文章编号:2095-2163(2019)05-0131-04 中图分类号:TN918.4 文献标志码:A

# 基于随机网格的视觉密码改进方案

曹 宇,王洪君,李 莹
(吉林师范大学 计算机学院,吉林 四平 136000)

**摘 要:** 针对视觉密码扩展度大的问题,提出了一种基于随机网格的视觉密码改进方案,所给方案不同于已有的基于随机网格的视觉密码方案,其在对秘密图像分享的过程中首先根据分享方案的不同产生多个与原始图像大小相同的分享矩阵,然后根据秘密图像像素颜色的不同利用分享矩阵产生分享图像,分享图像的叠加可以恢复秘密图像。通过实验对所给的分享方案进行验证,实验结果证实了所给方案的有效性,所恢复的秘密图像更清晰。

**关键词:** 随机网格;视觉密码;分享图像;秘密图像

## An improved visual cryptography scheme based on random grid

CAO Yu, WANG Hongjun, LI Ying
(College of Computer Science, Jilin Normal University, Siping Jilin 136000, China)

**【Abstract】** To solve the problem of pixel expansion, a visual cryptography scheme based on grid is proposed. The proposed scheme is different from the existing grid based visual cryptography scheme. In the process of secret image sharing, multi sharing matrices with the same size as the original image are firstly generated according to the scheme. Depending on the pixel color of the secret image and the sharing matrix, shares are generated. The superimposition of shared image could restore secret images. Experimental results demonstrate that the restored secret image is clearer, therefore verify the effectiveness of the proposed scheme.

**【Key words】** random grid; visual cryptography; sharing image; secret image

## 0 引 言

视觉密码把一幅秘密图像分割成多幅分享图像,多幅或全部分享图像的叠加可以恢复秘密图像,其解密过程不需要复杂的数学计算,只需人的一双眼睛就可实现[1]。然而视觉密码在对秘密图像进行加密时存在像素扩展问题,生成的分享图像比原始图像尺寸要大。这个缺点导致存储空间浪费,图像扭曲变形,分享图像不便携带。

随着视觉密码研究的深入,学者们提出了许多解决像素扩展问题的方法,其中大部分方案利用了概率视觉密码的思想。Ito 等人[2]和 Yang [3]利用黑色像素在黑色和白色区域出现概率的不同去区分恢复图像中的黑色和白色区域,黑色区域中黑色像素占的比例大,白色区域中黑色像素所占比例小,并且提出适用于二值图像的像素不扩展的方法。然而概率的随机性意味着黑白像素的分布不是很均匀,恢复的秘密图像效果差。Tu 等人[4]利用了 Ito 等人[2]的方法,但利用秘密图像中的多个连续像素作为加密单位,使得灰度级秘密图像产生大小不变的分享图像。Lin 等人[5]给出了一个图像大小不变的多秘密分享策略。Kafri 等人[6]提出随机网格可视秘密分享方法 RGVSS (random grid visual secret sharing),并且得到了更多的关注,RGVSS 方法的最大好处是分享图像没有像素扩展。随后,Shyu[7]扩展了 Kafri 等人[6]的 RGVSS 模型,提出了像素不扩展视觉密码方案。文献[8-18]也对像素不扩展方案进行了研究。传统的视觉密码方案和 RGVSS 所产生的分享图像是无意义的,这会给那些参与多个秘密分享任务的参与者带来管理上的问题。此外,一个毫无意义的图像的传输可能引起外界的怀疑,无形中就降低分享图像的安全性。Chen 等人[15]和 Lou 等人[16]分别给出了用户友好的像素不扩展的视觉密码方案。

针对视觉密码的像素扩展问题,提出了一种基于随机网格的视觉密码改进方案。此次研发方案产生的分享图像与原始秘密图像具有相同的大小,不存在像素扩展问题,同时该方案克服了基于随机网

**基金项目:** 国家自然科学基金(31070224)。

**作者简介:** 曹 宇(1991-),男,硕士研究生,助教,主要研究方向:信息安全、密码学、视觉密码;王洪君(1965-),男,博士,教授,主要研究方向:信息安全、密码学、视觉密码;李 莹(1994-),女,硕士研究生,主要研究方向:信息安全、密码学。

**通讯作者:** 王洪君 Email:jlnuwhj@sina.com

**收稿日期:** 2019-07-25

格视觉密码的像素分布随机性的弱点,使得分享图像黑白像素分布更均匀,恢复图像效果更好。

## 1 基于随机网格的视觉密码

Kafri 等人[6]首先提出基于随机网格的可视秘密分享方法,分享图像的每一像素被看成是一个网格,第一幅分享图像的网格颜色随机分配。当第一幅分享图像确定下来之后,根据秘密图像像素的颜色,第二幅分享图像的网格颜色与第一幅图像中对应的网格颜色或为相同、或为互补。文献[7,13,17,18]扩展了 Kafri 等人[7]方案,提出多个像素不扩展视觉密码方案。Kafri 等人[6]给出了具有不同对比度的 3 种算法,其中的一个算法模型见表1。表1中,白色方块表示白色像素,黑色方块表示黑色像素。

**表1 (2,2)基于随机网格的秘密分享方案**

**Tab. 1 A(2,2) visual cryptography scheme based on random grid**

| 秘密 | 概率/% | 分享1 | 分享2 | 叠加结果 |
|---|---|---|---|---|
| □ | 50 | □ | □ | □ |
| | 50 | ■ | ■ | ■ |
| ■ | 50 | □ | ■ | ■ |
| | 50 | ■ | □ | ■ |

## 2 基于随机网格的(2,2)视觉密码改进方案

传统的视觉密码方案存在一个基础矩阵,基础矩阵决定了分享图像中的黑白像素比例是固定的。给出一种基于传统视觉密码思想的(2,2)像素不扩展方案,其中利用了视觉密码中的基础矩阵,保证了分享图像中黑白像素分布均匀。对(2,2)视觉密码方案,保证黑白像素各占 50%,并且连续的 2 个像素中一定有一个黑像素和一个白像素。对此研发算法可做阐释论述如下。

**输入:**一幅 $L\times H$ 的二值秘密图像 $\boldsymbol{S}$

**输出:**两幅 L×H 的分享图像 $\boldsymbol{R}_1$ 和 $\boldsymbol{R}_2$

**Step 1** 利用文献[1]中的基础矩阵,生成 2 个 $L\times H$ 的二值矩阵 $\boldsymbol{M}_0$ 和 $\boldsymbol{M}_1$。其中,$\boldsymbol{M}_0$ 随机生成。用 $\boldsymbol{M}_k(i,j)(k=0,1)$ 表示矩阵 $\boldsymbol{M}_k$ 第 $i$ 行第 $j$ 列元素的值($k=0,1$);用 $\boldsymbol{M}_k(i,j..j+1)(k=0,1)$ 表示第 $i$ 行第 $j$ 列和第 $j+1$ 列元素的值。用数字 0 表示像素颜色为白色,用数字 1 表示像素颜色为黑色。此处运算拟用到如下数学公式:

$$\boldsymbol{M}_0(i,j..j+1)=\begin{cases}(0,1), & 0.5\leqslant r<1;\\ (1,0), & 0<r<0.5.\end{cases}$$

$$1\leqslant i\leqslant L,1\leqslant j\leqslant H/2, \tag{1}$$

$$\boldsymbol{M}_1(i,j..j+1)=\begin{cases}(1,0),\boldsymbol{M}_0(i,j..j+1)=(0,1);\\ (0,1),\boldsymbol{M}_0(i,j..j+1)=(1,0).\end{cases}$$

$$1\leqslant i\leqslant L,1\leqslant j\leqslant H/2. \tag{2}$$

其中,$r$ 为随机数。

**Step 2** 对秘密图像 $\boldsymbol{S}$ 的每一个像素 $\boldsymbol{S}(i,j)$ 进行编码,生成 2 幅分享图像 $\boldsymbol{R}_1$ 和 $\boldsymbol{R}_2$。此处运算拟用到如下数学公式:

$$\boldsymbol{R}_1(i,j)=\boldsymbol{M}_0(i,j),\ 1\leqslant i\leqslant L,1\leqslant j\leqslant H, \tag{3}$$

$$\boldsymbol{R}_2(i,j)=\begin{cases}\boldsymbol{M}_0(i,j), & \boldsymbol{S}(i,j)=0;\\ \boldsymbol{M}_1(i,j), & \boldsymbol{S}(i,j)=1.\end{cases}$$

$$1\leqslant i\leqslant L,\quad 1\leqslant j\leqslant H. \tag{4}$$

由于对秘密图像黑色像素的分享的基础矩阵中黑白像素是互补的,因此,在黑色像素的分享方案中无论子像素是什么颜色,2 个像素叠加都会产生黑色。而对于白色像素,其基础矩阵中 2 个分享子像素的颜色是相同的,因此对于秘密图像的白色区域,分享图像叠加后有 50% 的白色像素变为黑色像素,分享图像叠加后黑白区域区分明显,对比度为 1/2。

## 3 基于随机网格的(3,3)视觉密码改进方案

上节(2,2)视觉密码方案可以扩展为像素不扩展(3,3)方案。对此研发算法可做阐释论述如下。

**输入:**一幅 $L\times H$ 的二值秘密图像 $\boldsymbol{S}$。

**输出:**三幅 $L\times H$ 的分享图像 $\boldsymbol{R}_1$,$\boldsymbol{R}_2$ 和 $\boldsymbol{R}_3$。

**Step 1** 利用基础矩阵 $\boldsymbol{B}^0$ 和 $\boldsymbol{B}^1$,生成 6 个 L×H 的二值矩阵 $\boldsymbol{M}_0^1$、$\boldsymbol{M}_0^2$、$\boldsymbol{M}_0^3$、$\boldsymbol{M}_1^1$、$\boldsymbol{M}_1^2$ 和 $\boldsymbol{M}_1^3$。这里,$\boldsymbol{B}^0=\begin{bmatrix}1&1&0&0\\1&0&1&0\\0&1&1&0\end{bmatrix}$,$\boldsymbol{B}^1=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}$。其中,$\boldsymbol{B}^0$ 用于加密白色像素,$\boldsymbol{B}^1$ 用于加密黑色像素。此处运算拟用到如下数学公式:

$$\boldsymbol{M}_0^k(i,4*j-3..4*j)=\boldsymbol{B}^0(k,c), \tag{5}$$

$$\boldsymbol{M}_1^k(i,4*j-3..4*j)=\boldsymbol{B}^1(k,c), \tag{6}$$

其中,$1\leqslant i\leqslant L,1\leqslant j\leqslant H/4,1\leqslant k\leqslant 3,c=\pi([1,2,3,4])$,函数 $\pi(\boldsymbol{r})$ 实现对向量 $\boldsymbol{r}$ 进行随机列变换。

**Step 2** 对秘密图像 $\boldsymbol{S}$ 的每一个像素 $\boldsymbol{S}(i,j)$ 进行编码,生成 3 幅分享图像 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$ 和 $\boldsymbol{R}_3$。此处拟用到如下数学公式:

$$\boldsymbol{R}_k(i,j)=\begin{cases}\boldsymbol{M}_0^k(i,j), & \boldsymbol{S}(i,j)=0;\\ \boldsymbol{M}_1^k(i,j), & \boldsymbol{S}(i,j)=1.\end{cases} \tag{7}$$

其中,$1\leqslant i\leqslant L,1\leqslant j\leqslant H,1\leqslant k\leqslant 3$。

算法产生的分享图像中黑白像素各占 50%，并且分布均匀，克服了黑白像素随机分布造成的像素分布不均匀的缺点。任何 2 个分享叠加结果图像的黑白像素比为 3:1，并且分布均匀，不能区分原始像素的颜色。3 幅分享图像叠加，对于白色像素有 1/4 叠加后仍保持白色，有 3/4 叠加后转变为黑色；对于黑色像素叠加后仍为黑色，恢复图像的对比度为 0.25。因而可以区分原始图像的黑色区域和白色区域，即可识别出原图像的信息。

## 4　实验与比较

### 4.1　实验结果

对前述(2,2)和(3,3)视觉密码改进方案和文献[6-8,13,17-18]中的设计方案进行实验，研究选用软件为 Matlab7.0。本文实验结果演示详见如下。

(1)实验 1。对图 1 所示的秘密图像利用文献[6-7]的(2,2)方案和本文研发的(2,2)改进方案进行实验，实验结果分别如图 2 和图 3 所示。文献[6]的结果类似于文献[7]，从实验结果可以看出，本文提出的方案恢复图像更清晰。

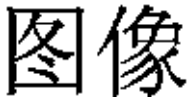
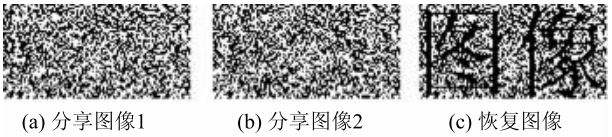



**图 1　秘密图像**

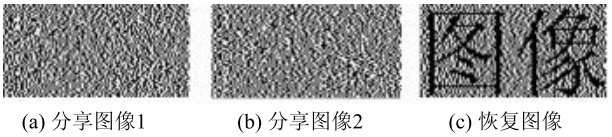
**Fig. 1　Secret image**



(a) 分享图像1　(b) 分享图像2　(c) 恢复图像
(a) Sharing image 1　(b) Sharing image 2　(c) Recovery image

**图 2　文献[6-7]所给(2,2)方案的实验结果**

**Fig. 2　Experiment result of (2,2) scheme presented in Ref. [6-7]**



(a) 分享图像1　(b) 分享图像2　(c) 恢复图像
(a) Sharing image 1　(b) Sharing image 2　(c) Recovery image

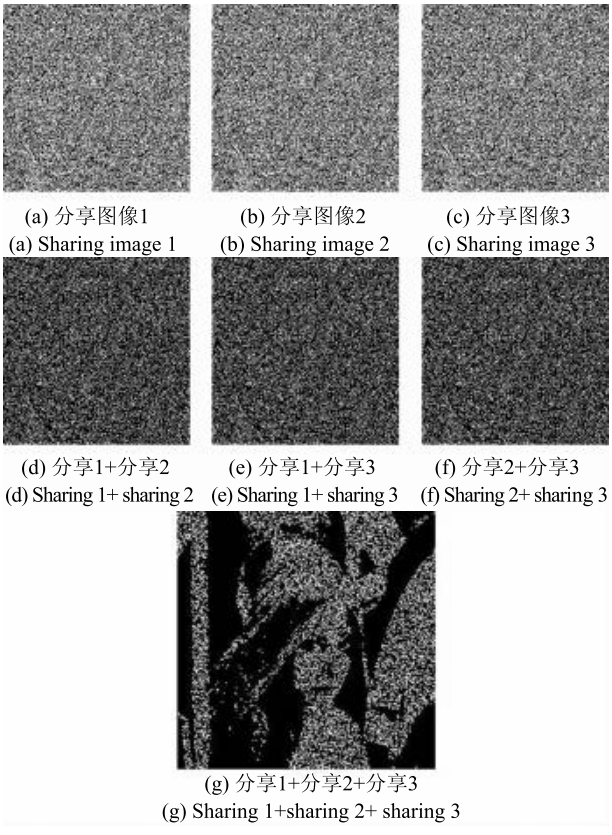
**图 3　所提出的(2,2)方案实验结果**

**Fig. 3　Experiment result of proposed (2,2) scheme**

(2)实验 2。对图 4 所示的 256×256 像素的秘密图像利用文献[8,13,17-18]的(3,3)方案和本文研发的(3,3)改进方案进行实验，实验结果分别如图 5 和图 6 所示。文献[8,17-18]的结果和文献[13]类似，从实验结果可以看出，本文提出的方案恢复图像效果更好。

**图 4　秘密图像**

**Fig. 4　Secret image**



(a) 分享图像1　(b) 分享图像2　(c) 分享图像3
(a) Sharing image 1　(b) Sharing image 2　(c) Sharing image 3

(d) 分享1+分享2　(e) 分享1+分享3　(f) 分享2+分享3
(d) Sharing 1+ sharing 2　(e) Sharing 1+ sharing 3　(f) Sharing 2+ sharing 3

(g) 分享1+分享2+分享3
(g) Sharing 1+sharing 2+ sharing 3

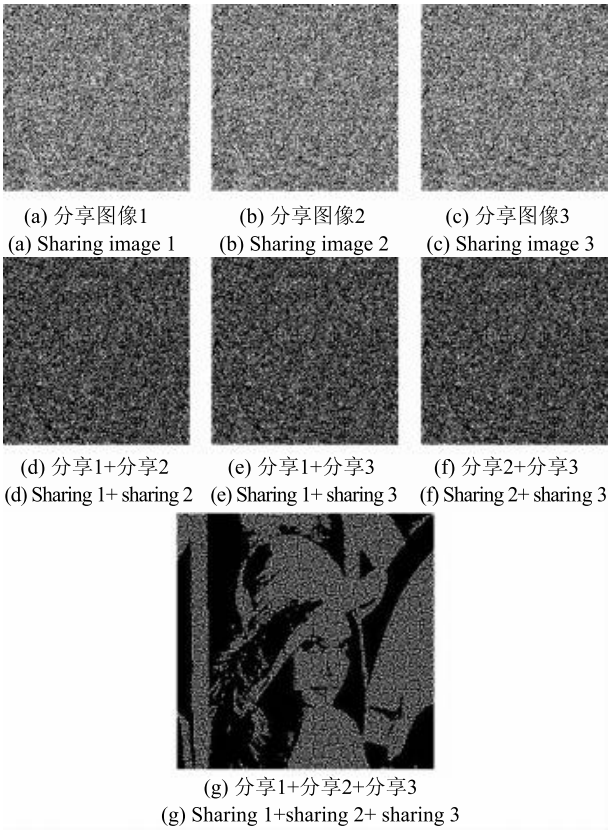
**图 5　文献[13]所给(3,3)方案的实验结果**

**Fig. 5　Experiment result of (3,3) scheme presented in Ref. [13]**

### 4.2　实验结果对比

峰值信噪比（peak signal-to-noise ratio，*PSNR*）和比特错误率（Bit error rate，*BER*）是衡量恢复图像质量的 2 个重要指标。*PSNR* 值越大，表明恢复的图像和原始图像越相似；*BER* 值越小越好，表明恢复的图像和原始图像越接近。为了证明本次研究的有效性，通过实验将本次研究与近两年的相关研究[13,17-18]进行了比较，由此得到的不同(3,3)视觉密码方案恢复图像的 *PSNR* 值和 *BER* 值见表 2。Chen 等人[15]利用概率思想设计分享方案，Shyu[8]、Chen 等人[17]和 Guo 等人[18]利用随机网格思想设计分享方案，这些方案产生的分享图像中黑白像素是随机分布，恢复图像的白色区域黑白像素分布也

是随机的。本研究所产生的分享图像及2幅分享图像的叠加结果黑白像素分布更均匀,恢复图像的白色区域黑白像素分布也更均匀,连续的4个像素一定有1个白色像素,这样恢复图像的视觉效果比已有的方法更好。



(a) 分享图像1 (a) Sharing image 1
(b) 分享图像2 (b) Sharing image 2
(c) 分享图像3 (c) Sharing image 3
(d) 分享1+分享2 (d) Sharing 1+ sharing 2
(e) 分享1+分享3 (e) Sharing 1+ sharing 3
(f) 分享2+分享3 (f) Sharing 2+ sharing 3
(g) 分享1+分享2+分享3 (g) Sharing 1+sharing 2+ sharing 3

**图6 所得出(3,3)方案实验结果**

**Fig. 6 Experiment result of proposed (3,3) scheme**

**表2 不同分享方案 *PSNR* 和 *BER* 值比较**

**Tab. 2 *PSNR* and *BER* values for various sharing schemes**

| 方案 | *PSNR* | *BER* |
|---|---|---|
| 文献[8] | 23.449 1 | 0.383 4 |
| 文献[13] | 23.457 5 | 0.383 1 |
| 文献[17] | 23.453 7 | 0.383 2 |
| 文献[18] | 23.453 9 | 0.383 0 |
| 本研究 | 23.665 3 | 0.371 7 |

## 5 结束语

衡量一个可视秘密分享方案优劣的标准是低扩展度和高对比度。提出的基于随机网格的可视秘密改进方案产生的分享图像具有和原秘密图像相同的大小,即像素不扩展。同已有的基于随机网格的视觉密码方案相比,本文提出方案产生的分享图像黑白像素分布更均匀,恢复的图像更清晰。本研究所给方法同样也可以扩展为$(k,n)$方案,后续工作将对基于随机网格的多秘密视觉密码展开深入研究。

## 参考文献


[1] NAOR M, SHAMIR A. Visual cryptography[C]// Eurocrypt´94, LNCS 950. Berlin: Springer-Verlag, 1994:1-12.

[2] ITO R, KUWAKADO H, TANAKA, H. Image size invariant visual cryptography[J]. IEICE Tansactions on Fundamentals of Electronics, Communications and Computer Sciences, 1999, E82-A(10):2172-2177.

[3] YANG C N. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, 25(4):481-494.

[4] TUA S F, HOUB Y C. Design of visual cryptographic methods with smooth-looking decoded images of invariant size for grey-level images[J]. The Imaging Science Journal, 2007, 55(2):90-101.

[5] LIN T L, HORNG S J, LEE K H, et al. A novel visual secret sharing scheme for multiple secrets without pixel expansion[J]. Expert Systems with Applications, 2010, 37(12):7858-7869.

[6] KAFRI O, KEREN E. Encryption of pictures and shapes by random grids[J]. Optics Letters, 1987, 12(6):377-379.

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

[8] SHYU S J. Image encryption by multiple random grids[J]. Pattern Recognition, 2009, 42(7): 1582-1596.

[9] CHEN T H, TSAO K H. Visual secret sharing by random grids revisited[J]. Pattern Recognition, 2009, 42(9): 2203-2217.

[10]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(2):149-153.

[11]郁滨,王翠. 像素不扩展的MSM视觉密码方案[J]. 信息工程大学学报,2007,8(2): 156- 160.

[12]FANG W P. Non-expansion visual secret sharing in reversible style[J]. International Journal of Computer Science and Network Security, 2009, 9(2):204-208.

[13]候永昌,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.

[14]胡浩,郁滨,沈刚. 像素不扩展视觉密码的边缘增强研究[J]. 计算机科学, 2015, 42(2): 103- 107.

[15]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, 21(11):1693-1703.

[16]LOU D C, CHEN H H, WU H C, et al. A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares[J]. Displays, 2011, 32(3):118-134.

[17]CHEN T H, TSAO K H. Threshold visual secret sharing by random grids[J]. Journal of Systems and Software, 2011, 84(7): 1197-1208.

[18]GUO T, LIU F, WU C K. K out of k extended visual cryptography scheme by random grids[J]. Signal Processing, 2014, 94(1):90-101.