密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2020, 7(1): 48–55

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

可变可视密码*

乔明秋, 赵振洲

北京政法职业学院 信息技术系, 北京 102628
通信作者: 乔明秋, E-mail: qiaomingqiu@163.com

摘 要: 传统的可视密码在加密时会产生像素扩张, 结果使分存图像比秘密图像大许多倍, 尤其是应用在灰度和彩色图像上, 其扩张的倍数更是惊人. 传统的可视密码都是单点加密, 本文在 Hou 的 m 点加密的基础上, 提出任意点加密可视密码, 即在加密的时候可以对任意个点进行加密, 我们称之为可变可视密码. 操作的时候, 对秘密图像的 r 个点同时进行加密, 当 $r = m$ 时, 该加密就是像素不扩展可视密码; 当 $r > m$ 时, 该加密得到的就是分存图像缩小的可视密码 (r 的增大会降低解密图像的对比度); 当 $r < m$ 时, 该加密得到的就是分存图像扩大的可视密码. 随着 r 的增大, 分存图像会变小, 同时对比度也会降低. 对 r 个点同时加密的时候, 需要计算 r 个点中黑点的个数 b, 对于有 b 个黑点的加密, 在 r 次加密中, 保证有 b 次使用黑色像素加密矩阵 B_1 加密, $r-b$ 次使用白色像素加密矩阵 B_0 加密. 可变可视密码一方面解决了传统可视密码像素扩张的问题; 一方面它非常灵活, 能使分享图像小于、等于或大于加密图像, 从而能有效减少存储空间, 或在存储空间和图像质量之间找到一个平衡点.

关键词: 可视密码; 秘密共享; 多点加密; 可变可视密码

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000348

中文引用格式: 乔明秋, 赵振洲. 可变可视密码[J]. 密码学报, 2020, 7(1): 48–55. [DOI: 10.13868/j.cnki.jcr.000348]

英文引用格式: QIAO M Q, ZHAO Z Z. Variable visual cryptography[J]. Journal of Cryptologic Research, 2020, 7(1): 48–55. [DOI: 10.13868/j.cnki.jcr.000348]

Variable Visual Cryptography

QIAO Ming-Qiu, ZHAO Zhen-Zhou

IT Department, Beijing College of Politics and Law, Beijing 102628, China
Corresponding author: QIAO Ming-Qiu, E-mail: qiaomingqiu@163.com

Abstract: Conventional visual cryptography needs to expand pixels and enlarge the size of shares. This situation is more serious for gray-level and color images. Conventional visual cryptography is single-pixel encryption. Based on Hou's m-pixel encryption, this study proposes a visual cryptography of any pixel encryption, which is called variable visual cryptography (VVC). When computing the shares, r pixels of the secret image are encrypted all together. If $r = m$, the encryption is the visual cryptography without expanding the pixels; if $r > m$, the encrypted image is smaller than the shared image (the increase of r will reduce the contrast of the decrypted image); if $r < m$, the encrypted image is larger than the shared image. With the increase of r, the image will be smaller and the contrast will

* 基金项目: 北京政法职业学院科研项目 (KY201917)
Foundation: Scientific Research Program of Beijing College of Politics and Law (KY201917)
收稿日期: 2019-01-23 定稿日期: 2019-06-28

be lower. When encrypting r pixels together, it is necessary to compute the number of black pixels b in r pixels. For encrypting b black pixels in r times, we use black pixel encrypting matrix B_1 for r times , and we use white pixel encrypting matrix B_0 for $r-b$ times. By doing that, it solves the pixel expansion problem of conventional visual cryptography, and it is so flexible that the sharing images can be smaller, equal or larger than the original secret image, so it can reduce the storage space effectively, or find a balance between storage and image quality.

Key words: visual cryptography; secret sharing; multi points encode; variable visual cryptography (VVC)

1 可视密码概述

可视密码 [1] 是一种秘密共享方法, 它将一个秘密图像加密成 n 个分存图像, 解密时只需 $k'(k' \geq k)$ 个分存图像叠加, 秘密图像就会呈现, 而少于 k 个分存图像将无法解密, 且不能分析出秘密图像的一点信息, Droste [2] 提出了可视密码新的研究成果. 目前, 已经提出了许多可视密码技术的拓展形式, 如像素不扩展型 [3–7]、基于分块字典的可视密码 [8,9]、基于栅格的可视密码 [10,11]、没有形变的可视密码 [12]、防欺骗可视密码 [13]、基于三维立体分享图像的可视密码 [14]、多级别的可视密码 [15] 等.

传统的可视密码都是单点加密, 在加密时会产生像素扩张, 结果使分享图像比原来的加密图像大许多倍, 尤其是应用在灰度和彩色图像上, 其扩张的倍数更是惊人. Hou 提出了像素不扩展的彩色可视密码 [3], 林克正等提出了基于分块字典的可视密码 [8]. 本文提出任意个点加密的可视密码, 即可变可视密码 (variable visual cryptography, VVC), 一方面它解决了传统可视密码像素扩张的问题; 另一方面它非常灵活, 能使分存图像小于、等于或大于秘密图像, 从而能有效减少存储空间, 或在存储空间和图像质量之间找到一个平衡点, 也许它的优越性远不止于此.

2 传统可视密码的数学定义

秘密图像中的每个像素都单独处理, 即单点加密, 由 n 个人共享, 每个共享由 m 个黑白子像素组成. 构建一个 $n \times m$ 布尔矩阵 $B=[B_{ij}]$, 当且仅当 $B_{ij}=1$ 时第 i 个共享者的第 j 个子像素为黑; 当且仅当 $B_{ij}=0$ 时第 i 个共享者的第 j 个子像素为白. 当把投影片叠放在一起时, 就相当于对于每一行都做了或运算. 叠放后图像的灰度值与进行或运算之后的向量 V 的汉明重量 $H(V)$ 成正比. 解密者利用视觉系统解释灰度值如下, 如果 $H(V) \geq d$ 该点像素为黑, 如果 $H(V) \leq d-\alpha m$ 该点像素为白.

定义 1 一个 (k,n) 可视密码体制含有两个 $n \times m$ 布尔矩阵簇 C_0 和 C_1, 如要共享一个白像素就随机从 C_0 中取出一个矩阵, 如要共享一个黑像素就随机从 C_1 中取出一个矩阵. 所选的矩阵定义了 n 个共享者中每一个子像素的颜色. 如果下列条件满足则该方法有效:

(1) 对于 C_0 中的任意一个矩阵 S, n 行中任意 k 行进行或运算之后的向量 V 满足 $H(V) \leq d-\alpha m$;

(2) 对于 C_1 中的任意一个矩阵 S, n 行中任意 k 行进行或运算之后的向量 V 满足 $H(V) \geq d$;

(3) 对于 $\{1,2,\cdots,n\}$ 中的任意一个子集 $\{i_1,i_2,\cdots,i_q\}$, $q<k$, 将 $C_t\,(t=0,1)$ 中每一个 $n \times m$ 矩阵限制到行 $i_1,i_2,\cdots,i_q$ 上, 得到的两个 $q \times m$ 矩阵簇 $D_t\,(t=0,1)$ 以同样的频率包含同样的矩阵, 因此不可区分.

其中:

(1) m 是像素扩展度, m 越小越好;

(2) α 是相对差, α 越大越好;

(3) $\alpha \cdot m$ 是对比度, $\alpha \cdot m$ 越大越好;

(4) 矩阵簇 C_t 是基础矩阵 B_t 进行随机列置换后所有矩阵的集合.

以 (2,2) 可视密码为例, 加密基础矩阵为式(1), C_0 和 C_1 分别是 B_0 和 B_1 进行随机列置换后所有矩阵的集合, 通过验证, 此基础矩阵满足定义的三个条件.

$$B_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{1}$$

再有 (2,4) 可视密码的基础矩阵为式 (2), 也满足定义的要求.

$$B_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

3 可变可视密码实现算法

我们不采用单点加密, 而是采用 r 点加密, 加密序列长度 r 可变 ($r > 1$), 那么分享图像大小就是秘密图像大小的 m/r 倍. 当 $r > m$ 时是分享图像比秘密图像小的方案; 当 $r = m$ 时是分享图像和秘密图像一样大的方案; 当 $1 < r < m$ 时是分享图像比秘密图像大的方案 (前两种情况更具应用性). 当然, r 不可能过大, 否则图像会难以识别.

对于 (k, n) 可视密码, 令 B_0、B_1 分别代表对应白点与黑点的基础矩阵, 基础矩阵是 $m \times n$ 矩阵, C_0、C_1 分别是对 B_0、B_1 进行随机列置换后的矩阵集, $M_0 \in C_0$, $M_1 \in C_1$. 加密序列长度为 r, 即我们一次取秘密图像上的连续 r 个点来加密, b 代表加密序列中的黑点个数 ($0 \le b \le r$), e_b 则代表具有 b 个黑点的加密序列已加密过的个数, 加密程序如下:

(1) 确定加密序列长度 r, 令 $e_b = 0$ for $b = 1, 2, \cdots, r$;

(2) 从秘密图像取出即将加密的序列, 并计算其黑点个数 b;

(3) if $e_b \bmod r < b$

$M = M_1$

else $M = M_0$

M 代表所取的加密矩阵, 将 M 的第 i 行分配给第 i 个分享者 ($1 \le i \le n$), 每个分享者拥有 m 个像素, 此 m 个像素的排列方法视情况而定, 排列宗旨是使解密图像变形最小;

(4) $e_b = e_b + 1$;

(5) 重复步骤 (2)–(4) 直到秘密图像上的所有像素都加密完毕.

4 可变可视密码证明

同传统的可视密码一样, 我们的方案也需要从对比性和安全性两个方面进行证明.

对比性: 对于本方案的 (k, n) 可视密码, 若 $k'(k' \ge k)$ 个人的分享图像叠加后, 具有 b 个黑点的加密序列和具有 $b + 1$ 个黑点的加密序列在叠加图像上是可区分的.

证明: B_0、B_1 是 (k, n) 可视密码的基础矩阵, 基础矩阵是 $m \times n$ 矩阵, C_0、C_1 分别是对 B_0、B_1 进行随机列置换后的矩阵集, $M_0 \in C_0$, $M_1 \in C_1$. $\mathrm{OR}(M, k')$ 代表将矩阵 M 的第 $i_1, i_2, \cdots, i_{k'}$ 列进行或运算所得到的向量. $E^{(b)}$ 代表秘密图像上具有 b 个黑点的加密序列, r 代表加密序列长度.

在 r 个 $E^{(b)}$ 加密序列中, 有 b 个使用 $M \in C_1$ 加密, 其余的 $r - b$ 个序列使用 $M \in C_0$ 加密, 因此在将 k 个分享图像叠加后的图像上, 在对应这 r 个区域上会有 $[b \times h_1 + (r - b) \times h_0]$ 个黑点, 其中 $h_1 = H(\mathrm{OR}(M \in C_1, k')), h_0 = H(\mathrm{OR}(M \in C_0, k'))$, H 表示取汉明重量, 因此这 r 个 $E^{(b)}$ 加密序列在叠加图像上的黑色程度可以表示成 $[b \times h_1 + (r - b) \times h_0]/(r \times m)$, 那么 r 个 $E^{(b+1)}$ 加密序列在叠加图像上的黑色程度可以表示成 $[(b + 1) \times h_1 + (r - b - 1) \times h_0]/(r \times m)$. 而我们知道 h_1 和 h_0 是可区分的, 所以 $E^{(b)}$ 和 $E^{(b+1)}$ 加密序列在叠加图像的黑色程度也是可区分的.

安全性: 对于本方案的 (k,n) 可视密码, 若 $k'(k'<k)$ 个人的分享图像叠加后, 不会泄漏秘密图像的任何信息.

证明: 秘密图像上的每个加密序列, 或者使用 $M\in C_0$ 加密, 或者使用 $M\in C_1$ 加密, 因为 C_0 和 C_1 满足上述安全性, 所以本方案也满足上述安全性.

5 可变可视密码实例

以 (2,3) 分享图像大小可变的可视密码为例, 图1所示为秘密图像 (256×256), 图2所示为 2 点加密, 图3所示为 3 点加密, 图4所示为 4 点加密, 在图2–4中图 (a) 是 Share1 图像, 图 (b) 是 Share2 图像, 图 (c) 是 Share3 图像, 图 (d) 是图 (a) 和图 (b) 叠加后的图像. 本文所有显示图像的大小是原图像的 50%.

图 1 秘密图像
Figure 1 Secret figure

(a) 2 点加密的分存图像 1
(a) Share1 for 2-point encryption

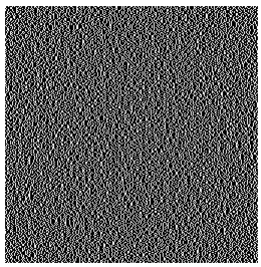
(b) 2 点加密的分存图像 2
(b) Share2 for 2-point encryption

(c) 2 点加密的分存图像 3
(c) Share3 for 2-point encryption

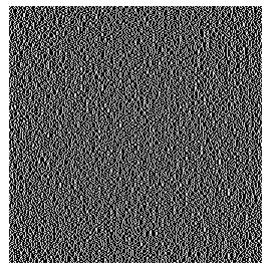
(d) 分存图像 1 和 2 叠加的图像
(d) Composition of Share1 and Share2

图 2 (2,3) 可视密码的 2 点加密
Figure 2 2-pioints encryption for (2,3) visual cryptography

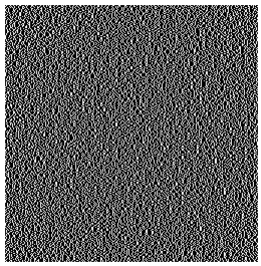
可见, 在图2所示的 2 点加密中分享图像是秘密图像的 3/2, 图3所示的 3 点加密和秘密图像一样大, 图4所示的 4 点加密分享图像是秘密图像的 3/4. 图2、4所示叠加后的图像会有变形 (其实传统可视密



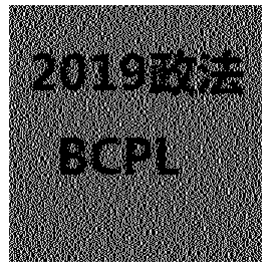
(a) 3 点加密的分存图像 1
(a) Share1 for 3-point encryption



(b) 3 点加密的分存图像 2
(b) Share2 for 3-point encryption



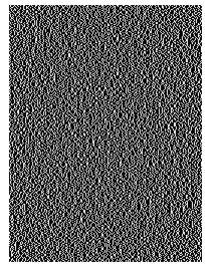
(c) 3 点加密的分存图像 3
(c) Share3 for 3-point encryption



(d) 分存图像 1 和 2 叠加的图像
(d) Composition of Share1 and Share2

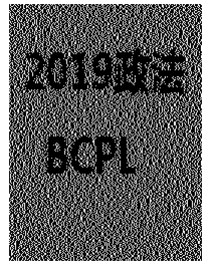
图 3 (2,3) 可视密码的 3 点加密
Figure 3 3-pioints encryption for (2,3) visual cryptography

(a) 4 点加密的分存图像 1
(a) Share1 for 4-point encryption



(b) 4 点加密的分存图像 2
(b) Share2 for 4-point encryption

(c) 4 点加密的分存图像 3
(c) Share3 for 4-point encryption



(d) 分存图像 1 和 2 叠加的图像
(d) Composition of Share1 and Share2

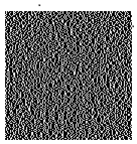
图 4 (2,3) 可视密码的 4 点加密
Figure 4 4-pioints encryption for (2,3) visual cryptography

码也产生变形).

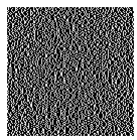
若要求叠加后的图像不变形, 就应该对 r 有所限制: 存在整数 p、q, 使 $m = p \times q$, 且 $|p-q|$ 最小, 那么 r 可取的集合是

$$\begin{cases} r \in \{(p+s) \times (q+s) \mid s \in z\}, & p = q \\ r \in \{(p \times s/t) \times (q \times s/t) \mid s \in z,\ t\text{是}p,q\text{的最大公约数}\}, & p \neq q \end{cases} \tag{3}$$

此例中, $m = 3 = 1 \times 3$, 即 $p = 1$, $q = 3$, $t = 1$, 假设 s 取 2, 那么 $r = (1 \times 2) \times (3 \times 2) = 12$, 此时叠加后的图像不会变形, 且缩小至秘密图像的 1/4, 如图 5 所示. 从图 5 中可见, 对于 (2,3) 可视密码, $r = 12$ 时叠加后的图像不会变形.



(a) 12 点加密的分存图像 1
(a) Share1 for 12-point encryption



(b) 12 点加密的分存图像 2
(b) Share2 for 12-point encryption

(c) 12 点加密的分存图像 3
(c) Share3 for 12-point encryption

(d) 分存图像 1 和 2 叠加的图像
(d) Composition of Share1 and Share2

图 5 (2,3) 可视密码的 12 点加密
Figure 5 12-pioints encryption for (2,3) visual cryptography

对于 (2,3) 可变可视密码, 分存图像的大小、分存图像的形变程度、图像恢复效果如表 1 所示, $r = 2$ 时是分存图像扩大的可视密码, 扩大为秘密图像的 3/2, 有形变, 人眼辨识图像恢复效果良好; $r = 3$ 时是像素不扩展可视密码, 无形变, 人眼辨识秘密图像恢复效果较好, 但图像个别位置边界模糊; $r = 4$ 时是分存图像缩小的可视密码, 缩小为秘密图像的 3/4, 人眼辨识图像恢复效果较好, 但边界模糊加重; $r = 12$ 时是分存图像缩小的可视密码, 缩小为秘密图像的 1/4, 无形变, 人眼辨识图像恢复效果尚可, 边界模糊较重.

表 **1** (2,3) 可变可视密码图像形变和图像恢复情况
Table 1 Image deformation and image restoration for (2,3) variable visual cryptography

变量 r	分存图像大小	形变程度	图像恢复效果
$r = 2$	秘密图像的 3/2	拉宽 3/2	良好
$r = 3$	秘密图像一样大	无形变	较好
$r = 4$	秘密图像的 3/4	变窄为 3/4	较好
$r = 12$	秘密图像的 1/4	无形变	尚可

如果对一个 $N \times N$ 大小的秘密图像进行加密, 本方案的分存图的个数为 n, 分存图大小为 $N \times N \times m/r$, 当 $r = m$ 时, 该加密就是像素不扩展可视密码; 当 $r > m$ 时, 该加密得到的就是分存图像缩小的可视密码 (r 的增大会降低解密图像的对比度); 当 $r < m$ 时, 该加密得到的就是分存图像扩大的可视密码. 本方案与其他方案的对比如表 2 所示.

表 **2** 本方案与其他方案比较

Table 2 Comparisons of this scheme with other schemes

方案	分存图个数	分存图大小
文献 [2]	n	$N \times N \times m$
文献 [8]	2	$N \times N$
本方案	n	$N \times N \times m/r$

6 总结与展望

本文提出任意点加密的可视密码, 即可变可视密码 (VVC), 一方面它解决了传统可视密码像素扩张的问题; 一方面它非常灵活, 能使分存图像小于加密图像、等于加密图像或大于加密图像, 从而能有效减少存储空间, 或在存储空间和图像质量之间找到一个平衡点.

当 r 较小时, 本文提出的可变可视密码加密的效果都非常好. 当 r 较大时, 会出现图像边界模糊的现象, 如何避免边界模糊是我们今后的工作, 如何设计出能够较好的应用于灰度和彩色图像的可变可视密码, 也是我们今后的工作.

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography[C]. In: Advance in Cryptology—EUROCRYPT '94. Springer Berlin Heidelberg, 1995: 1–12. [DOI: 10.1007/BFb0053419]

[2] DROSTE S. New results on visual cryptography[C]. In: Advance in Cryptology—CRYPTO '96. Springer Berlin Heidelberg, 1996: 401–415. [DOI: 10.1007/3-540-68697-5_30]

[3] HOU Y C. Visual cryptography techniques for color images without pixel expansion[J]. Journal of Information, Technology and Society, 2004, 2004(1): 95–110.
侯永昌. 像素不扩展之彩色视觉密码技术 [J]. Journal of Information, Technology and Society, 2004, 2004(1): 95–110.

[4] TUYLS P, HOLLMANN H D L, VAN LINT J H, et al. XOR-based visual cryptography schemes[J]. Designs, Codes and Cryptography, 2005, 37(1): 169–186. [DOI: 10.1007/s10623-004-3816-4]

[5] LI C Y. A digital watermarking algorithm based on image size invariant visual cryptography[J]. Journal of Dali University, 2017, 2(6): 19–21. [DOI: 10.3969/j.issn.2096-2266.2017.06.005]
李春艳. 基于像素不扩展视觉密码的水印算法 [J]. 大理大学学报, 2017, 2(6): 19–21. [DOI: 10.3969/j.issn.2096-2266.2017.06.005]

[6] WANG H J, MA D H, ZHANG E J, et al. A (3,3) visual cryptography scheme without pixel expansion[J]. Engineering Journal of Wuhan University, 2018, 51(12): 1123–1128. [DOI: 10.14188/j.1671-8844.2018-12-013]
王洪君, 马冬鹤, 张恩绮, 等. 一种无像素膨胀的 (3,3) 视觉密码方案 [J]. 武汉大学学报 (工学版), 2018, 51(12): 1123–1128. [DOI: 10.14188/j.1671-8844.2018-12-013]

[7] WANG H J, ZHAO T F, SHANG D L, et al. Non-expanded (2,2) visual cryptography scheme with masked image[J]. Journal of Nanjing University(Natural Science), 2018, 54(1): 157–162. [DOI: 10.13232/j.cnki.jnju.2018.01.017]
王洪君, 赵腾飞, 尚大龙, 等. 具有掩盖图像的像素不扩展的 (2,2) 视觉密码方案 [J]. 南京大学学报 (自然科学), 2018, 54(1): 157–162. [DOI: 10.13232/j.cnki.jnju.2018.01.017]

[8] LIN K Z, FAN B, YANG W. Visual cryptographic scheme with sub-block coding method[J]. Computer Engineering and Applications, 2010, 46(6): 160–162. [DOI: 10.3778/j.issn.1002-8331.2010.06.046]
林克正, 范波, 杨微. 基于分块字典的可视密码改进方法 [J]. 计算机工程与应用, 2010, 46(6): 160–162. [DOI: 10.3778/j.issn.1002-8331.2010.06.046]

[9] YU B, HU H, CHEN W P, et al. XOR-based region incrementing visual cryptography scheme with share block construction[J]. Journal of Electronics & Information Technology, 2015, 37(8): 1978–1983. [DOI: 10.11999/JEIT141385]
郁滨, 胡浩, 陈武平, 等. 一种共享份分块构造的异或区域递增式视觉密码方案 [J]. 电子与信息学报, 2015, 37(8): 1978–1983. [DOI: 10.11999/JEIT141385]

[10] FANG L G, FU Z X, SHEN G, et al. Color raster map-sharing algorithm based on visual cryptography[J]. Journal of Image and Graphics, 2018, 23(1): 123–132. [DOI: 10.11834/jig.170309]
房礼国, 付正欣, 沈刚, 等. 视觉密码的彩色栅格地图分存算法 [J]. 中国图象图形学报, 2018, 23(1): 123–132. [DOI: 10.11834/jig.170309]

[11] HAN Y Y, ZHANG J, YAN X X, et al. A color visual cryptography scheme based on grid structure[J]. Journal of Beijing Electronic Science and Technology Institute, 2018, 26(3): 8–17. [DOI: 10.3969/j.issn.1672-464X.2018.03.003]
韩妍妍, 张京, 闫晓璇, 等. 一种基于栅格结构的彩色可视密码方案 [J]. 北京电子科技学院学报, 2018, 26(3): 8–17. [DOI: 10.3969/j.issn.1672-464X.2018.03.003]

[12] HOU Y C, GUAN Z Y, CAI Z F, et al. $(3, n)$-visual secret sharing scheme with unexpanded shares[J]. Chinese Journal of Computers, 2016, 39(3): 441–453. [DOI: 10.11897/SP.J.1016.2016.00441]
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. [DOI: 10.11897/SP.J.1016.2016.00441]

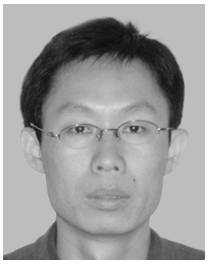
[13] ZHANG S, LI W, AI X C. Improved visual cryptography scheme to prevent cheaters[J]. Application Research of Computers, 2016, 33(12): 3770–3773. [DOI: 10.3969/j.issn.1001-3695.2016.12.055]
张舒, 李薇, 艾小川. 一种改进的防欺骗可视密码方案 [J]. 计算机应用研究, 2016, 33(12): 3770–3773. [DOI: 10.3969/j.issn.1001-3695.2016.12.055]

[14] GUO F, LIU L J, LIU X Y, et al. (2,2) visual cryptography scheme based on autostereogram sharing images[J]. Application Research of Computers, 2018, 35(9): 2752–2756, 2771. [DOI: 10. 3969/j.issn.1001-3695.2018.09.045]
郭璠, 刘丽珏, 刘熙尧, 等. 基于三维立体分享图像的 (2,2) 视觉密码方案 [J]. 计算机应用研究, 2018, 35(9): 2752—2756, 2771. [DOI: 10.3969/j.issn.1001-3695.2018.09.045]

[15] HE W C, LIU C, HAN Y Y, et al. Multi-level visual cryptography scheme with lossless recovery[J]. Application Research of Computers, 2017, 34(5): 1540–1543. [DOI:10.3969/j.issn.1001-3695.2017.05.059]
何文才, 刘畅, 韩妍妍, 等. 一种无损恢复的多级别的可视密码方案 [J]. 计算机应用研究, 2017, 34(5): 1540–1543. [DOI:10.3969/j.issn.1001-3695.2017.05.059]

作者信息

乔明秋(1982–), 黑龙江伊春人, 讲师. 研究领域为密码学、信息安全.
qiaomingqiu@163.com



赵振洲 (1978–), 辽宁人, 副教授. 研究领域为数据恢复、信息安全.
zhousun21@163.com