基于累积矩阵的可防欺骗视觉密码方案

郁 滨 徐晓辉 房礼国
(信息工程大学电子技术学院 郑州 450004)

摘 要：该文基于累积矩阵提出一种可防止欺骗的视觉密码方案，在不泄露秘密信息的前提下，不需要其他额外信息，可发现多个独立欺骗者的存在，及时阻止欺骗行为。与以往方案相比，该方案构造更为简单，能发现更多的欺骗者。

关键词：视觉密码；累积矩阵；共享份；欺骗者
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)04-0950-04

A Cheater Detectable VCS Based on Cumulative Array

Yu Bin Xu Xiao-hui Fang Li-guo
(*Institute of Electronic Technology*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: A cheater detectable Visual Cryptography Scheme(VCS) based on cumulative array which can find the cheater without extra information and does not show any information of the secret image is introduced in this paper. Compared to previous schemes, it is more convenient and can find more cheaters.

Key words: Visual cryptography; Cumulative Array (CA); Share; Cheater

1 引言

在保密通信中，为了实现信息的安全保密，常采用加密的手段来保护信息，而加密的核心是密钥的保护问题，密钥的管理直接影响着通信系统的安全，如何有效地管理和保护密钥就成为密码学中十分重要的课题。

Shamir[1]和 Blakley[2]分别于 1979 年独立地提出秘密共享的概念，并分别设计了具体的体制，来解决上述问题。所谓秘密共享体制就是将秘密 s 提供给参与者集合 p 中的所有成员分开保管，当且仅当集合 p 的授权子集中的所有成员出示他们的秘密份额时才能恢复出秘密 s ，而任何非授权子集得不到关于秘密 s 的任何信息。

Shamir 和 Naor 等人[3]于 1994 年的欧洲密码学会议上，提出了一种称为视觉密码(visual cryptography)的秘密分享新技术，主要思想是把秘密图像分享在若干称为共享份的分享图片中，每一张分享图片上都是随机分布的黑点和白点，不会泄露秘密的任何信息。这些图片可以存储在磁盘上或者印刷到透明胶片上。解密时，只需要将满足条件的胶片叠加在一起，不需要借助其他设备和复杂的密码运算，可以由人类视觉系统直接恢复出秘密。

视觉密码的安全强度相当于“一次一密”[3]，但是它跟普通秘密共享方案一样，也存在着欺骗问题。视觉密码的欺骗存在着两种方式：外部欺骗是指授权子集外的人伪装成参与者去骗取共享份，如果骗得的共享份可以组成一个授权子集的话，即可恢复出秘密信息；内部欺骗是指授权子集中的参与者不出示自己真正的共享份，破坏秘密信息的恢复或者骗取其他参与者的共享份。由于欺骗者错误共享份的存在，将使得秘密信息不能正确地恢复，且其他参与者无法知道谁是欺骗者。因此视觉密码方案在实际使用时，一方面必须防止外部欺骗，即防止敌手获得秘密；另一方面要防止内部欺骗，即防止参与者出示伪造的共享份破坏秘密恢复或者骗取其他参与者的共享份。

为了防止欺骗现象的发生，颜浩等人[4,5]通过将原始的 (k,n) 和 $(k-1,n)$ 视觉密码方案结合，构造出一种 (k,n) 可防欺骗视觉密码方案，在 k 个参与者中存在一个欺骗者时，可以通过能否恢复出验证图像检测出欺骗者。但是该方案在恢复的秘密图像中，仍然存在着验证图像的重影，影响对秘密图像的辨别。郁滨等人[6]通过原始 (k,n) 和改进的 $(k-1,k-1)$ 视觉密码方案，构造出一种更为简单，消除了验证图像的重影，可以清晰地恢复秘密信息的可防欺骗方案。文献[7]给出了该方案的进一步改进，在保证防欺骗功能的基础上，实现了多秘密共享。这几种防欺骗方案都使用与秘密图像 S 大小相同的图像 I 来做验证图像，I 不包含任何 S 的信息。$k-1$ 个参与者可以恢复 I ，k 个或 k 个以上参与者可以恢复 S 。因为欺骗者的共享份不能恢复出秘密图像 S ，同样也不能恢复出验证图像 I ，通过能否恢复出验证图像发现 k 个参与者中的一个欺骗者。但是当有多个欺骗者存在时，上述方案便无能为力了。

本文通过累积矩阵的视觉密码方案[8]，提出了一种可防多个独立欺骗者的视觉密码方案，能够发现多个欺骗者。当两个正确共享份能够恢复出验证图像时，可以发现最多的欺

2007-12-28 收到，2008-05-11 改回

骗者，这时在确认一个共享份的真实性的前提下，最多可以发现 k 个参与者中的 $k-1$ 个欺骗者。通过该方案，可以及时发现并阻止欺骗行为，保证了诚实参与者的利益。

2　累积矩阵的视觉密码方案

假设一组参与者 $p=(1,2,\cdots,n)$，　$(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}})$ 为该视觉密码方案的存取结构 Γ 。Γ_0 为 Γ 的最小授权子集集合(collection of minimal qualified sets)，定义为

$$\Gamma_0=\{A\in\Gamma_{\text{Qual}}:A'\notin\Gamma_{\text{Qual}}\text{ for all }A'\subset A\}$$

Z_M 为 Γ 的最大禁止子集集合(collection of maximal forbidden sets)，定义为

$$Z_M=\{B\in\Gamma_{\text{Forb}}:B\cup\{i\}\in\Gamma_{\text{Qual}}\text{ for all }i\in p\setminus B\}$$

Γ_{Qual} 的累积映射 (β,T) 为与有限集 T 对应的映射关系 β：$p\to 2^T$ 满足对所有 $Q\subseteq p$，有

$$\bigcup_{a\in Q}\beta(a)=T\Leftrightarrow Q\in\Gamma_{\text{Qual}}$$

通过最大禁止子集集合 $Z_M=\{F_1,\cdots,F_t\}$ 构造累积映射如下：

令 $T=\{T_1,\cdots,T_t\}$，$i\in p$ 有：

$$\beta(i)=\{T_j\mid i\notin F_j,1\le j\le t\}$$

从上面的映射关系可以看出，对于任一 $X\in\Gamma_{\text{Qual}}$，有 $\bigcup_{i\in X}\beta(i)=T$，而对于任一 $X\in\Gamma_{\text{Forb}}$，因为有 $X\subseteq F_j$，将至少缺少一个 $T_j\in T$。构造累积矩阵 **CA** 为一 $|p|\times|T|$ 布尔矩阵，当且仅当 $i\notin F_j$ 时，$\mathbf{CA}(i,j)=1$。

通过上述映射关系，构造视觉密码方案。Z_M 为最大禁止子集集合，$t=|Z_M|$，**CA** 为通过上述映射得到的累积矩阵。$\widehat{\boldsymbol{S}}^0$ 和 $\widehat{\boldsymbol{S}}^1$ 为根据文献[3,8]构造的 (t,t)-VCS 基础矩阵，$\widehat{\boldsymbol{S}}^0$ 的列为所有汉明重量为偶数的 t 维向量；$\widehat{\boldsymbol{S}}^1$ 的列为所有汉明重量为奇数的 t 维向量，扩展度为 $\widehat{m}=2^{t-1}$，相对差 $\alpha=1/2^{t-1}$。那么对应于存取结构 $(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}})$ 的基础矩阵构造如下：

对于 **CA** 的第 i 行，其中 $j_{i,1},\cdots,j_{i,gi}$ 为满足累积矩阵中 $\mathbf{CA}(i,j)=1$ 的整数 j，则基础矩阵 $\boldsymbol{S}^0$（$\boldsymbol{S}^1$）的第 i 行由 $\widehat{\boldsymbol{S}}^0$（$\widehat{\boldsymbol{S}}^1$）的 $j_{i,1},\cdots,j_{i,gi}$ 行相或得到。对于 $\boldsymbol{S}^0$ 和 $\boldsymbol{S}^1$ 中相同的列，可以删去，而不影响其性质[9]。

定理 1　$(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}})$ 为一强存取结构，$(\Gamma_{\text{Qual}},\Gamma_{\text{Forb}},m)$-VCS 为通过累积矩阵构造的视觉密码方案，基础矩阵为 $\boldsymbol{S}^0$，$\boldsymbol{S}^1$ 对于所有的 $Q\in\Gamma_{\text{Qual}}$，都有 $H(V_{\boldsymbol{S}^1})-H(V_{\boldsymbol{S}^0})=1$。

证明　研究累积矩阵 **CA** 发现，对于授权子集 $Q\in\Gamma_{\text{Qual}}$ 中所有的参与者，他们所对应的行相或之后，所得向量的汉明重量为 t，根据使用的 (t,t)-VCS，其基础矩阵为 $\widehat{\boldsymbol{S}}^0$，$\widehat{\boldsymbol{S}}^1$，$\widehat{m}=2^{t-1}$，可以看出，$H(V_{\widehat{S}^0})=2^{t-1}-1$，$H(V_{\widehat{S}^1})=2^{t-1}$。而对于所有的 $Q\in\Gamma_{\text{Qual}}$，$H(V_{S^0})$，$H(V_{S^1})$ 为 $H(V_{\widehat{S}^0})$，$H(V_{\widehat{S}^1})$ 减去各行相或后所得矩阵中相同的列数，它们汉明重量的差值仍然为 1，所以都有 $H(V_{S^1})-H(V_{S^0})=1$。

累积矩阵的视觉密码方案是基于通用存取结构提出的，同样也适用于门限方案，下面给出累积矩阵的 $(2,4)$-VCS 的构造。

$$\Gamma_0=\{12,13,14,23,24,34\},\quad Z_M=\{1,2,3,4\}$$

根据累积矩阵的构造法则：

$$\mathbf{CA}=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}\tag{1}$$

$t=|Z_M|=4$，则 $(4,4)$-VCS 的基础矩阵 $\widehat{\boldsymbol{S}}^0$，$\widehat{\boldsymbol{S}}^1$ 分别为

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

$$\widehat{\boldsymbol{S}}^1=\begin{bmatrix}1&0&0&0&1&1&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{bmatrix}\tag{2}$$

由上面的构造方案，根据累积矩阵 **CA** 各行中为 1 的位，将 $\widehat{\boldsymbol{S}}^0$，$\widehat{\boldsymbol{S}}^1$ 中对应的行相或，得到该 $(2,4)$-VCS 的基础矩阵：

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

$$\boldsymbol{S}^1=\begin{bmatrix}0&1&1&1&1&1&1&1\\1&0&1&1&1&1&1&1\\1&1&0&1&1&1&1&1\\1&1&1&0&1&1&1&1\end{bmatrix}\tag{3}$$

比较两个矩阵，其中都有 4 列全为 1，删去相同的列后，得到 $(2,4)$-VCS 的基础矩阵为

$$\boldsymbol{S}^0=\begin{bmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{bmatrix},\quad\boldsymbol{S}^1=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}\tag{4}$$

3　基于累积矩阵的可防欺骗视觉密码方案

$(k,\ n)$可防欺骗的视觉密码方案由 $\boldsymbol{S}_0^0$，$\boldsymbol{S}_0^1$，$\boldsymbol{S}_1^0$，$\boldsymbol{S}_1^1$ 4 个基础矩阵组成，其中基础矩阵的下标表示所分享的秘密图像 S 像素的颜色，上标表示验证图像 I 像素的颜色，0 表示白色，1 表示黑色。用来分享秘密图像和验证图像，分享规则如表 1 所示。

(k,n) 可防欺骗视觉密码方案的基础矩阵由两部分组成，为分享秘密图像的 $\boldsymbol{S}_0$（$\boldsymbol{S}_1$）和分享验证图像的 $\overline{\boldsymbol{S}}^0$（$\overline{\boldsymbol{S}}^1$）。其中 $\boldsymbol{S}_0$（$\boldsymbol{S}_1$）为普通 (k,n) 视觉密码方案的基础矩阵，$\overline{\boldsymbol{S}}^0$（$\overline{\boldsymbol{S}}^1$）为通过累积矩阵构造的特殊矩阵。

表 1 可防欺骗视觉密码方案分享规则

矩阵	秘密图像	验证图像
$\boldsymbol{S}_0^0$	白	白
$\boldsymbol{S}_0^1$	白	黑
$\boldsymbol{S}_1^0$	黑	白
$\boldsymbol{S}_1^1$	黑	黑

根据定理 1，由累积矩阵视觉密码方案的性质，构造 $\overline{\boldsymbol{S}}^0$ ($\overline{\boldsymbol{S}}^1$)如下：

$$\overline{\boldsymbol{S}}^0 = \boldsymbol{S}^0 \circ \boldsymbol{S}^{1'},\ \ \overline{\boldsymbol{S}}^1 = \boldsymbol{S}^1 \circ \boldsymbol{S}^{0'}$$

其中 $\circ$ 表示矩阵的连接， $\boldsymbol{S}^0$ ($\boldsymbol{S}^1$)和 $\boldsymbol{S}^{0'}$ ($\boldsymbol{S}^{1'}$)分别表示基于累积矩阵构造的 (h,n) 和 (k',n) 门限视觉密码方案的基础矩阵($2 \le h < k' \le k$)。根据视觉密码基础矩阵的性质和定理 1， $\overline{\boldsymbol{S}}^0$ ， $\overline{\boldsymbol{S}}^1$ 有如下性质， q 表示取的矩阵中的行数：

(1)当 $q < h$ 时： $H(V_{S^0}) = H(V_{S^1})$ ， $H(V_{S^{0'}}) = H(V_{S^{1'}})$ ，所以有 $H(V_{\overline{S}^0}) = H(V_{\overline{S}^1})$ ；

(2) 当 $h \le q < k'$ 时： $H(V_{S^1}) - H(V_{S^0}) = 1$ ， $H(V_{S^{0'}}) = H(V_{S^{1'}})$ ，所以有 $H(V_{\overline{S}^1}) - H(V_{\overline{S}^0}) = 1$ ；

(3) 当 $k' \le q \le n$ 时， $H(V_{S^1}) - H(V_{S^0}) = 1$ ， $H(V_{S^{1'}}) - H(V_{S^{0'}}) = 1$ ，所以有 $H(V_{\overline{S}^0}) = H(V_{\overline{S}^1})$ 。

为了发现更多的欺骗者，一般取 $h = 2$ ，这样在确定一个共享份真实性的情况下，可以最多发现 $k-1$ 个欺骗者； k' 的取值是任意的，但一般情况根据实际需要选取能使 (k',n) 扩展度达到最小的值，这样使得分享图片较小，或取 $k' = k$ ，那么在拥有 h 个到 $k-1$ 个正确共享份时都可以恢复出验证图像，从而发现欺骗者。

可防欺骗视觉密码方案的 4 个基础矩阵构造如下：

$$\boldsymbol{S}_0^0 = \boldsymbol{S}_0 \circ \overline{\boldsymbol{S}}^0,\ \boldsymbol{S}_0^1 = \boldsymbol{S}_0 \circ \overline{\boldsymbol{S}}^1,\ \boldsymbol{S}_1^0 = \boldsymbol{S}_1 \circ \overline{\boldsymbol{S}}^0,\ \boldsymbol{S}_1^1 = \boldsymbol{S}_1 \circ \overline{\boldsymbol{S}}^1$$

满足可防欺骗视觉密码方案的条件：

(1) 当 $q < h$ 时： $\boldsymbol{S}_0$ ($\boldsymbol{S}_1$)未达到门限值， $H(V_{S_0}) = H(V_{S_1})$ ，对于 $\overline{\boldsymbol{S}}^0$ ($\overline{\boldsymbol{S}}^1$)，也有 $H(V_{\overline{S}^0}) = H(V_{\overline{S}^1})$ ，所以 $H(V_{S_0^0}) = H(V_{S_0^1}) = H(V_{S_1^0}) = H(V_{S_1^1})$ ，对应行相或的汉明重量相等，黑白像素在视觉表现上相同，不会显示任何图像信息；

(2)当 $h \le q < k'$ 时： $\boldsymbol{S}_0$ ($\boldsymbol{S}_1$)未达到门限值， $H(V_{S_0}) = H(V_{S_1})$ ，而对于 $\overline{\boldsymbol{S}}^0$ ($\overline{\boldsymbol{S}}^1$)，有 $H(V_{\overline{S}^1}) - H(V_{\overline{S}^0}) = 1$ ，所以 $H(V_{S_0^0}) = H(V_{S_1^0}) = H(V_{S_0^1}) - 1 = H(V_{S_1^1}) - 1$ ，验证图像黑白像素存在对比度差异，而秘密图像黑白像素表现仍然相同，不显示秘密图像任何信息，只显示出验证图像；

(3)当 $k' \le q < k$ 时： $\boldsymbol{S}_0$ ($\boldsymbol{S}_1$)未达到门限值， $H(V_{S_0}) = H(V_{S_1})$ ，此时 $\overline{\boldsymbol{S}}^0$ ($\overline{\boldsymbol{S}}^1$)，有 $H(V_{\overline{S}^0}) = H(V_{\overline{S}^1})$ ，所以又有 $H(V_{S_0^0}) = H(V_{S_0^1}) = H(V_{S_1^0}) = H(V_{S_1^1})$ ，此时验证图像信息被掩盖，不会显示，而秘密图像的黑白像素表现仍然相同，不显示秘密图像信息；

(4) 当 $k \le q \le n$ 时： $\boldsymbol{S}_0$ ($\boldsymbol{S}_1$)达到门限值， $H(V_{S_0}) < H(V_{S_1})$ ，此时 $\overline{\boldsymbol{S}}^0$ ($\overline{\boldsymbol{S}}^1$)，仍有 $H(V_{\overline{S}^0}) = H(V_{\overline{S}^1})$ ，所以 $H(V_{S_0^0}) = H(V_{S_0^1}) < H(V_{S_1^0}) = H(V_{S_1^1})$ ，秘密图像黑白像素存在对比度差异，而验证图像差异被掩盖，验证图像不显示，只显示秘密图像。

这 4 个基础矩阵都是由普通视觉密码方案矩阵连接而成，满足视觉密码的安全性条件和对比性条件，同时满足可防欺骗视觉密码方案的定义。当有欺骗者存在时，可以通过能否恢复验证图像，找出欺骗者，使其欺骗行为不能得逞。

4 实验与分析

用本文方案构造 (4,4) 可防欺骗视觉密码方案，通过将 (4,4) , (2,4) , (4,4) 方案的基础矩阵相连接，其中 (2,4) 方案的基础矩阵为式(4)所表示矩阵，两个 (4,4) 方案的基础矩阵为式(2)所表示矩阵。连接之后，可以删去 4 个矩阵中相同的列，这不影响原来矩阵的安全性和对比性，且像素扩展度减小，得到如下该方案的 4 个基础矩阵：

$$\boldsymbol{S}_0^0 = \begin{bmatrix} 1&1&1&0&0&0&0&1&1&1&1&0&0&0 \\ 1&0&0&1&1&0&0&1&1&1&0&1&0&0 \\ 0&1&0&1&0&1&0&1&1&1&0&0&1&0 \\ 0&0&1&0&1&1&0&1&1&1&0&0&0&1 \end{bmatrix}$$

$$\boldsymbol{S}_0^1 = \begin{bmatrix} 0&1&1&1&0&0&0&1&1&1&1&0&0&0 \\ 0&1&0&0&1&1&0&1&1&0&0&1&1&0 \\ 0&0&1&0&1&0&1&1&0&1&0&1&0&1 \\ 0&0&0&1&0&1&1&1&0&0&1&0&1&1 \end{bmatrix}$$

$$\boldsymbol{S}_1^0 = \begin{bmatrix} 1&0&0&0&1&1&1&0&0&0&1&1&1&0 \\ 0&1&0&0&1&1&0&1&0&0&1&1&0&1 \\ 0&0&1&0&1&1&0&0&1&0&1&0&1&1 \\ 0&0&0&1&1&1&0&0&0&1&0&1&1&1 \end{bmatrix}$$

$$\boldsymbol{S}_1^1 = \begin{bmatrix} 1&0&0&0&0&1&1&1&1&1&1&0&0&0 \\ 0&1&0&0&1&0&1&1&1&0&0&1&1&0 \\ 0&0&1&0&1&1&0&1&0&1&0&1&0&1 \\ 0&0&0&1&1&1&1&0&0&0&1&0&1&1 \end{bmatrix}$$

因为该方案像素扩展度为 14，外形比例失真比较严重，在仿真时对每个基础矩阵增加两个全为 1 的列，像素扩展度为 16，解决外形比例失真的问题[10]。效果如图 1，图 2 所示：

表 2 给出了本文方案与其他两种可防欺骗方案的比较。从效果来看，本文方案的共享份图片较小，便于存储和传输；恢复出来的图像更为清晰，对比也更加明显，秘密信息容易辨认。另外，其他两个方案只有 3 张正确的共享份才可以恢复出验证图像，只能找出 4 个参与者中的一个欺骗者；而本文方案只需两张正确的共享份就可以恢复出验证图像，从而能够找出两个以上欺骗者，这也是本方案与其他方案相比具有的最明显的优势。

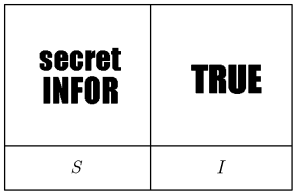


图 1 秘密图像和验证图像

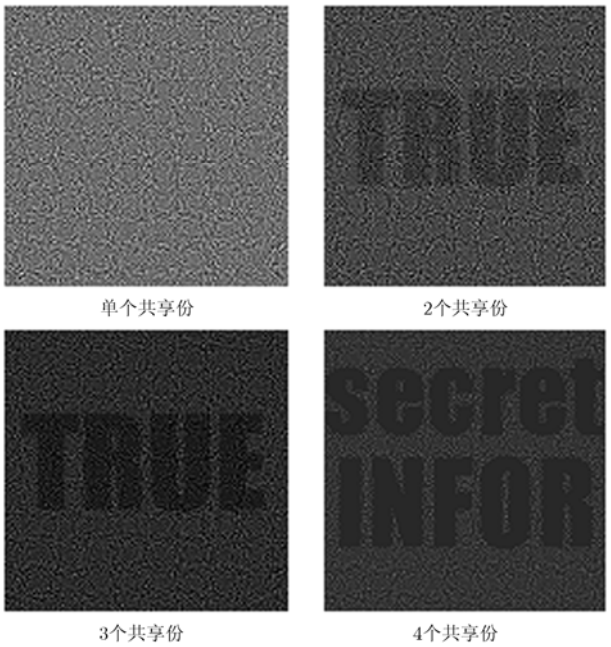
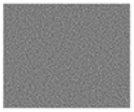
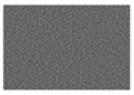


图 2 本文方案的仿真效果

表 2 3 种可防欺骗视觉密码方案比较

	共享份	恢复验证图像	恢复秘密图像	m	α
本文方案				16	1/16
文献[4]方案				30	1/30
文献[6]方案				24	1/24

5　结束语

本文提出基于累积矩阵的可防欺骗视觉密码方案，通过参与者所拥有的共享份，无需额外信息，可以发现其中的多个独立欺骗者。与其他可防欺骗方案相比，该方案构造简单，只需将通过累积矩阵生成的矩阵按照规则相连接，就可得到满足条件的基础矩阵。且该方案的像素扩展度相对较小，信息率较高。最突出的是，该方案可以发现多个欺骗者，加强了防欺骗功能。但是，这些防欺骗方案都是在确定一些共享份真实性的基础上实现的，因此如何构造一种可验证的视觉密码方案，对每一个共享份的正确性和真实性都能够进行验证，是今后进一步研究的方向。

参 考 文 献

[1] Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(11): 612–613.

[2] Blakley G R. Safeguarding cryptographic keys [C]. *Proceedings of the National Computer Conference*, 1979, 48: 242–268.

[3] Naor M and Shamir A. Visual cryptography. Advances in Cryptology-Eurocrypt'94, Lecture Notes in Computer Science, 1995, Vol.950: 1–12.

[4] 颜浩, 甘志, 陈克非.可防欺骗的可视密码分享方案[J]. 上海交通大学学报, 2004, 38(1): 107–110.
Yan Hao, Gan Zhi, and Chen Ke-fei. A cheater detectable visual cryptography scheme [J]. *Journal of Shanghai Jiaotong University*, 2004, 38(1): 107–110.

[5] 郭洁, 颜浩, 刘妍, 陈克非. 一种可防止欺骗的可视密码分享方案[J]. 计算机工程, 2005, 31(6): 126–128.
Guo Jie, Yan Hao, Liu Yan, and Chen Ke-fei. A cheater detectable visual cryptography scheme [J]. *Computer Engineering*, 2005, 31(6): 126–128.

[6] 徐晓辉, 郁滨. 无重影的可防欺骗视觉密码方案[C]. 计算机技术与应用进展(CACIS.2007)2007: 1335–1339.
Xu Xiao-hui and Yu Bin. A Cheater Detectable VCS without Fringes [C]. Progress of Computer Technology and Application in 2007 (CACIS.2007) 2007: 1335–1339.

[7] Yu Bin, Xu Xiao-hui, and Fang Li-guo. Multi-secret sharing threshold visual cryptography [C]. CIS Workshops 2007, Harbin, 2007: 815–818.

[8] Ateniese G, Blundo C, De Santis A, and Stinson D R. Visual cryptography for general access structures. Information and Computation, 1996, 129: 86–106.

[9] Ateniese G, Blundo C, De Santis A, and Stinson D R. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 2001, 250: 143–161.

[10] 郁滨, 房礼国. 外形比例不失真的可视门限方案的研究[J]. 计算机工程与设计, 2006, 27(11): 1998–1999, 2014.
Yu Bin and Fang Li-guo. Research on aspect ratio invariant visual threshold scheme [J]. *Computer Engineering and Design*, 2006, 27(11): 1998–1999, 2014.

郁　滨:　男，1964年生，教授，博士生导师，主要研究方向为视觉密码、蓝牙技术.

徐晓辉:　男，1981年生，硕士生，研究方向为视觉密码.

房礼国:　男，1981年生，助教，研究方向为信息安全.