**　男,1977年生于四川巴中,清华大学计算机科学与技术系博士研究生,主要研究领域为信息安全,算法设计与分析.

**王道顺**　男,1964年生于四川苍溪,博士,清华大学计算机科学与技术系副教授,研究兴趣为图像加密,数字水印和密码算法.
E-mail: daoshun@mail.tsinghua.edu.cn