Visual Cryptography and Random Grids Schemes

Zheng-xin Fu(✉) and Bin Yu

Zhengzhou Information Science and Technology Institute,
Zhengzhou 450004, People's Republic of China
{fzx2515,byu2009}@163.com

Abstract. Visual Cryptography (VC) and Random Grids (RG) are both visual secret sharing (VSS) techniques, which decode the secret by stacking some authorized shares. It is claimed that RG scheme benefits more than VC scheme in terms of removing the problems of pixel expansion, tailor-made codebook design, and aspect ratio change. However, we find that the encryption rules of RGS are actually the matrices sets of probabilistic VCS. The transformation from RGS to PVCS is proved and shown by means of giving theoretical analysis and conducting some specific schemes. The relationship between codebook and computational complexity are analyzed for PVCS and RGS. Furthermore, the contrast of PVCS is no less than the one of RGS under the same access structure, which is shown by experimental results.

Keywords: Visual cryptography · Random grids · Encryption rules · Transformation

1 Introduction

Visual secret sharing (VSS) techniques encrypt a secret image into several meaningless share images, and decrypt the secret by overlapping the some authorized shares. Due to the ease of decoding, VSS provides some new and secure imaging applications, e.g., visual authentication, steganography, and image encryption.

Visual cryptography scheme (VCS) was introduced by Naor and Shamir in Eurocrypt'94 [1]. The difference between visual cryptography and the traditional secret sharing schemes [2, 3] is the decryption process. Most secret sharing schemes are mainly realized by the computer, while visual cryptography schemes can decrypt secrets only with human eyes. In recent years, the studies of VCS focus on the general access structure [4], the optimization of the pixel expansion and the relative difference [5–8], and the grey and color images [9–12], etc.

In order to design the unexpanded shares, Ito et al. [13] firstly introduced a scheme without pixel expansion. Yang et al. [14, 15] provided a new model of visual cryptography scheme, in which the reconstruction of the secret image was probabilistic. In probabilistic model, the secret pixel is correctly reconstructed with probability. Thus, the quality of the reconstructed images depends on how big the probability is. The probabilistic scheme differs from the traditional VCS, which is now called deterministic scheme. The deterministic means that a white (black) original pixel can be

Y.Q. Shi et al. (Eds.): IWDW 2013, LNCS 8389, pp. 109–122, 2014.
DOI: 10.1007/978-3-662-43886-2_8,

represented in the reconstructed image by a set of subpixels with certain whiteness (blackness). Cimato et al. [16] introduced how to trade pixel expansion for the probability of a good reconstruction, which can be seen as a generalization of both the classical deterministic model and the probabilistic model.

Another VSS scheme is realized by Random Grids, which was proposed by Kafri and Keren in 1987 [17]. A binary secret image is encoded into two meaningless grids, which have the same size as the secret image. RG scheme (RGS) is mainly realized by using three different functions (f_{ran}, f_{equ}, f_{com}) recursively, and has no requirement of codebook which is the basis of VCS. Inspired of Kafri and Keren [17], Shyu [18] presented the other two RGSs to encrypt gray-level and color images in 2007. Later, Shyu [19] and Chen et al. [20, 21] proposed (2, n), (n, n) and (k, n) RGSs, which made further research.

In this paper, we mainly analyze the relationship between VCS and RGS, which is considered for the first time. It is found that the encryption rules of RGS are actually the set of distribution matrices in PVCS. In other words, there always exists a PVCS corresponding to every RGS. On the other hand, the corresponding RGS for every PVCS can not been guaranteed. Furthermore, the cost and contrast comparisons between RGS and PVCS are discussed in detail.

The rest of this paper is organized as follows. Section 2 briefly reviews RGS and PVCS. As the main part of this paper, Sect. 3 analyzes how to transform RGS into PVCS. Section 4 shows experimental results and discussions about the parameters of RGS and PVCS. Section 5 concludes the paper.

2 Related Studies

Prior to describing the proposed scheme, the reviews of RGS and PVCS are briefly introduced.

2.1 Random Grids Scheme

RGS mainly consists of three operations: (1) randomization, (2) complement, and (3) equivalence. The detailed definitions are given below.

Definition 1 (randomization) [20]. A random bit generation function

$$f_{ran}(.) = \begin{cases} 0 & \textit{with the probability } 0.5 \\ 1 & \textit{with the probability } 0.5 \end{cases}$$

is used to create the pixel of cipher-grid. Precisely, a certain pixel r of a grid R is assigned the value 0 or 1 to represent the color white or black with the same probability 1/2. In other words, $\mathrm{r} = f_{ran}(.)$ means $P(r = 1) = P(r = 0) = 1/2$.

Definition 2 (complement) [20]. According to a pixel r_1 of grid, say R_1, the complement function

$$f_{com}(x) = \begin{cases} 0 & if\ x = 1 \\ 1 & if\ x = 0 \end{cases}$$

turns r_1 inversely and assigns the inversed pixel value to a pixel r_2 of the other grid, say R_2. For instance, if r_1 is 0, the pixel value $r_2 = 1$ is obtained, i.e., $r_2 = f_{com}(r_1 = 0) = 1$.

Definition 3 (equivalence) [20]. The equivalence function

$$f_{equ}(x) = \begin{cases} 0 & if\ x = 0 \\ 1 & if\ x = 1 \end{cases}$$

referring to a pixel r_1 of grid R_1 assigns the same pixel value to a pixel r_2 of the other grid R_2. For instance, if r_1 is 0, the pixel value $r_2 = 0$ is obtained. In other words, $r_2 = f_{equ}(r_1 = 0) = 0$.

Definition 4 (Representation of corresponding area) [20]. Assume that $A(0)$ (resp. $A(1)$) is the corresponding area of all the white (resp. black) pixels in the secret image A, where $A = A(0) \cup A(1)$ and $A(0) \cap A(1) = \varnothing$. Hence, $B[A(0)]$ (resp. $B[A(1)]$) is the corresponding area of all the white (resp. black) pixels in the binary image B, which is reconstructed by the VSS scheme based on RG, with respect to the secret image A.

Definition 5 (Average light transmission) [20]. For a certain pixel r in a binary image B, the light transmission of a white (resp. black) pixel is defined as $t(r) = 1$ (resp. 0). In addition, for B with the size of $h \times w$, the average light transmission of B is defined as

$$T(B) = \frac{1}{h \times w} \cdot \sum_{i=1}^{h} \sum_{j=1}^{w} t(r[i,j]).$$

Definition 6 (Contrast) [20]. The contrast of the superimposed binary image B with respect to the original secret image A is,

$$\alpha = \frac{T(B[A(0)]) - T(B[A(1)])}{1 + T(B[A(1)])}.$$

α would be as large as possible. In other words, the larger the value of α, the more recognizable the superimposed secret will be.

Since the recovery of the secret images depends on the human visual system, the contrast of superimposed secret images plays a critical role in guaranteeing that the superimposed image can be visually recognized as the exact secret message. Consequently, the following definition is given.

Definition 7 (Visually recognizable) [20]. The reconstructed binary image B with respect to the original secret A by superimposing two RG is visually recognizable in the sense, at least, that its contrast is greater than or equal to a threshold value which is greater than zero. In principle, if the reconstructed binary image can be recognizable,

α must be greater than zero. The numerator of α is $T(B[A(0)]) - T(B[A(1)])$ that causes α to be a non-zero value. Therefore, if $T(B[A(0)])$ is greater than $T(B[A(1)])$, B is visual recognizable. On the contrary, if $T(B[A(0)])$ is equal to or less than $T(B[A(1)])$, B is meaningless.

2.2 Probabilistic Visual Cryptography Scheme

In a probabilistic scheme, the recovery property cannot be guaranteed. Each pixel can be correctly reconstructed only with a probability given as a parameter of the scheme. Given a qualified set of participants Q, let $p_{i|j}$ denote the probability of having a reconstructed pixel i, and the corresponding pixel in the secret image is j, where i, $j \in \{0, 1\}$. Then $p_{0|0}(Q)$ denotes the probability of correctly reconstructing a white pixel when stacking the shares of Q, and $p_{1|0}(Q)$ is the probability of incorrectly reconstructing a white pixel. In a similar way $p_{1|1}(Q)$ and $p_{0|1}(Q)$ can be defined. The formal definition of a β-probabilistic visual cryptography scheme is as follow.

Definition 8 (Probabilistic VCS) [15]. A $(\Gamma_{Qual}, \Gamma_{Forb}, m, \beta)$ -PVCS consists of two collections of $n \times m$ binary matrices, C_0 and C_1, satisfying the following properties:

1. (Contrast property) For any set $Q = \{i_1, i_2, \ldots, i_q\} \in \Gamma_{Qual}$, there exists $\beta > 0$ such that $p_{1|1}(Q) - p_{1|0}(Q) \geq \beta$ and $p_{0|0}(Q) - p_{0|1}(Q) \geq \beta$

2. (Security property) For any set $F = \{i_1, i_2, \ldots, i_f\} \in \Gamma_{Forb}$, the two collections of $f \times m$ matrices D_t, with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in C_t to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

In this paper, we mainly use PVCS scheme with no pixel expansion, that is having $m = 1$. Suppose $C_0 = \{M_0^1, M_0^2, \cdots, M_0^{c0}\}$, $C_1 = \{M_1^1, M_1^2, \cdots, M_1^{c1}\}$, $S[i, j]$ is the i-th row and j-th column pixel in secret image S, n shares denoted as $\{R_1, R_2, \ldots, R_n\}$. The secret sharing algorithm of PVCS only needs two steps: select and distribute.

Select: if $S[i, j] = 0$, generate a random number $k \in [1, \ldots, c_0]$, $M = M_0^k$.
else $S[i, j] = 1$, generate a random number $k \in [1, \ldots, c_1]$, $M = M_1^k$.

Distribute: $(R_1[i, j], R_2[i, j], \ldots, R_n[i, j])^{\mathrm{T}} = M$.

Example 1. (2, 2) -PVCS

$C_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}, C_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$. For this scheme, $m = 1$, $p_{1|1} = 1$, $p_{1|0} = 1/2$, $p_{0|0} = 1/2$, $p_{0|1} = 0$, and $= p_{1|1} - p_{1|0} = p_{0|0} - p_{0|1} = 1/2$.

3 A Transformation from RGS to PVCS

In RGS, the random grids are with the same size of the original secret image. The sharing algorithm of RGS relies on iterations and loops, which has no requirement of designing a codebook. Although RGS is called removing the problems of pixel

expansion, tailor-made codebook design, and aspect ratio change in VCS [20], we find that the encryption rules of RGS are actually the matrices sets of PVCS. In this section we will show how to transform a RGS into a PVCS with the same contrast and security.

Definition 9. (sets of encryption rules). Let $E_0 = \{f_1, f_2, \ldots, f_{e0}\}$ and $E_1 = \{g_1, g_2, \ldots, g_{e1}\}$ be two sets, where f_i and g_j are both $n \times 1$ Boolean vector ($i \in [1, \ldots, e_0]$, $j \in [1, \ldots, e_1]$). f_i denotes the i-th encryption rule by which a white pixel is encrypted, while g_j denotes the j-th encryption rule by which a black pixel is encrypted. We call E_0 and E_1 the sets of encryption rules, which represent all of the encryption rules of a RGS.

Definition 10. r denotes a random Boolean number, where $r = 0$ or 1 with the same probability 1/2. Let $[r]$ denote two 1×1 matrices [1] and [0]. Suppose x is a Boolean number, let $\begin{bmatrix} r \\ x \end{bmatrix}$ denote two 2×1 matrices $\begin{bmatrix} 0 \\ x \end{bmatrix}$ and $\begin{bmatrix} 1 \\ x \end{bmatrix}$. Suppose r_1 is another random Boolean number which is independent with r, let $\begin{bmatrix} r \\ r_1 \end{bmatrix}$ denote four 2×1 matrices $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Suppose $M = \{M_1, M_2, \ldots, M_m\}$ is a set of $n \times 1$ matrices, let $\begin{bmatrix} r \\ M \end{bmatrix}$ denote $2m\ (n + 1) \times 1$ matrices $\begin{bmatrix} 0 \\ M_1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ M_1 \end{bmatrix}$, $\begin{bmatrix} 0 \\ M_2 \end{bmatrix}$, $\begin{bmatrix} 1 \\ M_2 \end{bmatrix}$,…, $\begin{bmatrix} 0 \\ M_m \end{bmatrix}$, $\begin{bmatrix} 1 \\ M_m \end{bmatrix}$.

3.1 (2, 2)-RGS

Chen et al. proposed three different kinds of (2, 2)-RGSs, which were the basic model of RGS. In this section, we firstly analyze the sets of encryption rules of (2, 2)-RGS, and then prove that E_0 and E_1 are also the sets of distribution functions.

Algorithm 1. $(2, 2)_1$-RGS [20]

Input: A binary secret image $S = \{S[i, j] | S[i, j] \in \{0, 1\}, i \in [1, 2, \ldots, h], j \in [1, 2, \ldots, w]\}$

Output: Two cipher-grids $R_1 = \{R_1[i, j] | R_1[i, j] \in \{0, 1\}, i \in [1, 2, \ldots, h], j \in [1, 2, \ldots, w]\}$ and $R_2 = \{R_2[i, j] | R_2[i, j] \in \{0, 1\}, i \in [1, 2, \ldots, h], j \in [1, 2, \ldots, w]\}$

Step 1. $R_1[i, j] = f_{ran}(.)$, for all i and j. // Create R_1 as a cipher-grid

Step 2. $R_2[S(0)] = f_{equ}(R_1[S(0)])$. // Create the white area of R_2 corresponding to S by R_1

Step 3. $R_2[S(1)] = f_{com}(R_1[S(1)])$. //Create the black area of R_2 corresponding to S by R_1

The construction of encryption rules of Algorithm 1 will be described in detail, which is in accordance with the steps in Algorithm 1. The construction is as follows.

Step 1. $E_0 = \{[r]\}, E_1 = \{[r]\}R_1$, where r is a random Boolean number.

Step 2. $E_0 = \left\{ \begin{bmatrix} r \\ r \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$.

Step 3. $E_1 = \left\{ \begin{bmatrix} r \\ \bar{r} \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$, where $\bar{r}$ is the complement of r.

Since $r \in \{0,1\}$, we have $E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$ finally.

Theorem 1. E_0 and E_1 of $(2, 2)_1$-RGS are the sets of distribution functions of (2, 2)-PVCS.

Proof. (1) Contrast property. For two participants, $p_{1|1} = 1$, $p_{1|0} = 1/2$, $p_{0|0} = 1/2$ and $p_{0|1} = 0$. There exist $\beta = 1/2$ satisfying $p_{1|1} - p_{1|0} \geq \beta$ and $p_{0|0}\ (Q) - p_{0|1}\ (Q) \geq \beta$. Therefore, E_0 and E_1 satisfy the contrast property of Definition 2.

(2) Security property. For single participant, let D_t ($t \in \{0, 1\}$) denote the set of matrices, obtained by restricting each $n \times 1$ matrix in E_t to the single row. Since $D_0 = D_1 = \{[0], [1]\}$, E_0 and E_1 satisfy the security property of Definition 2.

To sum up, E_0 and E_1 are the sets of distribution functions of (2, 2)-PVCS. ■

Algorithm 2. $(2, 2)_2$-RGS [20]

Input and Output are as same as Algorithm 1.

Step 1. $R_1[i, j] = f_{ran}(.)$, for all i and j. // Create R_1 as a cipher-grid

Step 2. $R_2[S(0)] = f_{equ}(R_1[S(0)])$. // Create the white area of R_2 corresponding to S by R_1

Step 3. $R_2[S(1)] = f_{ran}(.)$, for all i and j. // Create the black area of R_2 corresponding to S

The construction of encryption rules of Algorithm 2 is as follows.

Step 1. $E_0 = \{[r]\}, E_1 = \{[r]\}R_1$, where r is a random Boolean number.

Step 2. $E_0 = \left\{ \begin{bmatrix} r \\ r \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$.

Step 3. $E_1 = \left\{ \begin{bmatrix} r \\ r_1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$, and r_1 is another random number, which is independent with r.

Since $r \in \{0,1\}$ and $r_1 \in \{0,1\}$, $E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$ can be gotten.

Theorem 2. E_0 and E_1 of $(2, 2)_2$-RGS are the sets of distribution functions of (2, 2)-PVCS.

Proof. (1) Contrast property. For two participants, $p1|1 = 3/4$, $p1|0 = 1/2$, $p0|0 = 1/2$ and $p0|1 = 1/4$. There exist $\beta = 1/4$ satisfying $p1|1 - p1|0 \geq \beta$ and $p0|0\ (Q) - p0|1\ (Q) \geq \beta$. Therefore, E0 and E1 satisfy the contrast property of Definition 2.

(2) Security property. For single participant, let D_t ($t \in \{0, 1\}$) denote the set of matrices, obtained by restricting each $n \times 1$ matrix in E_t to the single row. Since $D_0 = \{[0], [1]\}$ and $D_1 = \{[0], [0], [1], [1]\}$, D_0 and D_1 contain the same matrices ([0], [1]) with the same frequencies (1/2). Therefore, E_0 and E_1 satisfy the security property of Definition 2.

To sum up, E_0 and E_1 are the sets of distribution functions of (2, 2)-PVCS. ■

Algorithm 3. $(2, 2)_3$-RGS [20]

Input and Output are as same as Algorithm 1.

Step 1. $R_1[i, j] = f_{ran}(.)$, for all i and j. // Create R_1 as a cipher-grid

Step 2. $R_2[S(0)] = f_{ran}(R_1[S(0)])$. // Create the white area of R_2 corresponding to S by R_1

Step 3. $R_2[S(1)] = f_{com}(.)$, for all i and j. // Create the black area of R_2 corresponding to S

The construction of encryption rules of Algorithm 3 is as follows.

Step 1. $E_0 = \{[r]\}, E_1 = \{[r]\}R_1$, where r is a random Boolean number.

Step 2. $E_0 = \left\{ \begin{bmatrix} r \\ r_1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$, and r_1 is another random number, which is independent with r.

Step 3. $E_1 = \left\{ \begin{bmatrix} r \\ \bar{r} \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$, where $\bar{r}$ is the complement of r.

Since $r \in \{0,1\}$ and $r_1 \in \{0,1\}$, $E_0 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$ can be gotten.

Theorem 3. E_0 and E_1 of $(2, 2)_3$-RGS are the sets of distribution functions of (2, 2)-PVCS.

The proof is like as the proof of Theorem 2.

3.2 (n, n)-RGS

In this section, the n-out-of-n RGS is discussed. It is extended from the (2, 2)-RGS to form a general model. When encrypting the secret image into n cipher-grids, the (n, n)-RGS will recall the $(2, 2)_1$-RGS $(n - 1)$ times.

Algorithm 4. (n, n)-RGS [20]

Input: A binary secret image: $S = \{S[i, j] | \ S[i, j] \in \{0, 1\},\ i \in [1, 2, \ldots, h],\ j \in [1, 2, \ldots, w]\}$ and a number of cipher-grids: n.

Output: n cipher-grids: $R_k = \{R_k[i, j] | R_k[i, j] \in \{0, 1\}, i \in [1, 2,\ldots, h], j \in [1, 2, \ldots, w]\}$, where $k = 1, 2,\ldots, n$

Step 1. $R_1 \| \Re_2 = (2, 2)_1$-RGS(S). // Create R_1, $\Re_2$ as two cipher-grids

Step 2. If ($n > 2$) { for $k = 2$ to $n - 1$ $R_k \| \Re_{k+1} = (2, 2)_1$-RGS($\Re_k$)} // Create $R_2 \sim R_{n-1}$ as cipher-grids recursively

Step 3. $R_n = \Re_n$. // Create R_n as the last cipher-grid

The construction of encryption rules of Algorithm 4 is as follows.

Step1. $E_0^2 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$, $E_1^2 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ \Re_2 \end{matrix}$.

Step2. $E_0 = \left\{ \begin{bmatrix} 1 \\ E_1^2 \end{bmatrix}, \begin{bmatrix} 0 \\ E_0^2 \end{bmatrix} \right\}$, $E_1 = \left\{ \begin{bmatrix} 1 \\ E_0^2 \end{bmatrix}, \begin{bmatrix} 0 \\ E_1^2 \end{bmatrix} \right\} \begin{matrix} R_1 \\ \Re_2 \end{matrix}$.

$$\Rightarrow E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ \Re_3 \end{matrix}.$$

Step2'.

$$E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ E_0^2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ E_1^2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ E_1^2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ E_0^2 \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ E_1^2 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ E_0^2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ E_0^2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ E_1^2 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ \Re_3 \end{matrix}$$

$$\Rightarrow E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ R_3 \\ \Re_4 \end{matrix},$$

$$E_1 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ R_3 \\ \Re_4 \end{matrix}.$$

……

Step 3. E_0 is the set of all Boolean vectors of length n with an *even* number of ones, and E_1 is the set of all Boolean vectors of length n with an *odd* number of ones. Hence, $| E_0| = | E_1| = 2^{n-1}$.

Theorem 4. E_0 and E_1 of (n, n)-RGS are the sets of distribution functions of (n, n)-PVCS.

Proof. (1) Contrast property. For n participants, $p_{1|1} = 1$, $p_{1|0} = 1 - 2^{1-n}$, $p_{0|0} = 2^{1-n}$ and $p_{0|1} = 0$. There exist $\beta = 2^{1-n}$ satisfying $p_{1|1} - p_{1|0} \geq \beta$ and $p_{0|0}(Q) - p_{0|1}(Q) \geq \beta$. Therefore, E_0 and E_1 satisfy the contrast property of Definition 2.

(2) Security property. Let B_0 (resp. B_1) be a $n \times 2^{n-1}$ matrix, which is constructed by connecting all vectors of E_0 (resp. E_1). It is interesting that B_0 and B_1 are the basis matrices of (n, n)-VCS proposed by Naor and Shamir [1]. Therefore, E_0 and E_1 satisfy the security property of Definition 2.

To sum up, E_0 and E_1 are the sets of distribution functions of (n, n)-PVCS. ■

3.3 (2, *n*)-RGS

In this section, the 2-out-of-n RGS is analyzed. Assume a secret image S will be encrypted into n cipher-grids $R_1, R_2, \ldots, R_n$. The decryption process is superimposing directly any pair of cipher-grids and the original secret can be disclosed.

Algorithm 5. (2, *n*)-RGS [20]

Input: A binary secret image: $S = \{S[i, j] | \ S[i, j] \in \{0, 1\}, \ i \in [1, 2, \ldots, h], j \in [1, 2, \ldots, w]\}$ and a number of cipher-grids: n.

Output: n cipher-grids: $R_k = \{R_k[i, j] | \ R_k[i, j] \in \{0, 1\}, \ i \in [1, 2, \ldots, h], j \in [1, 2, \ldots, w]\}$, where $k = 1, 2, \ldots, n$

Step 1. $R_1[i, j] = f_{ran}(.)$, for all i and j. // Create R_1 as a cipher-grids

Step 2. For $k = 2$ to n // Create $R_2 \sim R_n$ as cipher-grids repeatedly

$$R_k[S(0)] = f_{equ}(R_{k-1}[S(0)]) \ //\text{Create the white area of } R_k$$
$$R_k[S(1)] = f_{ran}(.) \text{ for all } i \text{ and } j \ //\text{Create the black area of } R_k$$

The construction of encryption rules of Algorithm 5 is as follows.

Step1. $E_0 = \{[r]\}, E_1 = \{[r]\}R_1$

Step2. $E_0 = \left\{ \begin{bmatrix} r \\ r \end{bmatrix} \right\}, \ E_1 = \left\{ \begin{bmatrix} r \\ r_1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$

$$\Rightarrow E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}, \ E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \end{matrix}$$

Step3. $E_0 = \left\{ \begin{bmatrix} r \\ r \\ r \end{bmatrix} \right\}, \ E_1 = \left\{ \begin{bmatrix} r \\ r_1 \\ r_2 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ R_3 \end{matrix} \Rightarrow E_0 = \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\},$

$$E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ R_3 \end{matrix}$$

……

Step n. $E_0 = \left\{ \begin{bmatrix} r \\ r \\ \dots \\ r \end{bmatrix} \right\}, E_1 = \left\{ \begin{bmatrix} r \\ r_1 \\ \dots \\ r_{n-1} \end{bmatrix} \right\} \begin{matrix} R_1 \\ R_2 \\ \dots \\ R_n \end{matrix}$. r, r_1, …, r_{n-1} are random Boolean numbers, where any one of them is independent with others. Hence, $|E_1| = 2$ and $|E_1| = 2^n$.

Theorem 5. E_0 and E_1 of (2, n)-RGS are the sets of distribution functions of (2, n)-PVCS.

Proof. (1) Contrast property. For two participants, p1|1 = 3/4, p1|0 = 1/2, p0|0 = 1/2 and p0|1 = 1/4. There exist β=1/4 satisfying p1|1 − p1|0 ≥ β and p0|0 (Q) − p0|1 (Q) ≥ . Therefore, E0 and E1 satisfy the contrast property of Definition 2.

(2) Security property. For single participant, let D_t ($t \in \{0, 1\}$) denote the set of matrices, obtained by restricting each $n \times 1$ matrix in E_t to the single row. Since $D_0 = \{[0], [1]\}$ and D_1 consists of 2^{n-1} [0] and 2^{n-1} [1], D_0 and D_1 contain the same matrices ([0], [1]) with the same frequencies (1/2). Therefore, E_0 and E_1 satisfy the security property of Definition 2.

To sum up, E_0 and E_1 are the sets of distribution functions of (2, n)-PVCS. ■

3.4 (*k*, *n*)-RGS

In this section, (k, n)-RGS can encode a binary secret image S with the size of $h \times w$ into n random grids, denoted as $\{R_1, R_2, \dots, R_n\}$, which are so noise-like that no one can recognize the original secret information by any set of less than k random grids. In the decoding process, if participants collect and superimpose k or more random grids, denoted as $\{R_{i1}, R_{i2}, \dots, R_{ik}\}$ where $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$, the secret information can be disclosed by human visual system without extra computation cost.

Algorithm 6. (*k*, *n*)-RGS [21]

Step 1. Exploit traditional RGS to encode a pixel $S[i, j] \in S$ so that two bits R_1 and $\Re_2$ are obtained, $[i, j]$ being the pixel position in the secret image ($i \in [1, \dots, h]$ and $j \in [1, \dots, w]$). Encode $\Re_2$ in the same way to generate two bits R_2 and $\Re_3$. Repeat this operation until $R_1, R_2, \dots, \Re_k$ are generated (the final bit $\Re_k$ represented as R_k).

Step 2. The generated k bits are dispatched into k randomly selected random grid pixels $\{ R_{i1}[i, j], R_{i2}[i, j], \dots, R_{ik}[i, j]\}$, a subset of $\{ R_1[i, j], R_2[i, j], \dots, R_n[i, j]\}$; these k bits are arranged at the same spatial location, say $[i, j]$, in the individual random grids $R_{i1}, R_{i2}, \dots$, and R_{ik} .

Step 3. Lastly, the $(n - k)$ bits located in the same location $[i, j]$ of the remaining $(n-k)$ random grids $\{ R_1, R_2, \dots, R_n\} - \{ R_{i1}, R_{i2}, \dots, R_{ik} \}$ are generated by the function $f_{ran}(.)$ used to randomly select "0" or "1", representing a transparent or opaque pixel, respectively.

Step 4. Repeat Steps 1 ∼ 3 until all pixels $S[i, j]$ of secret image S are done.

The construction of encryption rules of Algorithm 6 is as follows.

$$E_0 = \left\{ \begin{bmatrix} E_0^k \\ r_{1,1} \\ r_{1,2} \\ \cdots \\ r_{1,n-k} \end{bmatrix}, \begin{bmatrix} r_{2,1} \\ E_0^k \\ r_{2,2} \\ \cdots \\ r_{2,n-k} \end{bmatrix}, \ldots, \begin{bmatrix} r_{C(n,k),1} \\ r_{C(n,k),2} \\ \cdots \\ r_{C(n,k),n-k} \\ E_0^k \end{bmatrix} \right\}, \; E_1 = \left\{ \begin{bmatrix} E_1^k \\ r_{1,1} \\ r_{1,2} \\ \cdots \\ r_{1,n-k} \end{bmatrix}, \begin{bmatrix} r_{2,1} \\ E_1^k \\ r_{2,2} \\ \cdots \\ r_{2,n-k} \end{bmatrix}, \ldots, \begin{bmatrix} r_{C(n,k),1} \\ r_{C(n,k),2} \\ \cdots \\ r_{C(n,k),n-k} \\ E_1^k \end{bmatrix} \right\}.$$

E_0^k and E_1^k are the encryption rules of (n, n)-RGS in Algorithm 4.
$| E_0| = | E_1| = C(n, k) \times 2^{k-1} \times 2^{n-k} = C(n, k) \times 2^{n-1}$.

Theorem 6. E_0 and E_1 of (k, n)-RGS are the sets of distribution functions of (k, n)-PVCS.

Proof. (1) Contrast property. For k participants, $p_{1|1} - p_{1|0} = \frac{1}{C(n,k)\times 2^{n-1}}$. Since $p_{0|1} = 1 - p_{1|1}$ and $p_{0|0} = 1 - p_{1|0}$, we have $\beta = p_{0|0} - p_{0|1} = p_{1|1} - p_{1|0} = \frac{1}{C(n,k)\times 2^{n-1}}$. Therefore, E_0 and E_1 satisfy the contrast property of Definition 2.

(2) Security property. For $k - 1$ participant, let D_t ($t \in \{0, 1\}$) denote the set of matrices, obtained by restricting each $n \times 1$ matrix in E_t to the $k - 1$ rows. Every matrix of D_0 (resp. D_1) has the character that i ($i \in [0,\ldots, k - 1]$) rows are from E_0^k(resp. E_1^k) and the other $k - 1 - i$ rows are random Boolean numbers. According to the security of E_0^k and E_1^k, we have $D_0^i = D_1^i$ for any i ($i \in [0,\ldots, k–1]$) participants. Therefore, $D_0 = D_1$, which means that E_0 and E_1 satisfy the security property of Definition 2.

To sum up, E_0 and E_1 are the sets of distribution functions of (k, n)-PVCS. ■

4 Experimental Results and Discussions

4.1 Codebook and Computational Complexity

The encryption of PVCS relies on codebook C_0 and C_1, which is easy to generate shares but needs more storage space costs than RGS. The encryption of RGS is realized by several recursive computing steps, which does not need codebook but requires more computing resources than PVCS.

Generally speaking, the complexity evaluation of an algorithm contains two aspects: space and time. PVCS and RGS are just good at one point, respectively. In some sense, PVCS and RGS are complementation for each other.

4.2 Contrasts of PVCS and RGS

The evaluation of contrast property in PVCS is $\beta = p_{0|0} - p_{0|1}$. In RGS, the recovery image is evaluated by $\alpha = \frac{T(B[A(0)]) - T(B[A(1)])}{1+T(B[A(1)])}$. α is used for measuring decrypted image as a whole. Since each pixel in original image is encrypted independently, we have $T(B[A(0)]) = p_{0|0}$ and $T(B[A(1)]) = p_{0|1}$. Therefore,

$$\alpha = \frac{p_{0|0} - p_{0|1}}{1 + p_{0|1}} = \frac{\beta}{1 + p_{0|1}}.$$

The recovery effects of PVCS and RGS can be compared under the same parameter α or β. For each RGS, there always exists a PVCS corresponding to it. However, transforming any PVCS to RGS can not be guaranteed, since some PVCSs can not be expressed by just f_{equ}, f_{ran} and f_{com}. Therefore, for (k, n) scheme, we have the following equations:

$$\alpha_{RGS} \leq \alpha_{PVCS} \text{ or } \beta_{RGS} \leq \beta_{PVCS}.$$

Taking (3, 4) scheme for example, a secret image S of size 512×512 pixels is encrypted. RGS is realized according to Algorithm 6. For PVCS, we construct C_0 and C_1 as follows.

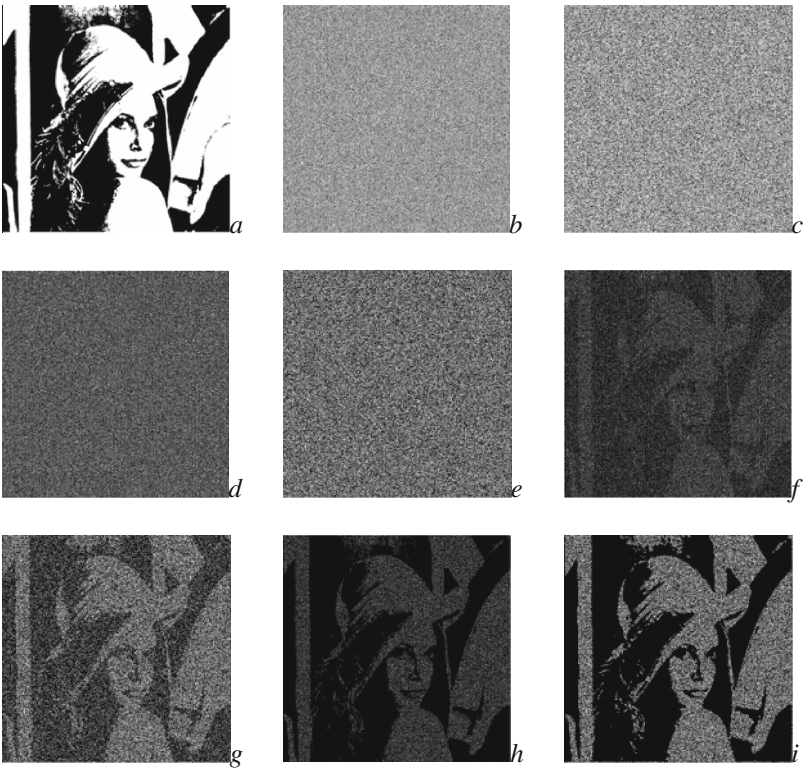

Fig. 1. The experimental results of the (3, 4)-RGS and (3, 4)-PVCS: (a) secret image S, (b) single grid of RGS with $\alpha_{RGS} = 0$, (c) single share of PVCS with $\alpha_{PVCS} = 0$, (d) two overlapped grids of RGS with $\alpha_{RGS} = 0$, (e) two overlapped shares of PVCS with $\alpha_{PVCS} = 0$, (f) three overlapped grids of RGS with $\alpha_{RGS} = 2/35$, (g) three overlapped shares of PVCS with $\alpha_{PVCS} = 1/7$, (h) four overlapped grids of RGS with $\alpha_{RGS} = 1/8$, (i) four overlapped shares of PVCS with $\alpha_{PVCS} = 1/3$.

$$C_0 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right\}, \; C_1 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

Figure 1 shows the results of (3, 4)-RGS and (3, 4)-PVCS, which encrypt secret S (Fig. 1(a)) into four random grids and shares, respectively. Nobody can recognize the original secret from single grid (Fig. 1(b)) or single share (Fig. 1(c)). Figure 1(d)–(e) show the noise-like decoding effects of two grids and two shares, respectively. The secret information can be recognized by stacking three grids or three shares, shown in Fig. 1(f)–(g) with contrast $\alpha_{RGS} = 2/35 < \alpha_{PVCS} = 1/7$. All grids or shares stacked, the reconstructed secrets are shown in Fig. 1(h) and Fig. 1(i) with contrast $\alpha_{RGS} = 1/8 < \alpha_{PVCS} = 1/3$.

5 Conclusion

The relationship between VCS and RGS is analyzed for the first time. It is interesting that the encryption rules of RGS are actually the set of distribution matrices in PVCS. Considering the costs of algorithms, PVCS is good at the computational complexity while RGS has advantage in no codebook needed. Generally speaking, the contrast of PVCS is better than RGS under the same access structure. Our future work is how to improve the contrast of RGS.

Acknowledgment. This work was supported by the National Natural Science Foundation of the People's Republic of China under Grant No. 61070086. The authors would like to thank the anonymous reviewers for their valuable comments.

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. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: Merwin, R.E., Zanca, J.T., Smith, M. (eds.) National Computer Conference, vol. 48, pp. 242–268. IEEE, New York (1979)
4. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**, 86–106 (1996)
5. Hsu, C.-S., Tu, S.-F., Hou, Y.-C.: An optimization model for visual cryptography schemes with unexpanded shares. In: Esposito, F., Raś, Z.W., Malerba, D., Semeraro, G. (eds.) ISMIS 2006. LNCS (LNAI), vol. 4203, pp. 58–67. Springer, Heidelberg (2006)
6. Liu, F., Wu, C., Lin, X.: Step construction of visual cryptography schemes. IEEE Trans. Inf. Forensics Secur. **5**, 27–38 (2010)
7. Shyu, S.J., Chen, M.C.: Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **6**, 960–969 (2011)

8. Yang, C.N., Wang, C.C., Chen, T.S.: Visual cryptography schemes with reversing. Comput. J. bxm118, pp. 1–13 (2008)
9. Lin, C.C., Tai, W.H.: Visual cryptography for gray-level images by dithering techniques. Pattern Recogn. Lett. **24**, 349–358 (2003)
10. Cimato, S., Prisco, R.D., Santis, A.D.: Optimal colored threshold visual cryptography schemes. Des. Codes Crypt. **35**, 311–335 (2005)
11. Yang, C.N., Chen, T.S.: Colored visual cryptography scheme based on additive color mixing. Pattern Recogn. **41**, 3114–3129 (2008)
12. Shyu, S.J.: Efficient visual secret sharing scheme for color images. Pattern Recogn. **35**, 866–880 (2006)
13. Ito, R., Hatsukazu, T.: Image size invariant visual cryptography. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E82-A**, 2172–2177 (1999)
14. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. **25**, 481–494 (2004)
15. Yang, C.N., Chen, T.S.: Size-adjustable visual secret sharing schemes. IEICE Trans. Fundam. **E88-A**, 2471–2474 (2005)
16. Cimato, S., Prisco, R.D., Santis, A.D.: Probabilistic visual cryptography schemes. Comput. J. **49**, 97–107 (2006)
17. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**, 377–379 (1987)
18. Shyu, S.J.: Image encryption by random grids. Pattern Recogn. **40**, 1014–1031 (2007)
19. Shyu, S.J.: Image encryption by multiple random grids. Pattern Recogn. **42**, 1582–1596 (2009)
20. Chen, T.H., Tsao, K.H.: Visual secret sharing by random grids revisited. Pattern Recogn. **42**, 2203–2217 (2009)
21. Chen, T., Tsao, K.: Threshold visual secret sharing by random grids. J. Syst. Softw. **84**, 1197–1208 (2011)