Equivalence Proof of Traditional and Random Grid-Based (2, 2) Visual Secret Sharing

Shen Wang*, Xuehu Yan, Jianzhi Sang, and Xiamu Niu

School of Computer Science and Technology,
Harbin Institute of Technology, Harbin, China
Shen.Wang@hit.edu.cn

Abstract. Visual secret sharing (VSS) has attracted considerable attention to scientists and engineers as another branch alongside conventional cryptography to protect the sensitive visual information from several rapacious behaviors. In the literature, there are a number of several techniques used to protect the visual information, among which traditional VSS and random grid (RG)-based VSS are the primary branches. In this letter, we show, by examples, the two means are equal. In addition, the color representation of traditional VSS and RG-based VSS found it different from digital applications like images. Based on the given examples, it is demonstrated that the color representation of the two means can be the same and confirm with digital processing applications.

Keywords: Visual cryptography, Visual secret sharing, Random grid, Equivalence proof, Color representation.

1 Introduction

Visual cryptography(VC) and general secret image sharing [1][2] protects the secret by sharing the user data into different secret shares (also called shadows) and distributing them among multiple carriers. They have attracted more attention of scientists and engineers. Visual secret sharing (VSS) also called visual cryptography scheme (VCS), and Shamir's polynomial-based scheme are the primary branches in this field.

Naor and Shamir [1] firstly propose the threshold-based VSS. The main properties of the VSS by [1] are simple recovery that is the decryption of secret image is completely based on human visual system (HVS) without any cryptographic computation. However, it also suffers from meaningless shadow images, lossy recovery and pixel expansion [2].

Attributed to the traditional VSS proposed by Naor and Shamir [1], various secret image sharing schemes have been proposed in the literature. However, most of the proposed schemes remained weakness to be resolved before secret

* This work is supported by the National Natural Science Foundation of China (61301099, 61100187, 11201100),Heilongjiang Province Educational Department Funds of China (12521107)

J.-S. Pan et al. (eds.), *Intelligent Data Analysis and Its Applications, Volume 2,*
Advances in Intelligent Systems and Computing 298,
DOI: 10.1007/978-3-319-07773-4_14, © Springer International Publishing Switzerland 2014

sharing can gain possibly pervasive applications. For instance, the scheme of Giuseppe et al. [3] has meaningful shadow images, but still has lossless recovery and pixel expansion problem. Yang [4] proposes a probability-based visual sharing scheme which is lossless and has no pixel expansion, but doesn't have meaningful shadow images. Wang et al. [5] proposes a secret sharing scheme based on Boolean operation that is lossless. However, these schemes suffer from pixel expansion problem.

Since VSS by random grids (RG) could avoid pixel expansion and has no codebook (basic matrices) needed, some other researchers [6],[12],[7], [9],[11] have paid more attention to RG-based VSS. Encryption of binary secret images based on RG is firstly presented by Kafri and Keren [6], each of which is generated into two noise-like RG (shadow images or share images) that have the same size as the original secret image. The decryption operation is Boolean OR operation which is the same as traditional VSS.

Though the traditional VSS and RG-based VSS are two primary branches of VSS, however they have some similarities about the key idea. In both traditional VSS and RG-based (2, 2) VSS, the color representation is "1" denotes black pixels, "0" denotes white pixels, which may be not convenient [5],[10],[8] in digital images and common digital processing software. In most digital image formats like BMP and JPEG, and common digital image processing related software, such as Matlab and Photoshop, 0 denotes black or opaque pixel value and 1 denotes white or transparent pixel value. Different color representations will increase computation time for reversing or complementing operations (that is $0 \to 1$ or $1 \to 0$).

In the paper, we show the traditional and random grid-based (2, 2) VSS is equal by given examples of generation ideas and visual quality. In addition, the color representation of traditional VSS and RG-based VSS found it different from digital images in the previous proposed approaches. Based on the given examples, it is demonstrated that the color representation of the two means is the same with digital images.

The rest of the paper is organized as follows. Section 2 gives the preliminary techniques of traditional VSS and RG-based VSS as the basis for the work. In Section 3, the equivalence proof of the two means is introduced. Finally, Section 4 concludes this paper.

2 Preliminary Techniques

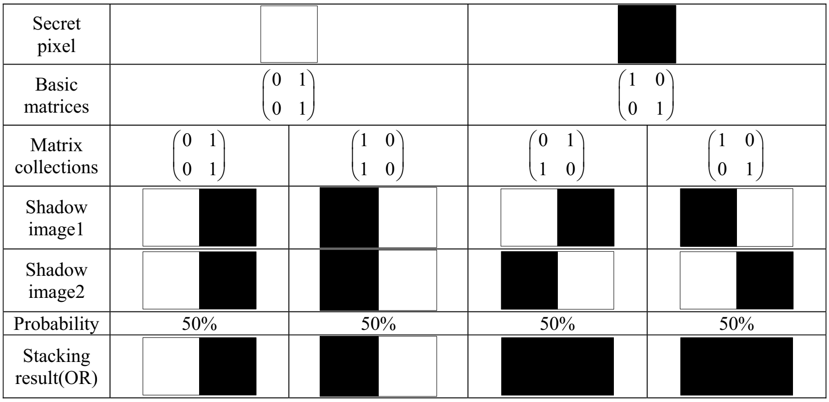
This section introduces the related works of traditional (2, 2) VSS [1] and one typical RG-based [6] VSS.

Shadow images number is 2, the binary secret image is denoted as S with pixel value $S(i, j), 1 \leq i \leq M, 1 \leq j \leq N$. The shadow images covered secret after sharing are denoted as SC. The recovered secret image from $k = 2$ shadow images is denoted as S'. In traditional VSS and RG-based VSS "1" denotes black pixels, “0” denotes white pixels, the decryption is Boolean OR operation. Here, the secret image “HIT” with size 256×256 is used to illustrate the idea. Symbols $\&, \oplus$ and $\otimes$ denote the Boolean AND, XOR and OR operations, respectively. $\overline{x}$ is a bit-wise complementary operation of x.

2.1 Traditional (2, 2) VSS

In traditional (2, 2) VSS, a binary secret image is shared by generating corresponding two noise-like shadow images. The two noise-like shadow images are superposed to recover the secret image visually based on HVS and probability. However, less than 2 participants cannot reveal any information of the secret image

Fig. 1 shows the idea of traditional (2, 2) VSS, a certain pixel of the secret image is split into a pair of white and black subpixels in each of the two shadow images. The subpixels are randomly selected from the two columns tabulated under the certain secret pixel, which leads to the certain secret pixel is encoded into two subpixels of white-black or black-white with the same probabilities (50%). Hence, an individual shadow image gives no information about the secret image. When the subpixels are stacked, the black secret pixel will be decoded into black pixel, and the white secret pixel into one white pixel and one black pixel. Thus, the secret image could be recovered by stacking the two shadow images together. Fig. 2 is an application example of the (2, 2) VCS, though the pixel expansion is 2 and some contrast is lost, the secret image could be recognized clearly by HVS.



Secret pixel	□		■	
Basic matrices	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	
Matrix collections	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Shadow image1	□■	■□	□■	■□
Shadow image2	□■	■□	■□	□■
Probability	50%	50%	50%	50%
Stacking result(OR)	□■	■□	■■	■■

Fig. 1. The idea of traditional (2, 2) VC

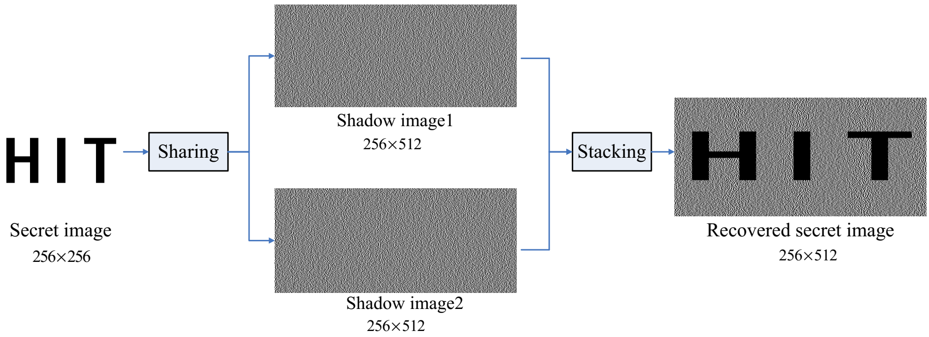


Fig. 2. An application example of traditional (2, 2) VC

2.2 RG-Based VSS

The generation and recovery phases of one typical (2, 2) RG-based [6] VSS are described below.

Step 1: Randomly generate 1 RG SC_1

Step 2: Compute SC_2 as in Eq. 1

Recovery: $S' = SC_1 \otimes SC_2$ as in Eq. 2. If a certain secret pixel of $S(i,j)$ is 1, the recovery result $SC_1 \otimes SC_2 = 1$ is always black. If a certain secret pixel of $S(i,j)$ is 0, the recovery result $SC_1 \otimes SC_2 = SC_1(i,j) \otimes SC_1(i,j)$ has half chance to be black or white since SC_1 is generated randomly

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if\ S = 0 \\ \overline{SC_1(i,j)} & if\ S = 1 \end{cases} \tag{1}$$

$$\begin{aligned} S'(i,j) &= SC_1(i,j) \otimes SC_2(i,j) \\ &= \begin{cases} SC_1(i,j) \otimes SC_1(i,j) & if\ S(i,j) = 0 \\ SC_1(i,j) \otimes \overline{SC_1(i,j)} = 1 & if\ S(i,j) = 1 \end{cases} \end{aligned} \tag{2}$$

Fig. 3 shows an application example of original (2, 2) RG-based VSS, among which, the shadow images are generated by the generation phase described above and the recovered secret image is recovered by the recovery phase described above of the original (2, 2) RG-based VSS.

From the generation and recovery phases of original (2, 2) RG-based VSS described above, we can present the idea of RG-based (2, 2) VSS in Fig. 4, a certain pixel of the secret image is generated into a white or black subpixel in each of the two shadow images. The subpixels are randomly selected from the two columns tabulated under the certain secret pixel, which lead to certain secret pixel that is encoded into two subpixels with the same probabilities (50%). Hence, an individual shadow image gives no information about the secret image.

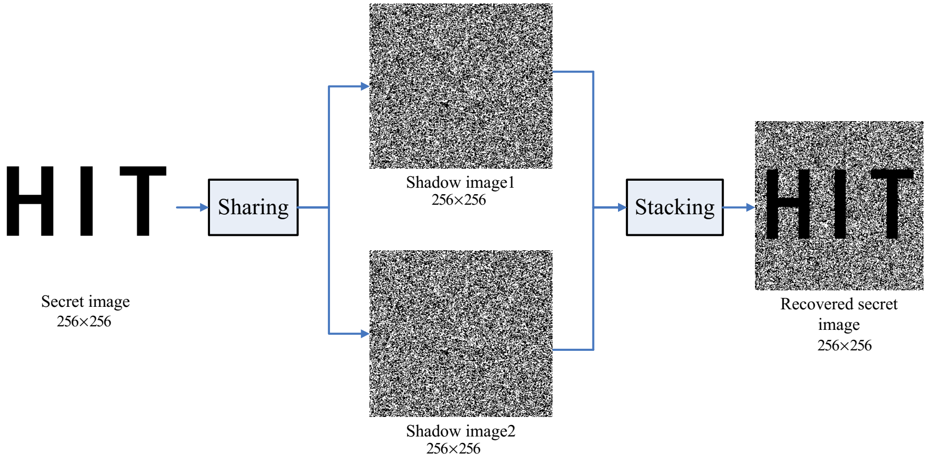


Fig. 3. An application example of original (2, 2) RG-based VSS

Secret pixel	□		■	
Matrix collections	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$
Shadow image1	□	■	□	■
Shadow image2	□	■	■	□
Probability	50%	50%	50%	50%
Stacking result(OR)	□	■	■	■

Fig. 4. The idea of original (2, 2) RG-based VSS

When the subpixels are stacked, the black secret pixel will be decoded into black pixel, and the white secret pixel into white pixel or black pixel with the same probabilities (50%). Thus, the secret image could be recovered by stacking the two shadow images together.

3 Equivalence Proof

3.1 Original Idea Equivalence

From Fig. 1 and Fig. 4, if the first column of matrix collections in Fig. 1 of the traditional (2, 2) VSS is gleaned, matrix collections in Fig. 4 of the RG-based (2,

2) VSS will be gained. This means that in the generation phase of traditional (2, 2) VSS, if only the first column is chosen randomly to the two shadow images, the same recovering result could be obtained.

One example is shown in Fig. 5, in the example, the traditional (2, 2) VSS is applied to share the secret image.

First, the shadow images with size $M \times 2N$are randomly assigned 0 or 1, the pixel expansion $m = 2$ since the pixel expansion of traditional VSS.

Second, for every pixel $S(i, j), 1 \leq i \leq M, 1 \leq j \leq N, M = N = 256$ of the secret image, the pixel values of shadow images $SC_1\left(i, j\right), SC_2\left(i, j\right)$ are decided by the first column of matrix collections in Fig. 1 of the traditional (2, 2) VSS randomly.

When the two shadow images are stacked together, the secret will be revealed in the left half part of the recovered secret image, that means if only the left part of the shadow images is assigned, there will only be the left part of the recovered secret image ,the result could be clearly shown in Fig. 6. The illustration is caused by the first column of matrix collections in Fig. 1 of the traditional (2, 2) VSS. Hence, the key idea of RG-based (2, 2) VSS is the same as traditional (2, 2) VSS.

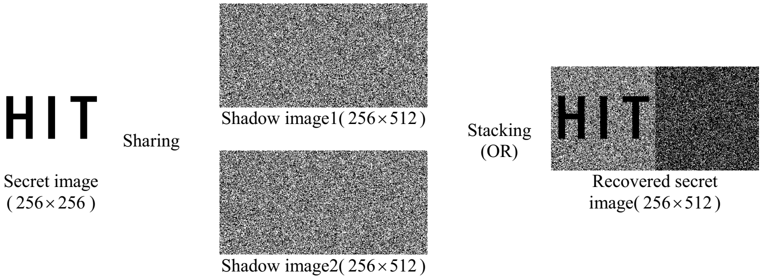


Fig. 5. An equivalence example of traditional (2, 2) and RG-based VC

3.2 Visual Quality Equivalence

Based on Fig. 3 and Fig. 6, the recovered secret images are the same based on human visual system (HVS), which means that the visual quality of the recovered secrets are the same, and the visual quality of traditional and RG-based (2, 2) VSS are equal. Furthermore, the equivalence of theoretical visual quality is analyses as follows:

The probability of pixel color is transparent (0) say $P\left(x = 0\right)$ and the same for the probability of pixel color is opaque (1). Besides, $\sum_{i=1}^{M} \sum_{j=1}^{N} X\left(i, j\right), 1 \leq i \leq M, 1 \leq j \leq N$.

The visual quality of traditional (2, 2) VSS [1] is evaluated by α_t, the relative difference in the Hamming weight, i.e., the loss in contrast between the recovered

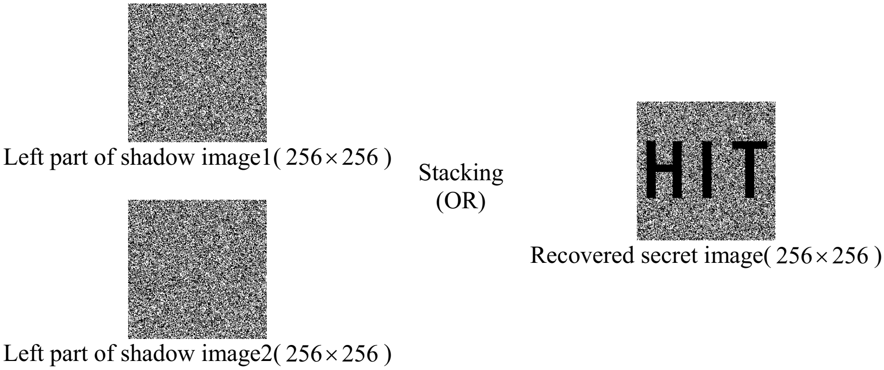

Left part of shadow image1(256×256)
Stacking
(OR)
HIT
Recovered secret image(256×256)
Left part of shadow image2(256×256)

Fig. 6. Stacking result of the left part of the shadow images in Fig. 5

secret pixels that is steaming from a white and black pixel in the original secret image. Hence, the contrast of traditional (2, 2) VSS is 1/2.

The visual quality and security of RG-based (2, 2) VSS [7] is evaluated by contrast α defined as follows:

Definition 1 (Contrast): The visual quality, which will decides how well human eyes could recognize the recovered image, of the recovered secret image S' corresponding to the original secret image S is evaluated by contrast defined as follows:

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P\left(S'\left[AS0\right] = 0\right) - P\left(S'\left[AS1\right] = 0\right)}{1 + P\left(S'\left[AS1\right] = 0\right)} \tag{3}$$

where α denotes contrast, P_0(resp.,P_1) is the appearance probability of white pixels in the recovered imageS'in the corresponding white (resp., black) area of original secret image$S$. $AS0$ (resp., $AS1$) is the white (resp., black) area of original secret image S, $AS0 = \{(i,j)\,|S\,(i,j) = 0, 1 \leq i \leq M, 1 \leq j \leq N\}$

The visual quality of RG-based (2, 2) VSS is evaluated by contrast, which is light contrast defined based on average light transmission of all the recovered secret pixels. Hence, the contrast of RG-based (2, 2) VSS is $\frac{P_0 - P_1}{1+P_1} = \frac{\frac{1}{2}-0}{1+0} = \frac{1}{2}$

Additionally, from Fig. 1, if the secret pixel is white (0), in the recovered secret pixels(01 or 10) the light transmission will be 0.5; if the secret pixel is black(1), in the recovered secret pixels(11) the light transmission will be 0. Hence, if the **Definition1** is applied for traditional (2, 2) VSS, the contrast of traditional (2, 2) VSS will be $\frac{P_0 - P_1}{1+P_1} = \frac{\frac{1}{2}-0}{1+0} = \frac{1}{2}$ which is the same as RG-based (2, 2) VSS.

From the contrast experimental results, the same situation could also be gained. The contrast calculated by **Definition1** of Fig. 3 is 0.49948, and contrast calculated by **Definition1** of Fig. 6 is 0.49979, which are very similar to each other, and close to theoretical value 0.5.

Based on the above analyses, it is demonstrated that the traditional (2, 2) VC and RG-based (2, 2) VSS have the same visual quality.

The security and visually recognizable of both traditional VSS and RG-based on VSS [1] is defined as follows:

Definition 2 (Security and visually recognizable): The recovered secret image S' could be recognized as the corresponding original secret image S if $\alpha > 0$ when $t \geq k$. The VSS is secure if $\alpha = 0$ when $t < k$ which means no information of S could be recognized through S'.

From **Definition1,** the security and visually recognizable of traditional VSS and RG-based on VSS is evaluated by the contrast, which means that the equal contrast will lead to equal security and visually recognizable, since they are defined or decided by the contrast of shadow images and recovered secret.

3.3 Further Discussion

The color representation of traditional and RG-based VSS is different from digital images. Furthermore, Yan et al. [8] have proposed a powerful RG-based VSS based on Boolean operations. This scheme has the same color representation method with digital images, where "1" denotes white pixels, "0" denotes black pixels

Herein, a (2, 2) threshold scheme is used as an example firstly to show the idea of Yan's scheme [8] . The generation and recovery phases are described below "1" denotes white pixels, "0" denotes black pixels

Step 1: Randomly generate 1 RG SC_1

Step 2: ComputeSC_2 as in Eq. 4.

Recovery: $S' = SC_1 \& SC_2$ as in Eq. 5. If a certain secret pixel of $S(i,j)$ is 0, the recovery result $SC_1 \& SC_2 = 0$ is always black. If a certain secret pixel of $S(i,j)$ is 1, the recovery result $SC_1 \& SC_2 = SC_1(i,j) \& SC_1(i,j)$has half chance to be black or white since SC_1 are generated randomly

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if\ S(i,j) = 1 \\ \overline{SC_1(i,j)} & if\ S(i,j) = 0 \end{cases} \tag{4}$$

$$\begin{aligned} S'(i,j) &= SC_1(i,j) \& SC_2(i,j) \\ &= \begin{cases} SC_1(i,j) \& SC_1(i,j) & if\ S(i,j) = 1 \\ SC_1(i,j) \& \overline{SC_1(i,j)} = 0 & if\ S(i,j) = 0 \end{cases} \end{aligned} \tag{5}$$

In addition, the idea applied in Yan's scheme, that is the color representation method is the same with color representation method of digital images not only could be applied in RG-based VSS, but also can be extended to traditional VSS. Herein, the traditional (2, 2) VSS is used as an example. Fig. 7 is an extended example of (2, 2) VSS, Here "0" denotes black pixels, "1" denotes white pixels. A certain pixel of the secret image is split into a pair of white and black subpixels in each of the two shadow images. When the subpixels are stacked (corresponding to Boolean AND operation), the black secret pixel will be decoded into black pixel, and the white secret pixel into one white pixel and one black pixel. Thus, the secret image could be recovered by stacking the two shadow images together. Fig. 8 is an extended application example of the traditional (2, 2) VSS, the secret image could be recognized clearly by HVS.

Secret pixel	□		■	
Basic matrices	$\begin{pmatrix}0 & 1\\0 & 1\end{pmatrix}$		$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$	
Matrix collections	$\begin{pmatrix}0 & 1\\0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\\1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
Shadow image1	■□	□■	■□	□■
Shadow image2	■□	□■	□■	■□
Probability	50%	50%	50%	50%
Boolean AND result	$\begin{pmatrix}0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0\end{pmatrix}$
Stacking(&) result	■□	□■	■■	■■

Fig. 7. An extended example of traditional (2, 2) VC

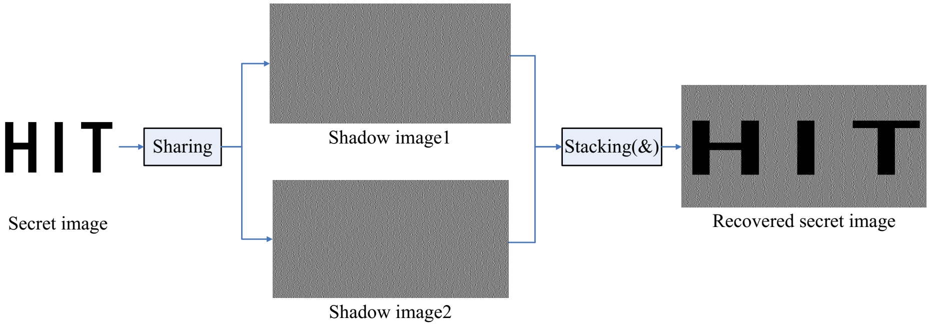


Fig. 8. An extended application example of traditional (2, 2) VC

4 Conclusion

In this paper, the traditional VSS and RG-based VSS found equal by the given examples. In addition, the color representation of traditional VSS and RG-based VSS found it different from digital images. Based on the given examples, it is showed that the color representation of the two means is the same with digital images. The presented work will be useful for understanding the relationship between the traditional VSS and RG-based VSS, and worthwhile in more digital applications.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
2. Weir, J., Yan, W.: A comprehensive study of visual cryptography. In: Shi, Y.Q. (ed.) Transactions on DHMS V. LNCS, vol. 6010, pp. 70–105. Springer, Heidelberg (2010)
3. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theor. Comput. Sci. 250(1), 143–161 (2001)
4. Yang, C.-N.: New visual secret sharing schemes using probabilistic method. Pattern Recognit. Lett. 25(4), 481–494 (2004)
5. Wang, D., Zhang, L., Ma, N., Li, X.: Two secret sharing schemese based on Boolean operations. Pattern Recognit. 40(10), 2776–2785 (2007)
6. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Optics Letters 12(6), 377–379 (1987)
7. Shyu, S.J.: Image encryption by random grids. Pattern Recognition 40(3), 1014–1031 (2007)
8. Yan, X., Wang, S., El-Latif, A.A.A., Niu, X.: Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. IEEE Trans. on Circ. and Sys. for Video Tech. 21(11), 1693–1703 (2011); Accepted for publication in Multimedia tools and application (2013), doi: 10.1007/s11042-013-1784-2,2013
9. Wu, X., Sun, W.: Improving the visual quality of random grid-based visual secret sharing. Signal Processing (2012)
10. Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error diffusion. IEEE Trans. Inf. Forensics Security 4(3), 383–396 (2009)
11. Guo, T., Liu, F., Wu, C.K.: Threshold visual secret sharing by random grids with improved contrast. Journal of Systems and Software (2013)
12. Chen, T.-H., Tsao, K.-H.: Threshold visual secret sharing by random grids. Journal of Systems and Software 84(7), 1197–1208 (2011)