文章编号：2095-2163(2022)10-0154-04 中图分类号：TP309.7 文献标志码：A

一种具有身份验证能力的防欺骗视觉密码方案

李长悦，王洪君
（吉林师范大学 数学学院，吉林 四平 136000）

摘 要：本文给出了一种分享为有意义图像的视觉密码方案，利用参与者和其他参与者的分享图像叠加能否恢复出验证图像来实现参与者真实性检验，分享图像不易引起攻击者的怀疑，并且还检验了其他参与者的真实性。该方案中分享图像都有意义且任意 2 个分享图像的叠加结果为验证图像，用来验证参与者身份真实性，不能泄露秘密图像的任何信息。实验证实了所给方案的有效性。

关键词：视觉密码；防欺骗；分享；秘密图像；验证图像

An anti-cheating visual cryptography scheme for authentication

LI Changyue, WANG Hongjun
(College of Mathematics, Jilin Normal University, Siping Jilin 136000, China)

【Abstract】 This paper proposes a visual cryptography scheme for sharing meaningful images. The scheme verifies the participants′ authenticity by superimposing the share of participants and the share of other participants together to restore the verified images . After that, the sharing images are not easy to arouse the suspicion of the attacker and in this way the authenticity of participants can also be checked. In this scheme, the sharing images are meaningful and the result of superimposing any two shared images is the verification image, which is used to verify the authenticity of the participants, and can not reveal any information of the secret image. The experiment has proved the effectiveness of the scheme.

【Key words】 visual cryptography; anti-cheating; share; secret image; authentication image

0 引 言

视觉密码（Visual Cryptography, VC）是 Naor 和 Shamir[1]在 1994 年的欧洲密码学年会上提出一种只需要人类视觉系统就可以恢复秘密的新的密码方案，基于方案的便捷性和保密性被广泛应用。在对信息进行加密过程中，主要是对秘密图像（secret image）用 Matlab 进行处理，得到秘密图像的若干分享份（share），而这些子分享份一般不具有明显的特征，攻击者无法直接识别出秘密信息。在恢复秘密过程中，通过将分享图像进行叠加，利用人的视觉系统就可以直接读出其中包含的秘密信息。视觉密码受到多方关注，目前在数学、密码学、计算机等相关领域均有涉及，其解密过程安全、简单、便捷并且可信度高，研究价值较大，因而有着广阔的研究和发展前景。

VCS（Visual Cryptography Scheme）方案假设参与者是诚实可信的，但是事实上秘密信息在传递过程中容易受到恶意攻击者通过篡改、隐瞒等欺骗手段破坏秘密信息的传递，如一些不诚实参与者会出示经过处理后的假的分享份来欺骗其他参与者，或者非法参与者冒充合法参与者进行信息干扰，并且大多欺骗都是发生在分享无意义的情况下。为了解决这类影响秘密信息传输的因素，学者们开始对防欺骗视觉密码[2]进行实验研究。文献[3]针对像素扩展问题，提出一种目标优化模型，并利用该模型构造了一种像素不扩展的防欺骗视觉密码方案。文献[4]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。文献[5]针对视觉密码存在的欺骗问题，提出了一种可防欺骗视觉密码方案，利用排列组合的方法构造分享验证图像的基础矩阵，使得参与者将自己的验证分享份和其他参与者的秘密分享份进行叠加，从而恢复出该参与者私有的验证图像。一般地，欺骗行为大致分为内部欺骗和外部欺骗，内部欺骗主要是由参与者以自己的分享份为依据，伪造出和真实分享份类似的分享份，从而达到欺骗目的。从参与者中欺骗者的数量来看，欺骗分为单独欺骗和共谋欺骗两种。其中，单独欺骗是指在恢复秘密过程中，某一个参与者出示了经过伪造的共享份；共谋欺骗是指部分参与者联合起来欺骗诚实参与者，

作者简介：李长悦（1996-），女，硕士研究生，主要研究方向：计算数学；王洪君（1965-），男，博士，教授，硕士生导师，主要研究方向：计算数学。
通讯作者：王洪君 Email：jlnuwhj@ sina.com

收稿日期：2022-03-07

做法是根据推测出的基矩阵来伪造共享份[6]。本文构造出一种具有身份验证能力的基于随机矩阵的视觉密码方案。

本文在文献[1]的视觉密码扩展方案的基础上，给出了一种分享图像为有意义图像的视觉密码方案，将分享图像各分享份隐藏在有意义的图像中，并采用或运算，利用各个参与者分享图像互相叠加能否恢复出验证图像来检验参与者的真实性，由于分享图像就是一幅有意义的图像，不易引起攻击者的怀疑并且还检验了其他参与者的真实性。该方案中任意 2 个分享图像的叠加结果为验证图像，用来验证参与者身份真实性，并且不会泄露秘密图像的任何信息，而 3 个分享图像的叠加可以恢复出秘密图像。

1　方案构建方法

通过对文献[1]视觉密码扩展方案的运算结果进行研究可以发现，如果分享图像像素点为白色，其对应的 4 个子像素中有 2 个“0”，如果分享图像像素点为黑色，其对应的 4 个子像素中只有一个“0”。如果秘密图像为白色像素，基本矩阵 2 行叠加的结果是 4 个子像素中只有一个“0”；如果秘密图像为黑色像素，基本矩阵 2 行叠加的结果是 4 个子像素中全是“1”。基于这样的思想，对于本文的视觉密码方案，考虑如果分享图像两两叠加像素点为白色，对应的基本矩阵的相应行至少有 2 个“0”；如果分享图像两两叠加像素点为黑色，对应的基本矩阵的相应行至少有一个“0”。基本矩阵的任意 2 行叠加有相同个数的“0”，这样就保证了任意 2 个分享图像叠加的结果是不可区分的。如果恢复出的秘密图像像素为白色，则基本矩阵的 3 行叠加的结果含有一个“0”；如果恢复出的秘密图像像素为黑色，基本矩阵 3 行叠加的结果就全是“1”[7]。基于此，可以构建的矩阵具体如下：

$$\boldsymbol{w}_{00}=\begin{pmatrix}1&1&1&1&1&1&0&0&0&1&1&1&1&0&0\\1&1&1&0&0&1&1&1&0&1&1&1&0&1&0\\0&0&0&1&1&1&1&1&1&1&1&1&0&1&1&0\end{pmatrix}$$

$$\boldsymbol{w}_{10}=\begin{pmatrix}1&1&1&1&1&1&0&0&0&1&1&1&1&0&0\\1&1&1&0&0&0&1&1&1&1&1&1&0&1&0\\0&0&0&1&1&1&1&1&1&1&1&1&0&1&1&0\end{pmatrix}$$

$$\boldsymbol{b}_{00}=\begin{pmatrix}1&1&1&1&1&1&1&0&0&1&1&1&1&0&0\\1&1&1&1&1&1&0&1&0&1&1&1&0&1&0\\1&1&1&1&1&1&0&0&1&1&1&1&0&1&1&0\end{pmatrix}$$

$$\boldsymbol{b}_{10}=\begin{pmatrix}1&1&1&1&1&1&1&0&0&1&1&1&1&0&0\\1&1&1&1&1&0&0&1&1&1&1&1&0&1&0\\1&1&1&0&0&1&1&1&1&1&1&1&0&1&1&0\end{pmatrix}$$

$$\boldsymbol{w}_{01}=\begin{pmatrix}1&1&1&1&1&1&0&0&0&1&1&1&1&0&0\\1&1&1&0&0&1&1&1&0&1&1&1&0&1&0\\1&1&0&0&1&1&1&1&0&1&1&1&1&0&0&1&0\end{pmatrix}$$

$$\boldsymbol{w}_{11}=\begin{pmatrix}1&1&1&1&1&1&0&0&0&1&1&1&1&0&0\\1&1&1&0&0&0&1&1&1&1&1&1&0&1&0\\0&0&0&1&1&1&1&1&1&1&1&1&0&0&1&0\end{pmatrix}$$

$$\boldsymbol{b}_{01}=\begin{pmatrix}1&1&1&1&1&1&1&0&0&1&1&1&1&0&0\\1&1&1&1&1&1&0&1&0&1&1&1&0&1&0\\1&1&1&1&1&1&1&0&0&1&1&1&1&0&0&1&0\end{pmatrix}$$

$$\boldsymbol{b}_{11}=\begin{pmatrix}1&1&1&1&1&1&1&0&0&1&1&1&1&0&0\\1&1&1&1&1&0&0&1&1&1&1&1&0&1&0\\1&1&1&0&0&1&1&1&1&1&1&1&0&0&1&0\end{pmatrix}$$

其中，矩阵名称中的第一个字符“w”或“b”表示掩盖图像颜色，第二个字符“0”或“1”表示分享图像两两叠加的颜色，最后一个字符“0”或“1”表示秘密图像的颜色。

2　算法实现

算法输入　一幅掩盖图像，一幅验证图像，一幅秘密图像

算法输出　3 幅分享图像

算法步骤：

(1)产生一个关于向量 (1,2,3,4,5,6,7,8,…,16) 的随机置换 r。

(2)如果秘密图像像素 f 是一个白色像素，那么对矩阵 $\boldsymbol{w}_{00},\boldsymbol{w}_{10},\boldsymbol{b}_{00},\boldsymbol{b}_{10}$ 之一做列置换 r，得到矩阵 $\boldsymbol{A}_1、\boldsymbol{A}_2、\boldsymbol{A}_3$；如果秘密图像像素 f 是一个黑色像素，那么对 $\boldsymbol{w}_{01}、\boldsymbol{w}_{11}、\boldsymbol{b}_{01}、\boldsymbol{b}_{11}$ 之一做列置换 r，得到矩阵 $\boldsymbol{A}_1、\boldsymbol{A}_2、\boldsymbol{A}_3$。

(3)对于 $\boldsymbol{A}_i(1\leqslant i\leqslant 3)$，把矩阵 $\boldsymbol{A}_i$ 分配给第 i 个参与者。

(4)第 $i(1\leqslant i\leqslant 3)$ 个参与者得到分享份 $\boldsymbol{B}_i$。

(5)参与者的分享份两两进行叠加得到验证图像。

(6)全部参与者的分享份叠加产生秘密图像。

3　实验结果对比及分析

实验中选用图像如图 1 所示，实验结果如图 2、图 3 所示。

(a) 掩盖图像　　(b) 验证图像　　(c) 秘密图像

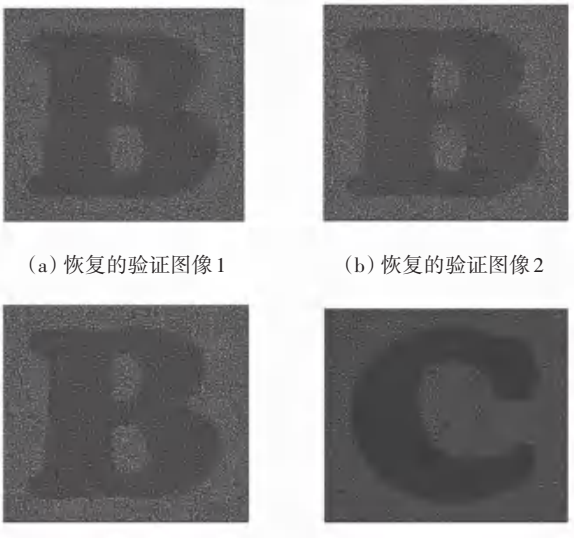
图 1　实验图像

Fig. 1　Experimental images

(a) 分享图像 1 (b) 分享图像 2 (c) 分享图像 3

图 2 分享图像

Fig. 2 Shared images



(a) 恢复的验证图像 1 (b) 恢复的验证图像 2

(c) 恢复的验证图像 3 (d) 恢复的秘密图像

图 3 实验结果

Fig. 3 Experimental results

从实验结果可以看出,3 个通过掩盖图像产生的分享图像是有意义的二值图像,其中任意 2 个分享图像叠加产生验证图像而不能产生秘密图像,使得秘密图像的安全性、隐蔽性大大提升,并且只有 3 个分享图像叠加在一起的情况下才可以恢复出秘密图像。因此,参与者可以通过验证来判断其他参与者是否诚实。Shyu[8] 所给方案分别为 (2,2) 方案和 (k,n) 方案,恢复图像的对比度为 $\frac{1}{2}$,但所生成的分享图像无意义。颜浩等人[9] 提出了一种可以检测出一个欺骗者的 (k,n) 门限的可视密码方案,但生成的分享图像无意义。Chen 等人[10] 给出了基于网格的 (2,2) 分享方案,掩盖图像颜色互补。Guo 等人[11] 提出的 (n,n) 门限方案,分享图像有意义,任意图像均可为掩盖图像,不受影响。Monoth 等人[12] 给出用户友好的(2,2)多秘密分享方案,实现 3 个不同秘密图像的分享。每个分享图像都呈现掩盖图像的内容,可以把秘密图像分辨出来。Chiua 等人[13] 给出的 (k,n) 门限视觉密码方案,可以对分享图像和恢复图像的对比度进行调节,掩盖图像颜色互补。张舒等人[14] 提出一种改进的防欺骗视觉密码方案,能同时发现分发者和参与者的欺骗行为。Yang 等人[15] 提出了一种需要特定的参与者和其它参与者来恢复秘密图像的视觉密码方案。方案比较结果见表 1。

表 1 方案比较

Tab. 1 Comparison of schemes

方案	秘密数	分享数	分享图像是否有意义	是否具有验证功能
文献[8]	1	2	否	否
文献[9]	1	3	否	是
文献[14]	1	3	否	是
文献[15]	1	4	否	是
本文研究	1	3	是	是

4 结束语

本文构造了一个基于随机数的防欺骗视觉密码,利用或运算来实现真实性检验,由于大多欺骗都是发生在分享无意义的情况下,本方案在保证分享图像有意义的同时验证了参与者的真实性,并使恢复的秘密图像更加清晰。

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography[M]//De SANTIS A. Advances in Cryptology-Eurocrypt'94. Eurocrypt 1994. Lecture Notes in Computer Science. Berlin/Heidelberg: Springer, 1994, 950:1-12.

[2] 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(06):126-128.

[3] 王益伟,郁滨付,正欣,等. 像素不扩展的防欺骗视觉密码方案研究[J]. 信息工程大学学报, 2011,12(02):149-153.

[4] 郁滨,王益伟,房礼国,等. 基于概率法的防欺骗视觉密码方案[J]. 计算机应用, 2009,29(07):1782-1784.

[5] 陈勤,彭文芳,徐坤,等. 基于排列组合的可防欺骗视觉密码方案[J]. 计算机应用研究,2011,28(01):318-321,325.

[6] 郁滨,付正欣,沈刚,等. 视觉密码[M]. 安徽:中国科学技术大学出版社,2014.

[7] 王洪君,张慧,李静雪,等. 一种具有身份验证能力的视觉密码方案[J]. 沈阳师范大学学报(自然科学版), 2013, 31(03): 397-400.

[8] SHYU S J. Image encryption by random grids [J]. Pattern Recognition, 2007,40(3): 1014-1031.

[9] 颜浩,甘志,陈克非. 可防止欺骗的可视密码分享方案[J]. 上海交通大学学报,2004,38(01):107-110.

[10] CHEN T H, TSAO K H. User-friendly random-grid-based visual secret sharing[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 3 (11): 1693-1703.

[11] GUO Teng, LIU Feng, WU Chuankun. k out of k extended visual cryptography scheme by random grids [J]. Signal Processing (Elesvier), 2014, 94(1): 90-101.

(下转第 162 页)