

基于概率法的防欺骗视觉密码方案

郁 滨,王益伟,房礼国

(信息工程大学 电子技术学院,郑州 450004)

(wyw6912173@126.com)

摘 要:利用概率法构造了一种防欺骗视觉密码方案,在不需要其他额外信息的前提下,可发现欺骗者的存在。同时,本方案还可以控制秘密图像的恢复效果。仿真实验表明,该方案扩展度小,恢复效果好,并可以通过控制概率来调整秘密图像的恢复效果。

关键词:视觉密码;概率法;共享份;欺骗者

中图分类号: TP391 **文献标志码:** A

Anti-cheating visual cryptography scheme based on probability

YU Bin, WANG Yi-wei, FANG Li-guo

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

Abstract: An anti-cheating Visual Cryptography Scheme (VCS) scheme based on probability, which can find the cheaters without extra information, was proposed. Meanwhile, the visual effects of recovered secret image could be controlled in this scheme. Performance analysis and simulation results show that this scheme has little pixel expansion and the visual effect of recovered secret image can be adjusted by controlling probability.

Key words: visual cryptography; probability; share; cheater

0 引言

秘密共享是现代密码学领域中一个非常重要的分支,也是信息安全方向一个重要的研究内容。视觉密码(Visual Cryptography)作为一种新型的秘密共享技术,自 Naor 和 Shamir^[1]在 1994 年欧洲密码学年会上提出后,由于其安全、简单、实用的特点,便引起了广大学者的浓厚兴趣,越来越多学者投入这一领域的研究^[1-8]。文献[2-4]利用排列方法构造的 $(2, n)$ 方案使像素扩展度和相对差都有较大改进,同时利用组合方法设计了像素扩展度最优的 $(2, n)$ 视觉密码方案。文献[5]提出的通用存取结构视觉密码方案,将参与者的集合分为授权子集和禁止子集,只有授权子集中参与者的共享份叠加后才可以恢复出秘密信息,而禁止子集中参与者的共享份叠加时则得不到任何信息。文献[6]提出了一种新视觉密码方案,将通用存取结构分为强存取结构和非强存取结构,并详细分析了非强存取结构视觉密码方案的构造方法。

然而,视觉密码同其他秘密共享体制一样,也面临着欺骗攻击的威胁。在恢复秘密信息时,如果参与者出示了一份假的共享份,则共享份在叠加时就不能恢复出秘密图像,而且欺骗者在骗取到一定数量的共享份后就可以得到秘密信息,从而导致秘密信息的泄露。为了防止这种欺骗行为的发生,文献[9-10]通过将原始的 (k, n) 和 $(k-1, n)$ 视觉密码方案结合,构造出 (k, n) 可防欺骗视觉密码方案,该方案虽然可以实现防欺骗的功能,但在恢复秘密图像中,存在验证图像的重影,影响秘密图像的分辨。为改进这一方案,文献[11]利用 (k, n) 和改进的 $(k-1, k-1)$ 视觉密码方案设计了一种无重影的可防欺骗视觉密码方案。该方案在消除验证图像重影的

同时,可以清晰地恢复出秘密图像的信息。文献[12]利用累积矩阵构造了一种防欺骗视觉密码方案,该方案扩展度小,秘密图像恢复效果好。

上述防欺骗视觉密码方案虽然可以实现防欺骗的功能,但像素扩展度较大,不便于共享份的存储和传输。为解决这一问题,本文提出一种概率法防欺骗视觉密码方案,通过改变共享份的生成方式,减小像素扩展度,提高秘密图像的恢复效果。

1 概率法防欺骗视觉密码方案

1.1 概率法模型基本思想

现有的防欺骗视觉密码方案的设计思想均是通过矩阵连接等方式构造满足条件的基础矩阵,然后根据基础矩阵生成共享份。而概率法模型的设计思想则是首先分别生成分享秘密图像和验证图像的共享份,然后利用概率对相应共享份中的所有像素逐一进行随机选择,进而生成防欺骗视觉密码方案的共享份。

在概率法模型中,秘密图像和验证图像的共享份分别由普通 (k, n) 方案^[5]和非强存取结构^[6]构造。在实际的构造过程中,设分享秘密图像的基础矩阵的扩展度为 m' ,分享验证图像的基础矩阵的扩展度为 m'' ,令 $m = \lceil \sqrt{\max(m', m'')} \rceil^2$,为避免共享份及恢复信息的失真,首先将两方案的基础矩阵分别用全为 1 的列扩充补足至 m 列,再根据基础矩阵分别生成分享秘密图像和验证图像的共享份。

1.2 概率法模型建立

根据上述分析,概率法模型为一个五元组:

$$G = (S, V, R, p, p_0)$$

其中,

收稿日期:2009-02-04;修回日期:2009-03-17。

作者简介:郁滨(1964-),男,河南郑州人,教授,博士生导师,博士,主要研究方向:视觉密码、网络监控;王益伟(1983-),男,山东潍坊人,硕士研究生,主要研究方向:视觉密码;房礼国(1981-),男,江苏盐城人,讲师,硕士,主要研究方向:视觉密码、网络监控。

S 为分享秘密图像的共享份的集合,其中每一个共享份均为 $w \times h$ 的黑白二值图像:

$$S = \{S_1, S_2, \dots, S_n\}$$

V 为分享验证图像的共享份的集合,其中每一个共享份均为 $w \times h$ 的黑白二值图像:

$$V = \{V_1, V_2, \dots, V_n\}$$

R 为生成的概率法防欺骗方案共享份的集合,其中每一个共享份均为 $w \times h$ 的黑白二值图像:

$$R = \{R_1, R_2, \dots, R_n\}$$

p 为一给定概率;

p_0 为一随机数, $p_0 \in (0, 1)$;

R 的生成按如下步骤完成:

- 1) 选择共享份 R_k 中的任一像素 $R_k[i, j], i \in [1, w], j \in [1, h]$;
- 2) 生成随机数 p_0 ;
- 3) 若 $p_0 \leq p$, 则对于 $\forall k, R_k[i, j] = S_k[i, j]$; 相反地, 若 $p_0 > p$, 对于 $\forall k, R_k[i, j] = V_k[i, j]$ 。

1.3 方案流程

设要构造的防欺骗视觉密码方案为一个 (k', k, n) 方案, 其中 n 为所有参与者的集合, 即当 $k \leq q \leq n$ 时, 恢复秘密图像 S , 当 $k' \leq q < k$ 时, 恢复验证图像 V , 通过任意 q 个共享份之间的相互叠加看能否得到验证图像的信息来查找欺骗者。概率法防欺骗视觉密码方案设计流程如图1所示。

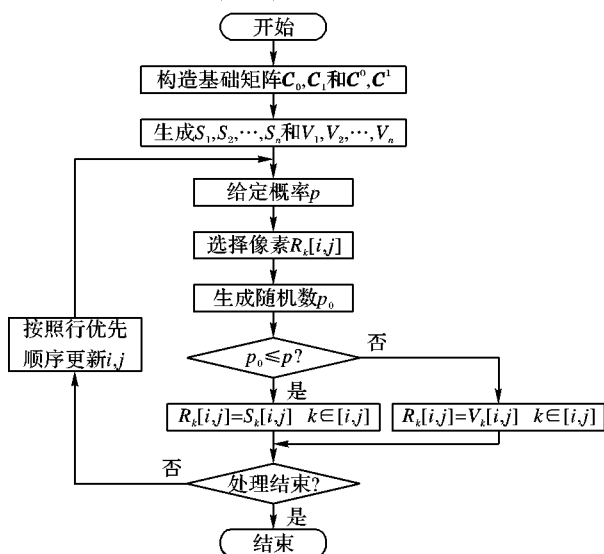


图1 概率法防欺骗视觉密码方案流程

1.4 方案分析

1.4.1 性质分析

设原秘密图像的一个白(黑)像素在共享份 S_1, S_2, \dots, S_n 中任意 q 个叠加后的汉明重量为 $w(S_0)(w(S_1))$, 在 R_1, R_2, \dots, R_n 中任意 q 个叠加后的汉明重量为 $w(S_0')(w(S_1'))$; 原验证图像的一个白(黑)像素在共享份 V_1, V_2, \dots, V_n 中任意 q 个叠加后汉明重量为 $w(V_0)(w(V_1))$, 在 R_1, R_2, \dots, R_n 中任意 q 个叠加后的汉明重量为 $w(V_0')(w(V_1'))$, 则必有 $w(S_i') = p \cdot w(S_i) + (1-p) \cdot w(V_i), w(V_i') = p \cdot w(S_i) + (1-p) \cdot w(V_i)$, 其中 $i \in \{0, 1\}, j \in \{0, 1\}, q$ 为共享份的数目, 该方案有如下性质。

1) 当 $q < k'$ 时, 共享份叠加后得不到任何图像的信息。

证明 当 $q < k'$ 时, $w(S_0) = w(S_1), w(V_0) = w(V_1)$, 故 $w(S_0') = w(S_1'), w(V_0') = w(V_1')$, 对于原秘密图像和验证

图像中的黑白像素在叠加共享份时视觉表现上相同, 不会显示任何图像信息。

2) 当 $k' \leq q < k$ 时, 共享份叠加后得到验证图像的信息, 得不到秘密图像的信息。

证明 当 $k' \leq q < k$ 时, 有 $w(S_0) = w(S_1), w(V_0) < w(V_1)$ 。对于验证图像中的黑像素有 $w(V_1') = p \cdot w(S_i) + (1-p) \cdot w(V_i)$, 对于白像素有 $w(V_0') = p \cdot w(S_i') + (1-p) \cdot w(V_0')$, 故 $w(V_0') < w(V_1')$ 。原验证图像的黑白像素在叠加共享份中存在对比差异, 显示出验证图像信息。

对于秘密图像中的黑像素有 $w(S_1') = p \cdot w(S_1) + (1-p) \cdot w(V_i)$, 对于白像素有 $w(S_1') = p \cdot w(S_0) + (1-p) \cdot w(V_i)$, 此时 $w(S_1')$ 和 $w(S_0')$ 取值均为 $p \cdot w(S_1) + (1-p) \cdot w(V_0)$ 或者 $p \cdot w(S_1) + (1-p) \cdot w(V_1)$, 且取上述二值的概率相同, 故原秘密图像中的黑白像素在叠加共享份中视觉表现上相同, 不会显示原秘密图像的任何信息。

3) 当 $k \leq q \leq n$ 时, 共享份叠加后得到秘密图像的信息, 得不到验证图像的信息。

证明 当 $k \leq q \leq n$ 时, $w(S_0) < w(S_1), w(V_0) = w(V_1)$ 。对于验证图像中的黑像素有 $w(V_1') = p \cdot w(S_i) + (1-p) \cdot w(V_i)$, 对于白像素有 $w(V_0') = p \cdot w(S_i) + (1-p) \cdot w(V_0)$, 此时 $w(V_1')$ 和 $w(V_0')$ 取值均为 $p \cdot w(S_1) + (1-p) \cdot w(V_i)$ 或者 $p \cdot w(S_0) + (1-p) \cdot w(V_i)$, 且取上述二值的概率相同, 故原验证图像中的黑白像素在叠加共享份中视觉表现上相同, 不会显示原验证图像的任何信息。

对于秘密图像中的黑像素有 $w(S_1') = p \cdot w(S_1) + (1-p) \cdot w(V_i)$, 对于白像素有 $w(S_0') = p \cdot w(S_0) + (1-p) \cdot w(V_i)$, 此时 $w(S_0') < w(S_1')$, 原秘密图像的黑白像素在叠加共享份中存在对比差异, 显示出秘密图像信息。

1.4.2 相对差分析

设分享秘密图像的方案中相对差为 α_s , 分享验证图像的方案中相对差为 α_v , 根据性质分析可得该防欺骗视觉密码方案的相对差 $\alpha = p \cdot \alpha_s + (1-p) \cdot \alpha_v$, 当有 $q(k \leq q \leq n)$ 个叠加时, 得不到验证图像的信息, 故此时 $\alpha_v = 0, \alpha = p \cdot \alpha_s, 0 < \alpha < 1$ 。显然, 可以通过控制 p 来控制秘密图像的恢复效果。

2 仿真实验与结果分析

用本文方案构造一个 $(2, 4, 4)$ 防欺骗视觉密码方案。四个共享份叠加时, 显示秘密信息, 任意两个或三个共享份叠加时, 显示验证信息。

首先构造秘密图像的共享份 S_1, S_2, \dots, S_n 和验证图像的共享份 V_1, V_2, \dots, V_n , 其中基础矩阵分别为:

$$C_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

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

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

在上述基础矩阵中,扩展度分别为 $m' = 8, m'' = 6$, 则该防欺骗视觉密码方案的扩展度 $m = \lceil \sqrt{\max(m', m'')} \rceil^2 = 9$, 将 $C_0(C_1)$ 和 $C^0(C^1)$ 分别用全为 1 的列补足 9 列, 并分别生成秘密图像的共享份 S_1, S_2, \dots, S_n 和分享验证图像的共享份 V_1, V_2, \dots, V_n 。

然后分别取 $p = 0.6, p = 0.5$, 根据概率法模型, 得到该防欺骗视觉密码方案共享份和恢复效果如图 1 所示。



图 2 概率法防欺骗视觉密码方案实际效果

图 3 给出了四种防欺骗视觉密码方案, 现将本文两方案与其他两方案对比如下:

1) 从构造难易程度来说, 文献[11]方案需要将一个普通(4,4)方案和三个改进(3,3)方案的基础矩阵交叉连接。文献[12]方案的基础矩阵在构造过程中, 需要首先将(2,4)方案和(4,4)方案的基础矩阵连接, 然后再与一个(4,4)方案的基础矩阵交叉连接。本文方案只需构造一个(4,4)方案和非强存取结构, 不需进行矩阵的交叉连接, 构造更为简单。

2) 从像素扩展度上来说, 由于文献[11]和[12]的方案在构造过程中, 采用的是矩阵交叉连接的方式, 像素扩展度较大, 分别为 24 和 16, 而本文方案在构造过程中利用概率选取秘密图像和验证图像共享份中的像素, 因此像素扩展度较上述两方案会有大幅减少, 便于共享份的存储和传输。

3) 从相对差上来看, 根据本文 1.4.2 节中的相对差分析, 当 $p = 0.6$ 时, $\alpha = 1/15$, 是四个方案中最大的, 因此该方案恢复出来的秘密图像更清晰, 对比更明显, 同时, 在保证验证图像清晰的前提下, 本文方案可以通过控制 p 来选择合适的相对差, 这是其他方案所不具备的优点。

4) 从查找欺骗者上来看, 文献[11]方案只有在拥有三张正确的共享份时才可以恢复出验证图像, 所以只能找出四个参与者中的一个欺骗者; 而本文方案只需拥有任意两张正确的共享份就可以恢复出验证图像, 而且在确认一个共享份真实性的前提下, 可以找出多个欺骗者, 在一定程度上可以抵制共谋欺骗。

3 结语

针对防欺骗视觉密码方案扩展度较大的问题, 本文构造了一种基于概率法的防欺骗视觉密码方案。通过参与者所拥有的共享份相互叠加, 无需其他额外信息, 就可以发现其中的欺骗者。该方案的像素扩展度小, 相对差大, 便于共享份的存储和秘密图像信息的恢复。同时, 在保证验证图像清晰的前提下, 本方案可以通过控制 p 来选择合适的调整秘密图像的恢复效果。

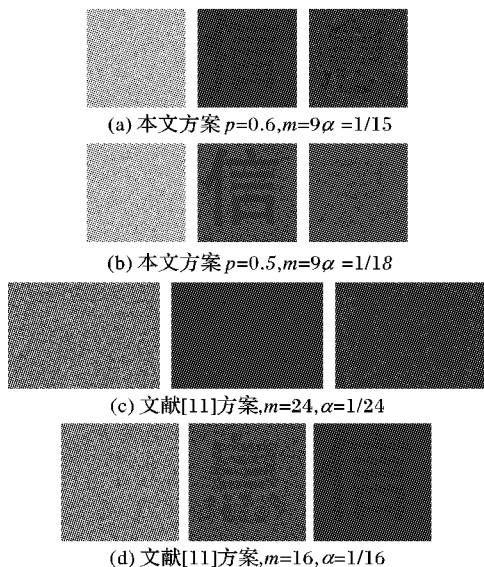


图 3 四种防欺骗视觉密码方案效果对比

参考文献:

- [1] NAOR M, SHAMIR A. Visual cryptography[EB/OL]. [2008-10-23]. <http://people.csail.mit.edu/rivest/voting/papers/Naor-Shamir-VisualCryptography.ps>.
- [2] 房礼国. 视觉密码参数优化及外形失真研究[D]. 郑州: 信息工程大学电子技术学院, 2006.
- [3] 房礼国, 郁滨. 一种基于排列的(2, n)可视门限方案[J]. 计算机工程, 2007, 33(9): 157-159.
- [4] 房礼国, 郁滨. 一种像素扩展度最优的(2, n)可视门限方案[J]. 电子技术学院学报, 2006, 18(7): 11-15.
- [5] ATENIESE G, BLUNDO C, De SANTIS A, et al. Visual cryptography for general access structures[J]. Information and Computation, 1996, 129(2): 86-106.
- [6] 邱善福. 新视觉化密码编码法的分析[D]. 台湾: 台湾国立交通大学资讯科学研究所, 2001.
- [7] DROSTE S. New results on visual cryptography[EB/OL]. [2008-10-25]. <http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C96/401.PDF>.
- [8] HOU Y C, TU S F. A visual cryptographic technique for chromatic images using multi-pixel encoding method[J]. Journal of Research and Practice in Information Technology, 2005, 37(2): 179-182.
- [9] 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.
- [10] 郭洁, 颜浩, 刘妍, 等. 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.
- [11] 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会议论文集. 合肥: 中国科学技术大学出版社, 2007: 1335-1339.
- [12] 徐晓辉. 可防欺骗的视觉密码研究[D]. 郑州: 信息工程大学电子技术学院, 2008.