

基于迭代算法的可验证视觉密码

郁 滨 卢锦元* 房礼国
(信息工程大学电子技术学院 郑州 450004)

摘 要: 通过改变验证图像的分享和恢复方式, 该文提出了一种基于迭代算法的可验证视觉密码方案。该方案设计专用算法分享验证图像, 利用算法的迭代优化验证过程, 不仅大幅减小了像素扩展度, 而且显著提高了验证效率。同时, 通过引入异或操作实现了验证图像的完全恢复。

关键词: 视觉密码; 可验证; 防欺骗; 像素扩展度

中图分类号: TP309.7

文献标识码: A

文章编号: 1009-5896(2011)01-0163-05

DOI: 10.3724/SP.J.1146.2010.00270

Verifiable Visual Cryptography Based on Iterative Algorithm

Yu Bin Lu Jin-yuan Fang Li-guo

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract: By changing sharing and recovering ways of the verification image, a verifiable Visual Cryptography Scheme (VCS) based on iterative algorithm is proposed in this paper. Since the verification image is shared with special algorithms, and the verification process is optimized through iterative algorithm, the proposed scheme not only makes the pixel expansion much smaller, but also improves the checking efficiency greatly. Furthermore, verification images are perfectly recovered by the XOR operation introduced.

Key words: Visual cryptography; Verifiable; Cheating prevention; Pixel expansion

1 引言

秘密共享概念最早由 Shamir^[1]和 Blakley^[2]分别于 1979 年独立提出, 至今已成为现代密码学领域中一个非常重要的研究方向。大多数秘密共享方案的加解密过程会带来高额的计算开销。视觉密码 (visual cryptography) 作为一种新的秘密共享技术, 适合于低开销的计算环境, 特别是其恢复过程的简便性, 一经提出便引起广大学者的重视和研究兴趣。自 Naor 和 Shamir^[3]于 1994 年提出以后, 视觉密码的研究主要集中在存取结构^[4,5]、参数优化^[6-8]、彩色图像^[9-11]及多秘密分享^[12-14]等方面, 并取得了丰硕的成果。然而, 以上研究都没有考虑欺骗者的存在, 为了进一步丰富和完善视觉密码的理论体系, 部分学者开始对视觉密码中的欺骗问题展开研究^[15-20]。

视觉密码中的欺骗行为, 按参与者人数划分, 有单独欺骗和共谋欺骗两种。陈玲慧^[15]针对(2,2)门限结构, 提出了两种具有信息验证功能的视觉密码方案, 能够检测恢复图像是否受到非法篡改。文献

[16] 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, 可以通过能否恢复验证图像检测出 k 个参与者中的一个欺骗者。遗憾的是, 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。为此, 文献[17]通过结合原始 (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, 但是没有考虑多个欺骗者合作的情况。

针对多个参与者的共谋欺骗行为, 文献[18]提出了两种方案, 第 1 种通过对共享份验证来实现, 但是每个参与者除了需要保管自己的共享份外, 还得另外保管一个验证份, 增加了参与者的负担; 第 2 种方案是利用 $(2, n+l)$ 方案来代替 $(2, n)$ 方案, 使得欺骗者共谋时无法确认另外一个参与者共享份的具体信息, 但是该方案中, 欺骗者能够确定秘密图像中的白像素, 可以通过将白像素改变为黑像素而原来的黑像素保持不变, 进行特殊的欺骗。文献[19]构造了一种基于非强存取结构的 (k', k, n) 可防欺骗视觉密码方案, 该方案能抵抗少于 k' 人的共谋欺骗, 然而当共谋者较多, 达到 $l (k' \leq l \leq k)$ 人时, 则无能为力。另外, 由于以上方案都是参与者之间互相检测, 当参与者数量增多时必然导致方案操作的复杂, 因此

2010-03-23 收到, 2010-08-25 改回
国家自然科学基金(61070086)和河南省科技创新杰出青年基金
(094100510002)资助课题
*通信作者: 卢锦元 lujinyuan1999@sina.com

文献[20]提出了一种基于可信第三方的可验证视觉密码方案,其中可信第三方只负责检验参与者的真伪,不参加秘密图像的恢复,从而简化了方案的操作过程。同时,通过对每个共享份进行真实性检验,能够有效防止共谋欺骗。但该方案仍存在两点不足:(1)采用将秘密矩阵和验证矩阵并置的方式构造基础矩阵,导致像素扩展度增大,恢复效果不佳;(2)每次只能验证一个共享份,当共享份较多时,会明显影响方案的效率。

综上所述,本文将提出一种基于迭代算法的可验证视觉密码方案,该方案通过设计专用算法对验证图像进行分享,并在验证时运用异或操作,不仅能够大幅减小共享份的像素扩展度,而且可以实现验证图像中黑白像素的完全恢复。同时,该方案每次可检验多个共享份的真伪,验证效率得到了显著提高。

2 方案构思

(1)存取结构 参与者集合为 $P=\{P_1, P_2, \dots, P_n\}$,可信第三方为 P_{n+1} ;秘密图像 S 的存取结构为 $(\Gamma_{\text{Qual}}^S, \Gamma_{\text{Forb}}^S)$,其中 $\Gamma_{\text{Qual}}^S = \{P_{i1}, P_{i2}, \dots, P_{ik}\}$,生成的秘密共享份为 $S_i (i=1, 2, \dots, n)$;与 S 大小相等的验证图像 V 存取结构为 $(\Gamma_{\text{Qual}}^V, \Gamma_{\text{Forb}}^V)$,生成的验证份为 T_i 。

(2)基本思想 前期研究表明,现有视觉密码方案,无论是门限结构还是通用存取结构,无论是单秘密分享还是多秘密分享,都是基于基础矩阵构造的。而可验证视觉密码则通过将秘密矩阵和验证矩阵并置来分享机密图像。很明显,基于矩阵构造的视觉密码方案,不可避免的带来了像素扩展度的增大,对比度的降低。为此,本文避开基础矩阵的构造,通过算法设计实现对验证图像的分析,其特点体现在以下3个方面:首先,通过设计专用算法来分享验证图像,使像素扩展度大幅减少,该算法以参与者的共享份和验证图像为输入,输出即为该参与者的验证份,使分享过程更高效。其次,在验证时,通过引入代数结构为群的异或操作,使验证图像实现了黑白像素完全恢复,增大了对比度。最后,对验证过程进行优化,通过分享算法的迭代调用,能够同时检验多个共享份的真实性,显著提高了方案效率。

(3)构造方法 根据基本思想,构造方法如下:分享过程中,对于秘密图像仍采用一般的视觉密码方案,对于验证图像则采取专用算法来分享。具体流程图如图1所示。

恢复过程中,秘密图像仍然是直接叠加授权集 Γ_{Qual}^S 中的共享份;验证图像的恢复中则引入了异或

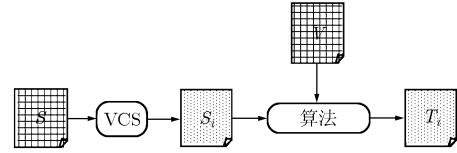


图1 分享流程图

操作。即: $S = S_{i1} + S_{i2} + \dots + S_{ik}$ (“+”表示“或”操作), $V = S_i \oplus T_i$ (“ \oplus ”表示“异或”操作)。

3 方案设计

本节首先给出了方案的分享及恢复流程,其次对核心算法进行了设计,并在最后对方案有效性作了证明。

3.1 方案流程

该方案中,可信第三方 P_{n+1} 保管一张验证图像 V 和 n 张验证份 $T_i (i=1, 2, \dots, n)$,各参与者 P_i 只保管一张共享份 S_i 。

(1)分享流程 分享流程如图2所示,具体步骤如下:

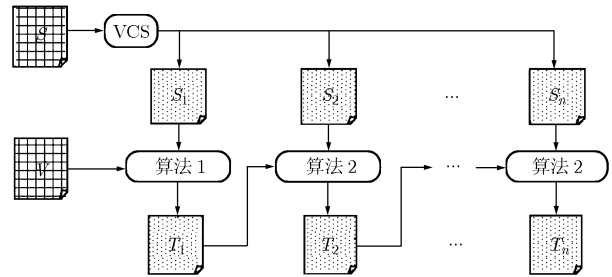


图2 分享流程图

步骤1 对秘密图像 S ,用 $(\Gamma_{\text{Qual}}^S, \Gamma_{\text{Forb}}^S) - \text{VCS}$ 进行分享,生成秘密共享份 S_1, S_2, \dots, S_n ;

步骤2 对验证图像 V ,当 $i=1$ 时,以 V 和 S_1 为算法1的输入,输出即为验证份 T_1 ;当 $i>1$ 时,以 T_{i-1} 和 S_i 为算法2的输入,输出即为验证份 T_i 。

(2)恢复流程

秘密图像恢复:属于授权集的共享份直接叠加就可恢复秘密图像 S ,即

$$S = S_{i1} + S_{i2} + \dots + S_{ik} \quad (1)$$

验证过程:通过将共享份集合与某些验证份相异或,来验证该共享份集合的真伪。但具体与哪些验证份运算,需要结合 $V' = S_1 \oplus T_1, T_{l-1} = T_l \oplus S_l (l>1)$ 进行简单的推导,具体如何推导将在实验中举例说明。此处 V' 为将 V 长宽各放大 \sqrt{m} 倍所得的图像,其中 m 为 $(\Gamma_{\text{Qual}}^S, \Gamma_{\text{Forb}}^S) - \text{VCS}$ 的像素扩展度(不妨设 m 为平方数,因为它为非平方数时,可以通过添加若干全1列,将其转化为平方数)。

3.2 算法设计

分享算法是本方案的核心, 它分为两部分, 算法1以验证图像和共享份作为输入, 算法2则以共享份和前一过程的输出作为输入, 进行迭代。具体算法如下:

算法1(表1)输入为图像 I_1 和图像 I_2 , 输出为图像 O , 其中 I_1 的一个像素点对应于 I_2 及 O 中一个大小为 $\sqrt{m} \times \sqrt{m}$ 的像素块。当 I_1 中像素点为0时, 输出 O 中对应该像素点的像素块取值与 I_2 中相同, 否则相反。

表1 算法1

输入	图像 I_1 , 大小为 $a \times b$; 图像 I_2 , 大小为 $a\sqrt{m} \times b\sqrt{m}$ 。
输出	图像 O , 大小为 $a\sqrt{m} \times b\sqrt{m}$ 。
步骤1	选取图像 I_1 的一个像素点 $I_1[i, j]$, 其中 $1 \leq i \leq a$, $1 \leq j \leq b$ 。若 $I_1[i, j] = 0$, 转步骤2, 否则跳转到步骤3;
步骤2	将 I_2 中对应位置处的像素块复制后, 填入 O 中, 即 for ($1 \leq e \leq \sqrt{m}$, $1 \leq f \leq \sqrt{m}$), $O[\sqrt{m}(i-1)+e, \sqrt{m}(j-1)+f] = f_{\text{equ}}(I_2[\sqrt{m}(i-1)+e, \sqrt{m}(j-1)+f])$ 。然后直接跳转到步骤4;
步骤3	将 I_2 中对应位置处的像素块取反后, 填入 O 中。即 for ($1 \leq e \leq \sqrt{m}$, $1 \leq f \leq \sqrt{m}$), $O[\sqrt{m}(i-1)+e, \sqrt{m}(j-1)+f] = f_{\text{com}}(I_2[\sqrt{m}(i-1)+e, \sqrt{m}(j-1)+f])$;
步骤4	对 I_1 的下一像素点重复以上步骤, 直至所有像素处理完毕;
步骤5	输出图像 O 。

算法2(表2)输入为图像 I_1 和图像 I_2 , 输出为图像 O , 这3幅图像大小相等。当 I_1 中像素点为0时, 输出 O 中对应位置像素点取值与 I_2 中相同, 否则相反。

表2 算法2

输入	图像 I_1 , 大小为 $a \times b$; 图像 I_2 , 大小为 $a \times b$ 。
输出	图像 O , 大小为 $a \times b$ 。
步骤1	选取图像 I_1 的一个像素点 $I_1[i, j]$, 其中 $1 \leq i \leq a$, $1 \leq j \leq b$ 。若 $I_1[i, j] = 0$, 转步骤2, 否则跳转到步骤3;
步骤2	将 I_2 中对应位置处的像素点复制后, 填入 O 中, 即 $O[i, j] = f_{\text{equ}}(I_2[i, j])$ 。然后直接跳转到步骤4;
步骤3	将 I_2 中对应位置处的像素点取反后, 填入 O 中。即 $O[i, j] = f_{\text{com}}(I_2[i, j])$;
步骤4	对 I_1 的下一像素点重复以上步骤, 直至所有像素处理完毕;
步骤5	输出图像 O 。

其中 $f_{\text{equ}}(x)$ 为等值函数, 即通过等值操作生成新共享份。根据共享份 S_1 中像素点取值 s_1 , 等值函数:

$$f_{\text{equ}}(x) = \begin{cases} 0, & x = 0 \\ 1, & x = 1 \end{cases} \quad (2)$$

将 s_1 直接拷贝, 生成新共享份 S_2 中像素点的取值 s_2 。例如: $s_1=0$ 时, $s_2=0$, 即 $s_2 = f_{\text{equ}}(s_1 = 0) = 0$ 。

$f_{\text{com}}(x)$ 为取反函数, 即通过取反操作生成新共享份。根据共享份 S_1 中像素点取值 s_1 , 取反函数:

$$f_{\text{com}}(x) = \begin{cases} 0, & x = 1 \\ 1, & x = 0 \end{cases} \quad (3)$$

将 s_1 取反, 生成新共享份 S_2 中像素点的取值 s_2 。例如: $s_1=1$ 时, $s_2=0$, 即 $s_2 = f_{\text{com}}(s_1 = 1) = 0$ 。

3.3 有效性证明

对于秘密图像, 本文采用一般视觉密码方案来处理, 比如通用存取结构下的 $(\Gamma_{\text{Qual}}^S, \Gamma_{\text{Forb}}^S)$ -VCS, 其满足视觉密码的安全性条件和对比性条件, 在此不需再作证明。下面针对验证图像进行有效性证明。

(1)安全性条件证明 方案中各参与者 P_i 拥有的共享份 S_i , 是根据一般视觉密码方案分享流程生成的随机黑白图像, 它们在分享验证图像之前已经产生, 与验证图像相互独立。另外所有验证份都由可信第三方保管, 所以由参与者所持有的共享份无法推出验证图像, 满足安全性条件。

(2)对比性条件证明 如图2所示, 首先当 $l>1$ 时, 方案以共享份 S_l 和前一过程的输出 T_{l-1} 作为算法2的输入, 进行迭代调用, 生成验证份 T_l 。即当 $T_{l-1}[i, j] = 0$ 时, T_l 中对应的像素点与 S_l 中相等, 否则相反。而在异或操作中, 两相同分量异或得0, 反之得1, 所以有 $T_{l-1} = T_l \oplus S_l$ 。其次当 $l=1$ 时, 方案以验证图像 V 和共享份 S_1 作为算法1的输入, 生成验证份 T_1 。即当 $V[i, j] = 0$ (白像素)时, T_1 中对应该像素的像素块与 S_1 中相等, 否则相反。在验证时, 通过将 S_1 和 T_1 相异或来恢复验证图像, 而异或操作中, 两分量相同时, 恢复全白, 反之则恢复全黑。因此, 黑白像素实现了完全恢复, 即满足对比性条件。

4 实验结果与分析

(1)实验结果 本节以一个实例来对方案效果进行检验。设参与者集合 $P = \{P_1, P_2, P_3, P_4\}$, 验证方为 P_5 , 秘密图像 S 的存取结构为(2,4)门限结构。图3为原始秘密图像 S 和验证图像 V ; 图4为生成



图3 秘密图像及验证图像

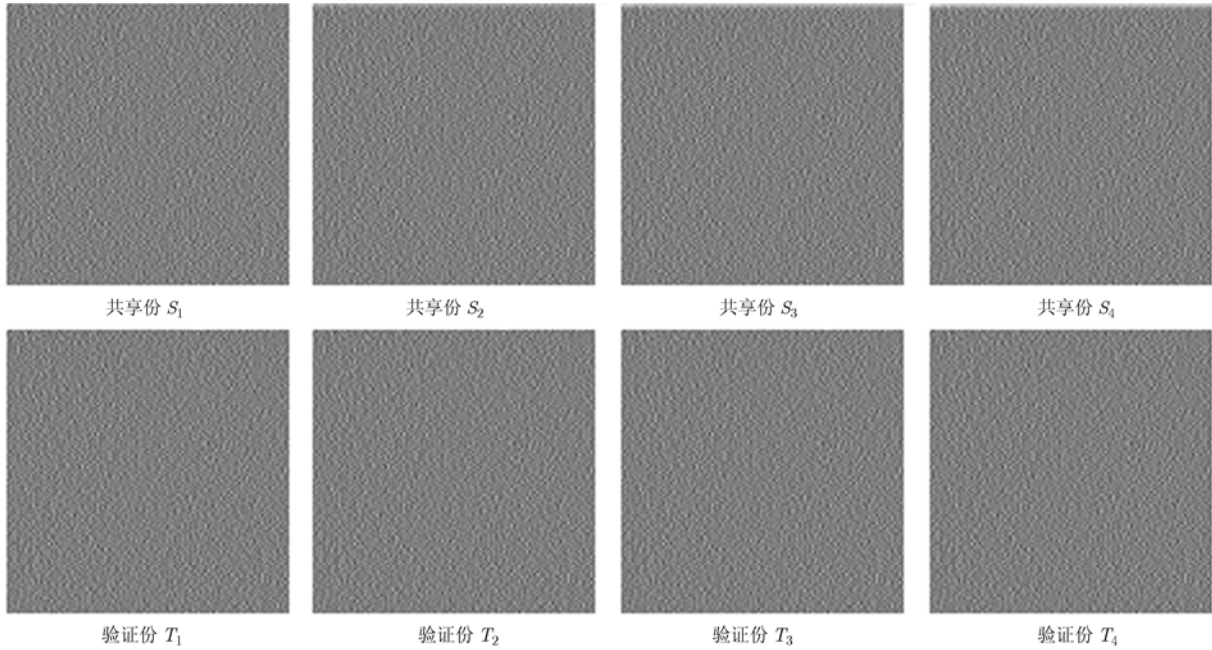


图4 各共享份及验证份

的秘密共享份及对应的验证份。

在验证时，依照检验集合 P' 中所包含成员的不同，分两种情况予以考虑：

情况 1 检验集合 P' 中包含 P_1 ，即 $P_1 \in P'$ 。此时，依据 $V' = S_1 \oplus T_1$ ， $T_{l-1} = T_l \oplus S_l (l > 1)$ 将包含在 P' 中的共享份直接代入，不包含在 P' 中共享份用验证份代入，即可完成验证。不妨设要检验参与者集合 $\{P_1, P_2\}$ 的真实性，由如下方程组：

$$\begin{cases} V' = S_1 \oplus T_1 \\ T_1 = S_2 \oplus T_2 \end{cases} \quad (4)$$

求得 $V' = S_1 \oplus S_2 \oplus T_2$ ，因此将共享份 S_1, S_2 和验证份 T_2 相异或，便可对该参与者集合 $\{P_1, P_2\}$ 进行验证。

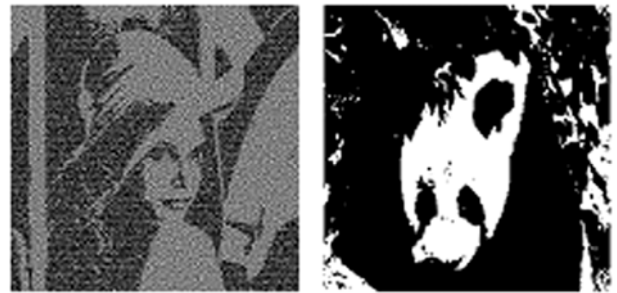
情况 2 检验集合 P' 中不包含 P_1 ，即 $P_1 \notin P'$ 。此时，依据 $V' = 0 \oplus V'$ ， $T_{l-1} = T_l \oplus S_l (l > 1)$ 将包含在 P' 中的共享份直接代入，不包含在 P' 中共享份用验证份代入，即可完成验证。不妨设要检验参与者集合 $\{P_2, P_3\}$ 的真实性，由如下方程组：

$$\begin{cases} T_1 = S_2 \oplus T_2 \\ T_2 = S_3 \oplus T_3 \end{cases} \quad (5)$$

求得 $T_1 \oplus S_2 \oplus S_3 \oplus T_3 = 0$ ，因此将图像 V' ，共享份 S_2, S_3 及验证份 T_1, T_3 相异或，便可对该参与者集合 $\{P_2, P_3\}$ 进行验证。

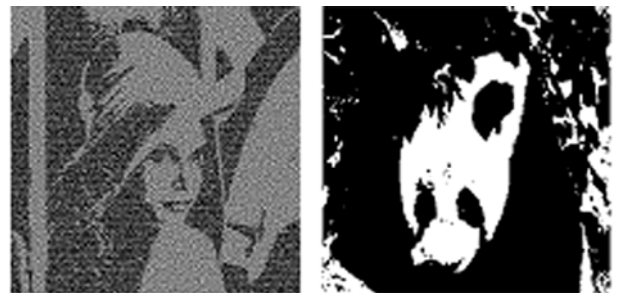
图 5，图 6 分别为情况 1，情况 2 的恢复效果图，从图中可以看出，方案恢复效果良好，而且验证图像实现了黑白像素完全恢复。

(2)实验分析 对于视觉密码而言，像素扩展度和相对差是两个重要的参数，可以用来评价方案的



(a) 恢复秘密图像 S (b) 恢复验证图像 V

图5 情况 1 恢复效果图



(a) 恢复秘密图像 S (b) 恢复验证图像 V

图6 情况 2 恢复效果图

优劣。表 3 是本文方案与文献[20]方案的参数对比。其中 m, h, l 分别为 $(\Gamma_{Qual}^S, \Gamma_{Forb}^S) - VCS$ 中像素扩展度、白像素的白度、黑像素的白度， n 为参与者人数。

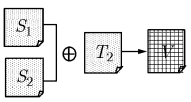
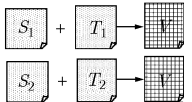
由表 3 可知，本文方案在两个参数上都有显著改善，特别是验证图像实现了黑白像素完全恢复。

表 4 是本文方案与文献[20]方案验证复杂度的比较，从表中可以看出，本文方案验证次数及同等

表 3 本文方案与文献[20]方案参数对比

	本文方案		文献[20]方案	
	像素扩展度	相对差	像素扩展度	相对差
秘密图像	m	$(h-l)/m$	$m+2n$	$(h-l)/(m+2n)$
验证图像	m	1	$m+2n$	$1/(m+2n)$

表 4 本文方案与文献[20]方案验证效率对比

	本文方案	文献[20]方案
验证步骤		
验证次数	1 次	2 次
验证耗时	0.011205s	0.048979s

条件下验证耗时(运行环境为 Windows XP, matlab7.1)均减少了。总之,本方案与以往相比,有如下两个显著优点:

(1)恢复效果更好 通过设计分享算法来分享验证图像,缩小了像素扩展度,并且在验证时,引入异或操作,实现了黑白像素完全恢复。

(2)检验效率提高 对验证过程进行优化,可以同时检验多个共享份的真假,大幅提高了方案检验效率。

5 结束语

本文避开传统的验证矩阵构造,设计了一种迭代算法用于分享验证图像。并将异或操作引入到共享份验证中,使验证图像中的黑白像素得以完全恢复。同时,通过迭代算法优化验证过程,使验证效率大幅提高。实验结果表明,本方案减小了存储空间,提高了分享效率,恢复图像易于辨认。

参 考 文 献

- [1] Shamir A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612-613.
- [2] Blakley G R. Safeguarding cryptographic keys[C]. Proceedings of the National Computer Conference, NJ, USA, 1979, 48: 242-268.
- [3] Naor M and Shamir A. Visual cryptography[C]. Advances in Cryptology-Eurocrypt'94, Lecture Notes in Computer Science, 1995, 950: 1-12.
- [4] Ateniese G, Carlo B, and Santis A D, et al. Visual cryptography for general access structures[J]. *Information and Computation*, 1996, 129(2): 86-106.
- [5] Steve L, Daniel M, and Rafail O. Visual Cryptography on Graphs[C]. COCOON 2008, LNCS 5092: 225-234.
- [6] Boundo C, Santis A D, and Stinson D R. On the contrast in

visual cryptography schemes[J]. *Journal of Cryptography*, 1999, 12(4): 261-289.

- [7] Fang Li-guo and Yu Bin. Research on pixel expansion of $(2, n)$ visual threshold scheme[C]. 1st International Symposium on Pervasive Computing and Applications Proceedings (SPCA06), Ningbo, 2006: 856-860.
- [8] Lin Sen-jen, Lin Ja-chen, and Fang Wen-pinn. Visual Cryptography (VC) with non-expanded shadow images Hilbert-curve approach[C]. ISI2008, Taipei, 2008: 271-272.
- [9] Cimato S, De Prisco R, and De Santis A. Optimal colored threshold visual cryptography schemes[J]. *Designs, Codes and Cryptography*, 2005, 35(3): 311-335.
- [10] Yang Ching-nung and Chen Tse-shih. Colored visual cryptography scheme based on additive color mixing[J]. *Pattern Recognition*, 2008, 41(10): 3114-3129.
- [11] Ng F Y and Wong D S. On the security of a visual cryptography scheme for color images[J]. *Pattern Recognition*, 2009, 42(5): 929-940.
- [12] Wu H C and Chang C C. Sharing visual multi-secrets using circle shares[J]. *Computer Standards & Interfaces*, 2005, 134(28): 123-135.
- [13] Yu B, Fu Z X, and Fang L G. A modified multi-secret sharing visual cryptography scheme[C]. CIS2008, Suzhou, 2008: 351-354.
- [14] Fu Z X and Yu B. Research on rotation visual cryptography scheme[C]. International symposium on information engineering and electronic commerce, IEEE, Ternopil, Ukraine, 2009: 533-536.
- [15] 陈玲慧. 视觉化密码之研究及其应用. 中国台湾专题研究计划成果报告, 计划编号: NSC 89-2213-E-009-016, 1999.
- [15] Chen Ling-hui. A study on visual cryptography and its applications. NSC 89-2213-E-009-016, 1999.
- [16] 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.
- [16] Guo Jie, Yan Hao, Liu Yan, and Chen Ke-fei. A cheater detectable visual cryptography scheme[J]. *Computer Engineering*, 2005, 31(6): 126-128.
- [17] 徐晓辉, 郁滨. 无重影的可防欺骗视觉密码方案[C]. 全国第18届计算机技术与应用学术会议(CACIS2007), 宁波, 2007: 1335-1339.
- [17] Xu Xiao-hui and Yu Bin. A cheater detectable VCS without fringes[C]. CACIS2007, Ningbo, 2007: 1335-1339.
- [18] Gwoboa H, Tzungher C, and Dushiau T. Cheating in visual cryptography[J]. *Designs, Codes and Cryptography*, 2006, 38(2): 219-236.
- [19] 王益伟, 郁滨. 一种 (k, k, n) 可防欺骗视觉密码方案[C]. 全国第19届计算机技术与应用学术会议(CACIS08), 合肥, 2008: 492-496.
- [19] Wang Yi-wei and Yu Bin. A (k, k, n) -cheater prevention VCS[C]. CACIS08, Hefei, 2008: 492-496.
- [20] Yu B, Fang L G, and Xu X H. A Verifiable visual cryptography scheme[C]. CIS2008, Suzhou, 2008: 347-350.

郁 滨: 男, 1964年生, 教授, 博士生导师, 研究方向为视觉密码和网络安全。

卢锦元: 男, 1985年生, 硕士生, 研究方向为视觉密码。

房礼国: 男, 1981年生, 讲师, 研究方向为视觉密码和网络安全。