Published in IET Information Security
Received on 28th September 2011
Revised on 7th July 2012
doi: 10.1049/iet-ifs.2012.0046

ISSN 1751-8709

Visual secret sharing for general access structures by random grids

X. Wu[1] *W. Sun*[2]

[1]*School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, People's Republic of China*
[2]*School of Software, Sun Yat-sen University, Guangzhou 510006, People's Republic of China*
E-mail: sunwei@mail.sysu.edu.cn

Abstract: Visual secret sharing (VSS) is a way to protect a secret image among a group of participants by using the notions of perfect ciphers and secret sharing. However, each share generated by conventional VSS is m times as big as the original secret image, where m is called pixel expansion. Random grid (RG) is an alternative approach to implement VSS without pixel expansion. However, reported RG-based VSS methods are threshold schemes. In this study, RG-based VSS for general access structures is presented. Secret image is encoded into n RGs while qualified sets can recover the secret visually and forbidden sets cannot. The proposed scheme is a generalisation of the threshold methods, where those reported RG-based schemes can be considered as the special cases of the proposed scheme. Experimental results are provided, demonstrating the effectiveness and advantages of the proposed scheme.

1 Introduction

Sensitive digital contents kept by only one person is easily lost or destructed. Secret sharing is a method to share the secret information among a group of participants against destruction and modification. The basic concept of secret sharing was introduced by Blakley [1] and Shamir [2] independently in 1979.

Visual secret sharing (VSS), which is also called visual cryptography, is a novel type of secret sharing that focuses on sharing images. An initial model of VSS was proposed by Naor and Shamir [3] in 1995. In a (k, n)-threshold scheme, a binary secret image is encrypted into n meaningless images called shares or shadows, which are then distributed to n associated participants. When any k or more participants share their shadows, the secret image is visually revealed by printing their shares on transparencies and stacking them together. However, the stacked results of any $k-1$ or less shares give no clue about the secret. Advanced merit of VSS is that the decryption is completely based on human visual system without the aid of computers.

A simple construction of a 2-out-of-2 VSS is given in Fig. 1. Every secret pixel p is encrypted into the subpixel patterns which are pre-defined in the six columns of Fig. 1. If p is a white (resp. black) pixel, one of the six columns is randomly chosen with equal probabilities and replaced p. Each pattern gives no clue about the associated secret pixel, since each of them contains two black and two white subpixels. When two associated patterns are stacked together, a secret pixel is visually revealed. The stacked result is interpreted as black when four black subpixels are recovered. Whereas, the stacked result is interpreted as white when two black and two white subpixels are reconstructed. An example of a 2-out-of-2 VSS scheme is demonstrated in Fig. 2, where the original secret image is shown in Fig. 2*a*, two shares generated by the construction are illustrated in Figs. 2*b* and *c*, and the stacked result of the two shares is given in Fig. 2*d*.

In conventional VSS, a code book (all the pre-defined patterns) is required for share construction. Each pattern in the code book consists of $m \geq 2$ black and white pixels, where m is referred to pixel expansion. In the above example, $m = 4$. Pixel expansion indicates that each share is m times as big as the original secret image. Transmitting and storing the shares would be further burdened by pixel expansion problem.

Based on the pioneer work of Naor and Shamir, wide studies on VSS were presented. Constructions of VSS for general access structures were discussed in [4, 5]. Investigations on bounds and contrast were presented in [6–8]. Schemes for sharing grey-level images and colour images were proposed in [9–11]. However, three deficiencies are remained in these mentioned conventional VSS schemes, as described below.

- *Pixel expansion:* The share is $m \geq 2$ times as big as the original secret image. When the number of participants increases, m becomes much larger. Pixel expansion problem further burdens the shared data transmission and storage.
- *Tailor-made code book required:* In general, the (k, n)-threshold conventional VSS schemes with different k and n always need different code books. Sometimes, the design of code book for a specific sharing strategy is not trivial.
- *Shape distortion:* The aspect ratio of encoded share is sometimes changed because of the effect of pixel expansion.

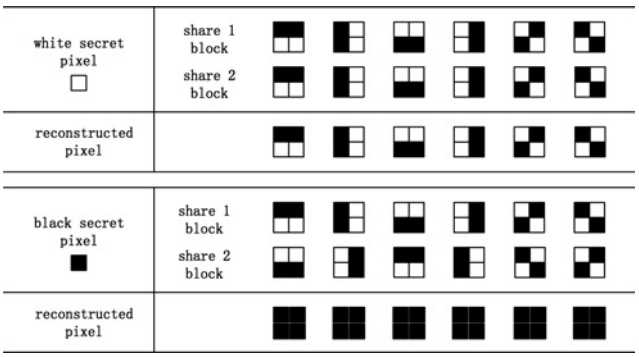

Fig. 1 *Construction of a 2-out-of-2 VSS scheme*

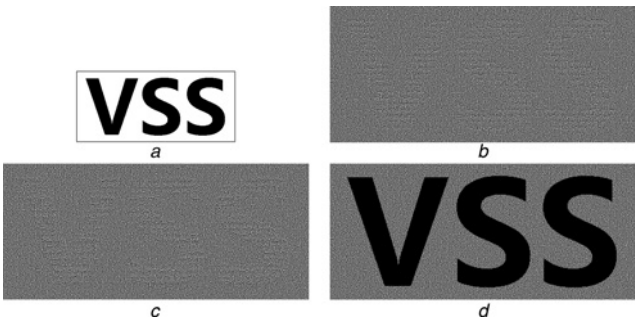

Fig. 2 *Example of a 2-out-of-2 VSS scheme*

a Secret image
b First share
c Second share
d Reconstructed secret image

Probabilistic VSS, which is one of the most significant branch of conventional VSS, was proposed to solve the pixel expansion problem. Ito *et al.* [12] introduced a size invariant VSS that encodes a black (resp. white) pixel by a column selected from the black (resp. white) basis matrix with equal probabilities. Yang [13] proposed several constructions for implementing non-expansible probabilistic VSS. Cimato *et al.* [14] further extended the model proposed by Yang to form a generalised probabilistic VSS. For $m = 1$, their method reduces to the one of Yang. For big enough value of m, for which a deterministic scheme exists, their method reduces to the classical deterministic model. However, the mentioned probabilistic approaches still require tailor-made code book for encryption. Further, those methods are just designed for the threshold schemes, whereas the cases for general access structures are not considered.

Usually, the code book can be constructed by permuting the columns in the basis matrices in all possible ways. To a certain degree, the basis matrices can partially alleviate the burden of constructing code book. However, sometimes, designing such tailor-made basis matrices is complicated as well.

In order to keep aspect ratio as well as decrease the pixel expansion, aspect ratio-invariant VSS schemes were proposed by Yang and Chen [15, 16]. The secret pixels are represented by fewer subpixels at the expense of lowering the quality of the reconstructed secret image.

Random grid (RG) is an alternative approach to realise VSS. Advanced properties of the RG-based VSS are: (i) the generated share is the same size as the original secret image, and (ii) code book is not required for constructing the shares. The most significant difference between RG-based VSS and conventional VSS is that, the three potential deficiencies in conventional VSS are removed in RG-based VSS. To encrypt a secret image into two shares, Kafri and Keren [17] first introduced three different algorithms. A binary secret image is encoded into two RGs in which the areas containing information in the two RGs are intercorrelated. When the two RGs are superimposed together, the correlated areas are visually revealed from the random background because of the difference in light transmission. Inspired by Kafri and Keren, Shyu [18] proposed an approach to share a grey scale/colour image into two RGs. Later, the same author [19] introduced a methodology to conceal an image into multiple RGs. Chen and Tsao [20] further extended Kafri and Keren's methods to 2-out-of-n and n-out-of-n schemes. Recently, Chen and Tsao [21] proposed a construction for the (k, n)-threshold RG-based VSS. However, complicated sharing strategy cannot be fully implemented by those mentioned RG-based VSS schemes, since they are all threshold cases. There are many real-life examples that can only be implemented by access structures. The following example can be considered. According to the policy of a graduate school, a graduate who applies a postgraduate position must have letters of recommendation. Suppose that the candidate must have at least one recommendation letter from a professor and one from an associated professor. There are totally one professor (P_1) and two associated professors (P_2 and P_3). As a result, recommendations from $\{P_1, P_2\}$, $\{P_1, P_3\}$ or $\{P_1, P_2, P_3\}$ are all acceptable. However, recommendations from $\{P_1\}$, $\{P_2\}$, $\{P_3\}$ or $\{P_2, P_3\}$ are rejected.

In this paper, we further exploit the capacity of RG to develop RG-based VSS for general access structures. More complicated sharing strategies can be implemented by the proposed scheme. Meanwhile, threshold schemes can be considered as special cases of the proposed method.

The remaining part of this paper is organised as follows. Section 2 describes three image encryption algorithms proposed by Kafri and Keren [17] and the concept of VSS for general access structures [4]. The proposed algorithm is demonstrated in Section 3. Also, analysis and proofs on the properties of the proposed scheme are provided. Experimental results and discussions are illustrated in Section 4. Section 5 concludes our work.

2 Related works

2.1 Sharing a binary image into two RGs

Kafri and Keren [17] defined an RG as a transparency comprising a two-dimensional array of pixels. Each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. There is no correlation between the values of different pixels in the array.

To share a binary secret image, three distinct algorithms were proposed by Kafri and Keren. The algorithms encrypt a binary secret image $\boldsymbol{S}$ into two RGs, denoted as $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$. When $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$ are stacked together, the secret image is visually recovered. Let $\otimes$ denote the Boolean OR operation. The stacked result of two RGs is represented by $\boldsymbol{R}_1 \otimes \boldsymbol{R}_2$. The three encryption algorithms are described as follows.

Algorithm 1–3: Sharing a binary image into two RGs.
Input: A $M \times N$ binary secret image $\boldsymbol{S}$.
Output: Two RGs $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.

doi: 10.1049/iet-ifs.2012.0046

$[\boldsymbol{R}_1, \boldsymbol{R}_2] = \text{Encryption}(\boldsymbol{S})$ (Figs. 3–5).

Procedure 'Encryption' can be implemented by any one of Algorithms 1, 2 or 3. To analyse RG-based VSS, light transmission, area representation and contrast are used, as defined as follows.

Definition 1 (average light transmission): For a certain pixel r in a binary image $\boldsymbol{R}$ whose size is $M \times N$, the light transmission of a white pixel is defined as $T(r) = 1$; whereas, $T(r) = 0$ for r is a black pixel. Totally, the average light transmission of $\boldsymbol{R}$ is defined as

$$T(\boldsymbol{R}) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(\boldsymbol{R}(i,j))}{M \times N} \tag{1}$$

Definition 2 (area representation): Let $\boldsymbol{S}(0)$ (resp. $\boldsymbol{S}(1)$) be the area of all the white (resp. black) pixels in secret image $\boldsymbol{S}$ where $\boldsymbol{S} = \boldsymbol{S}(0) \cup \boldsymbol{S}(1)$ and $\boldsymbol{S}(0) \cap \boldsymbol{S}(1) = \emptyset$. Therefore $\boldsymbol{R}[\boldsymbol{S}(0)]$ (resp. $\boldsymbol{R}[\boldsymbol{S}(1)]$) is the corresponding area of all the white (resp. black) pixels in image $\boldsymbol{R}$.

Definition 3 (contrast): The contrast of the reconstructed secret image $\boldsymbol{R}_{\boldsymbol{R}_1 \otimes \cdots \otimes \boldsymbol{R}_n} = \boldsymbol{R}_1 \otimes \cdots \otimes \boldsymbol{R}_n$ with respect to the original secret image $\boldsymbol{S}$ is

$$\alpha = \frac{T(\boldsymbol{R}_{\boldsymbol{R}_1 \otimes \cdots \otimes \boldsymbol{R}_n}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{\boldsymbol{R}_1 \otimes \cdots \otimes \boldsymbol{R}_n}[\boldsymbol{S}(1)])}{1 + T(\boldsymbol{R}_{\boldsymbol{R}_1 \otimes \cdots \otimes \boldsymbol{R}_n}[\boldsymbol{S}(1)])}$$

Contrast α is considered to be as large as possible. Secret information in the reconstructed secret image can be easily identified by naked eye with large α. Let α_1, α_2 and α_3 be the contrasts of the reconstructed secret images by Figs. 3–5, respectively. In [18], they are calculated as

$$\alpha_1 = \frac{(1/2) - 0}{1 + 0} = \frac{1}{2}, \quad \alpha_2 = \frac{(1/2) - (1/4)}{1 + (1/4)} = \frac{1}{5}$$

$$\text{and } \alpha_3 = \frac{(1/4) - 0}{1 + 0} = \frac{1}{4}$$

We know that recovered secret image by Algorithm 1 achieves the best visual quality.

Algorithm 1:
Step 1: Construct an $M \times N$ matrix $\boldsymbol{R}_1$ whose elements are randomly assigned the value 0 (white) or 1 (black).
Step 2: For each pixel at position (i, j) of $\boldsymbol{S}$, compute

$$\boldsymbol{R}_2(i,j) = \begin{cases} \boldsymbol{R}_1(i,j) & \text{if } \boldsymbol{S}(i,j) = 0 \\ \overline{\boldsymbol{R}_1(i,j)} & \text{otherwise} \end{cases}$$

where $\overline{\boldsymbol{R}_1(i,j)}$ is the inverse of $\boldsymbol{R}_1(i,j)$.
Step 3: Output the two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.

Fig. 3 *Algorithm 1*

Algorithm 2:
Step 1: Construct a $M \times N$ matrix $\boldsymbol{R}_1$ whose elements are randomly assigned the value 0 (white) or 1 (black).
Step 2: For each pixel at position (i, j) of $\boldsymbol{S}$, compute

$$\boldsymbol{R}_2(i,j) = \begin{cases} \boldsymbol{R}_1(i,j) & \text{if } \boldsymbol{S}(i,j) = 0 \\ d & \text{otherwise} \end{cases}$$

where d is randomly chosen from {0, 1}.
Step 3: Output the two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.

Fig. 4 *Algorithm 2*

Algorithm 3:
Step 1: Construct an $M \times N$ matrix $\boldsymbol{R}_1$ whose elements are randomly assigned the value 0 (white) or 1 (black).
Step 2: For each pixel at position (i, j) of $\boldsymbol{S}$, compute

$$\boldsymbol{R}_2(i,j) = \begin{cases} d & \text{if } \boldsymbol{S}(i,j) = 0 \\ \overline{\boldsymbol{R}_1(i,j)} & \text{otherwise} \end{cases}$$

where d is randomly chosen from {0, 1}.
Step 3: Output the two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.

Fig. 5 *Algorithm 3*

2.2 General access structures of conventional VSS

Let $P = \{1, \ldots, n\}$ be a set of elements called participants of a VSS scheme and let 2^P denote the set of all subsets of P. Let $\Gamma_{\text{Qual}} \subseteq 2^P$ and $\Gamma_{\text{Forb}} \subseteq 2^P$, where $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$. Members of Γ_{Qual} are defined as qualified sets and members of Γ_{Forb} are defined as forbidden sets. The pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called the access structure of this scheme [4].

Define Γ_0 to consist of all the minimal qualified sets

$$\Gamma_0 = \{Q \in \Gamma_{\text{Qual}} : Q' \notin \Gamma_{\text{Qual}}, \quad \text{for all } Q' \subset Q\}$$

A participant $p \in P$ is an essential participant if there exists a set X such that $X \cup \{p\} \in \Gamma_{\text{Qual}}$ but $X \notin \Gamma_{\text{Qual}}$. If a participant p is not essential, then we can construct a VSS scheme by giving him a share completely white or even nothing as his share. A non-essential participant does not need to participant actively in the reconstruction of the image, since the information in his share is not needed by any subset in P. In this paper, all participants are assumed to be essential.

In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = 2^P$, the access structure is said to be strong, and Γ_0 is termed a basis.

In conventional VSS, a secret pixel is encoded into n-shared pixels. Each shared pixel contains m black and white subpixels. This can be described by an $n \times m$ Boolean matrix $\boldsymbol{S} = [s_{ij}]$, where $s_{ij} = 1$, if and only if, the jth subpixel in the ith transparency is black. The grey level of the combined share, obtained by stacking the transparencies $i_1, \ldots, i_s$, is proportional to the Hamming weight $H(V)$ of the $\boldsymbol{m}$-vector $\boldsymbol{V} = \text{OR}(r_{i_1}, \ldots, r_{i_s})$ where $r_{i_1}, \ldots, r_{i_s}$ are the rows of $\boldsymbol{S}$ associated with the transparencies we stack. The grey level is interpreted by human visual system as black or white in accordance with the contrast.

Definition 4: Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on a set of n participants. A $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ VSS scheme with pixel expansion m, relative difference $\alpha(m)$ and set of thresholds $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$ is realised using the two collections of $n \times m$ Boolean matrices $\boldsymbol{C}_0$ and $\boldsymbol{C}_1$ if the following two conditions are satisfied.

(i) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$ (i.e. if X is a qualified set), then the $\boldsymbol{V}$ of rows $i_1, i_2, \ldots, i_p$ of any $\boldsymbol{M} \in \boldsymbol{C}_0$ meets $H(\boldsymbol{V}) \leq t_X - \alpha(m) \times m$, whereas for any $\boldsymbol{M} \in \boldsymbol{C}_1$, it results that $H(\boldsymbol{V}) \geq t_X$.
(ii) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$ (i.e. if X is a forbidden set), the two collections of $p \times m$ matrices $\boldsymbol{D}_t$ with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in $\boldsymbol{C}_t$ to rows $i_1, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first condition makes sure that any qualified set can visually recover the secret image. The second condition guarantees that any forbidden set gives no clue about the secret image.

3 Proposed algorithm

RG-based VSS for general access structures is proposed in this section. Access structures in this paper are considered to be strong. That is, Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$. In the proposed scheme, each participant is considered to be essential. Briefly speaking, each participant is listed in the qualified set. Moreover, each qualified set contains at least two or more participants according to the concept of secret sharing.

In the share construction phase, a trusted party called dealer and n participants are involved. A secret image and an access structure are pre-determined by the dealer and fed to the share construction algorithm as input. Usually, the access structure is constructed by the dealer according to the sharing strategy of the current application, where the application is referred to the scenario to which the VSS scheme is applied, such as the letters of recommendation for applying a postgraduate position and so on. Two cases are considered when the dealer constructs the access structure: (i) the threshold case and (ii) non-threshold case. For the (k, n)-threshold case, the dealer only determines the value of k. The qualified sets can be generated by selecting any $t \geq k$ participants. For the non-threshold case, the minimal qualified sets should be determined first by the dealer according to the application. Then, any set which contains at least one of the minimal qualified sets is selected as qualified set. When the qualified sets are generated, the forbidden sets can be constructed as well. Finally, the access structure is obtained.

In one application, totally n shares are constructed and distributed to n associated participants by the dealer. Every participant would receive the associated share, and must keep it safe. For example, four participants P_1, P_2, P_3 and P_4 are involved. Then, four shares, denoted as $\boldsymbol{R}_1$, $\boldsymbol{R}_2$, $\boldsymbol{R}_3$ and $\boldsymbol{R}_4$, are generated and delivered to P_1, P_2, P_3 and P_4, respectively. P_1 only holds $\boldsymbol{R}_1$, P_2 only holds $\boldsymbol{R}_2$ and so on. For all participants in any one qualified set, they can collaboratively reconstruct the secret image by stacking their own shares together. If two qualified sets $\{P_1, P_2, P_3\}$ and $\{P_1, P_2, P_4\}$ are used, the secret can be visually revealed when participants P_1, P_2, P_3 stack their shares $\boldsymbol{R}_1$, $\boldsymbol{R}_2$, $\boldsymbol{R}_3$ together, as well as when participants P_1, P_2, P_4 superimpose their shares $\boldsymbol{R}_1$, $\boldsymbol{R}_2$, $\boldsymbol{R}_4$. A participant only holds one share and uses the same share to reconstruct the secret in different sets when these sets contain the current participant. Hence, participant P_1 presents his/her same share $\boldsymbol{R}_1$ for revealing the secret of either $\{P_1, P_2, P_3\}$ or $\{P_1, P_2, P_4\}$. However, for participants in the forbidden set, no clue about the secret is revealed. In addition, each participant should in some way identify his/her own share since only the right shares in the qualify set can recover the secret. Note that, each participant only obtains one share in one application. However, one participant can be involved in multiple applications. The number of shares held by a participant depends on the number of applications he/she gets involved in. If a participant gets involved in multiple applications, some skills such as marking some special symbols on the associated shares can help the participant to identify the right share and present it for revealing the secret. However, those marked symbols should be removable and not damage the share.

Diagram of the share construction for binary images is shown in Fig. 6. For encoding each secret pixel, one minimal qualified set $\{i_1, \ldots, i_p\}$ is randomly chosen from the set of minimal qualified sets Γ_0, where Γ_0 is obtained from the input access structure. p bits are generated according to the (p, p) threshold RG-based VSS [20], and

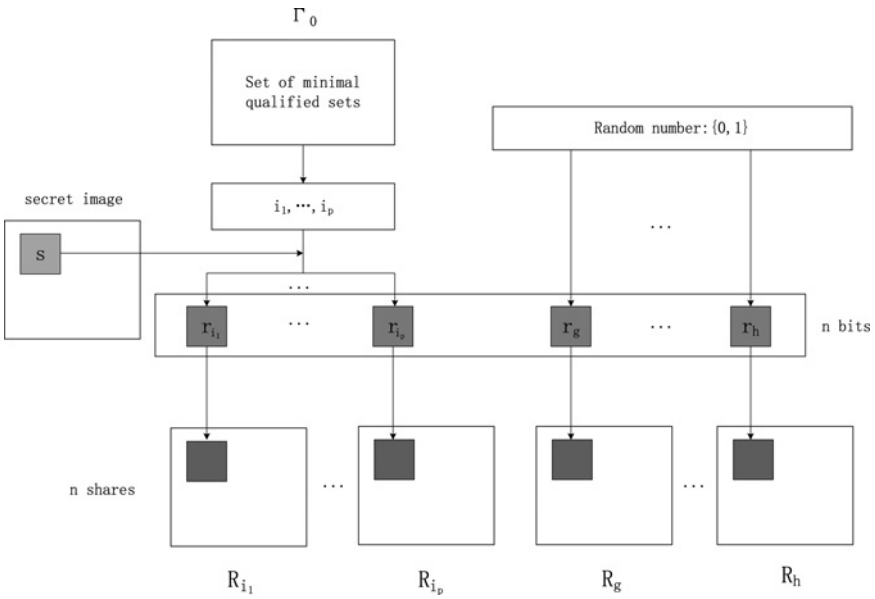

Fig. 6 *Diagram of share construction of the proposed scheme for binary images, where Γ_0 is the set of minimal qualified sets obtained from the access structure; $\{i_1, \ldots, i_p\}$ is a set randomly chosen from Γ_0; $r_{i_1}, \ldots, r_{i_p}$ are the p bits constructed according to (p, p) RG-based VSS; and $r_h, \ldots, r_g$ are the $n - p$ random bits chosen from {0, 1}*

IET Inf. Secur., 2012, Vol. 6, Iss. 4, pp. 299–309
doi: 10.1049/iet-ifs.2012.0046

$n-p$ bits are constructed by randomly assigning them the value 0 or 1. The n generated bits are finally assigned to n associated shares. Detailed description is formulated as follows.

Algorithm 4: The proposed (Γ_{Qual}, Γ_{Forb}) sharing algorithm for binary images.
Input: A $M \times N$ binary secret image $\boldsymbol{S}$ and access structure $\{\Gamma_{Qual}, \Gamma_{Forb}\}$.
Output: n binary shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.
Step 1: Denote Γ_0 as the basis of access structure $\{\Gamma_{Qual}, \Gamma_{Forb}\}$ which consists of all minimal qualified sets.
Step 2: For each pixel at position (i, j) of $\boldsymbol{S}$, repeat Steps 3–8.
Step 3: Randomly select a minimal qualified set $Q = \{i_1, \ldots, i_p\} \in \Gamma_0$ where $p \leq n$.
Step 4: Generate $p-1$ bits $r_{i_1}, \ldots, r_{i_{p-1}}$ by assigning them the value 0 (white) or 1 (black) randomly.
Step 5: Construct r_{i_p} by

$$r_{i_p} = \boldsymbol{S}(i, j) \oplus r_{i_1} \oplus \cdots \oplus r_{i_{p-1}}$$

where $\oplus$ denotes the Boolean XOR operation.
Step 6: Assign the p bits $r_{i_1}, \ldots, r_{i_p}$ to the associated p shares $\boldsymbol{R}_{i_1}(i, j), \ldots, \boldsymbol{R}_{i_p}(i, j)$, respectively.
Step 7: Generate $n-p$ bits $r_g, \ldots, r_h$ by randomly assigning them the value 0 or 1, where $g, \ldots, h$ are the $n-p$ indices in $\{1, \ldots, n\} - \{i_1, \ldots, i_p\}$.
Step 8: Assign the $n-p$ bits $r_g, \ldots, r_h$ to the associated $n-p$ shares $\boldsymbol{R}_g(i, j), \ldots, \boldsymbol{R}_h(i, j)$, respectively.
Step 9: Output the n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.

Participants of any qualified set can visually reconstruct the secret image by stacking their shares together without the aid of any computational devices. Analysis on the proposed scheme is formulated as follows.

Lemma 1: By stacking t independent bits $r_1, \ldots, r_t$ which are randomly assigned the value 0 or 1 to form $r_{1 \otimes \ldots \otimes t}$, the light transmission of the stacked result is

$$T(r_{1 \otimes \cdots \otimes t}) = \left(\frac{1}{2}\right)^t$$

Proof: Since each bit is randomly assigned the value 0 or 1, the probability for $r_i = 0$ $(1 \leq i \leq n)$ is $\text{Prob}(r_i = 0) = (1/2)$. The t bits are independent, the probability for all the t bits to be white is $\text{Prob}(r_1 = 0 \cup \ldots \cup r_t = 0) = (1/2)^t$. The stacked result is white, if and only if, all the t bits are white. We obtain $\text{Prob}(r_{1 \otimes \ldots \otimes t} = 0) = (1/2)^t$. Therefore $T(r_{1 \otimes \ldots \otimes t}) = (1/2)^t$. □

Lemma 2: Given t independent bits $r_1, \ldots, r_t$, which are randomly assigned the value 0 or 1, $r_{1 \oplus \ldots \oplus t} = r_1 \oplus \ldots \oplus_t$ is the XOR result of the t bits. We have

$$\text{Prob}(r_{1 \oplus \cdots \oplus t} = 0) = \text{Prob}(r_{1 \oplus \cdots \oplus t} = 1) = \frac{1}{2}$$

Proof: By induction on t, (1) when $t = 2$, $r_{1 \oplus 2} = r_1 \oplus r_2$. If $r_1 = 0$, $r_2 = 0$ or $r_1 = 1$, $r_2 = 1$, $r_{1 \oplus 2} = 0$. If $r_1 = 1$, $r_2 = 0$ or $r_1 = 0$, $r_2 = 1$, $r_{1 \oplus 2} = 1$. Therefore we have $\text{Prob}(r_{1 \oplus 2} = 0) = \text{Prob}(r_{1 \oplus 2} = 1) = (1/2)$.

(2) Assume that the claim holds for $t-1$, that is, $\text{Prob}(r_{1 \oplus \ldots \oplus t-1} = 0) = \text{Prob}(r_{1 \oplus \ldots \oplus t-1} = 1) = (1/2)$. We need to prove that it also holds for t. For $r_{1 \oplus \ldots \oplus t} = r_{1 \oplus \ldots \oplus t-1} \oplus r_t$, if $r_{1 \oplus \ldots \oplus t-1} = 0$, $r_t = 0$ or $r_{1 \oplus \ldots \oplus t-1} = 1$, $r_t = 1$, $r_{1 \oplus \ldots \oplus t} = 0$. If $r_{1 \oplus \ldots \oplus t-1} = 1$, $r_t = 0$ or $r_{1 \oplus \ldots \oplus t-1} = 0$, $r_t = 1$, $r_{1 \oplus \ldots \oplus t} = 1$. As a result, we have $\text{Prob}(r_{1 \oplus \ldots \oplus t} = 0) = \text{Prob}(r_{1 \oplus \ldots \oplus t} = 1) = 1/2$. □

Lemma 3: Given a secret pixel s and n bits $r_1, \ldots, r_n$, $n-1$ bits $r_1, \ldots, r_{p-1}, r_{p+1}, \ldots, r_n$ are randomly assigned value 0 or 1 and $r_p = s \oplus r_1 \oplus \ldots \oplus r_{p-1}$. The light transmissions of each bit are

$$T(r_i[s = 0]) = T(r_i[s = 1]) = \frac{1}{2}, \quad 1 \leq i \leq n$$

Proof: (i) Since the $n-1$ bits $r_1, \ldots, r_{p-1}, r_{p+1}, \ldots, r_n$ are randomly assigned the value 0 or 1, we obtain $\text{Prob}(r_i = 0) = \text{Prob}(r_i = 1) = 1/2$ for $i = 1, \ldots, p-1, p+1, \ldots, n$. The $n-1$ random bits are independent of the secret pixel s, we have $T(r_i[s = 0]) = T(r_i[s = 1]) = 1/2$ for $i = 1, \ldots, p-1, p+1, \ldots, n$.

(ii) By Lemma 2, we have $\text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 0) = \text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 1) = 1/2$. When $s = 0$, $r_p = s \oplus r_1 \oplus \ldots \oplus r_{p-1} = r_{1 \oplus \ldots \oplus p-1}$. We obtain $\text{Prob}(r_p = 0) = \text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 0) = 1/2$ and $\text{Prob}(r_p = 1) = \text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 1) = 1/2$. That is $T(r_p[s = 0]) = 1/2$. When $s = 1$, $r_p = s \oplus r_1 \oplus \cdots \oplus r_{p-1} = \overline{r_{1 \oplus \cdots \oplus p-1}}$. We obtain $\text{Prob}(r_p = 0) = \text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 1) = 1/2$ and $\text{Prob}(r_p = 1) = \text{Prob}(r_{1 \oplus \ldots \oplus p-1} = 0) = 1/2$. That is $T(r_p[s = 1]) = 1/2$. Hence, $T(r_p[s = 0]) = T(r_p[s = 1]) = 1/2$.

Totally, we have $T(r_i[s = 0]) = T(r_i[s = 1]) = 1/2$, $1 \leq i \leq n$. □

Lemma 4: Given a secret pixel s and n bits $r_1, \ldots, r_n$, $n-1$ bits $r_1, \ldots, r_{p-1}, r_{p+1}, \ldots, r_n$ are randomly assigned value 0 or 1 and $r_p = s \oplus r_1 \oplus \ldots \oplus r_{p-1}$. By stacking any $t < p$ bits $r_{i_1}, \ldots, r_{i_t}$ to form $r_{i_1 \otimes \cdots \otimes i_t}$, the light transmissions are

$$T(r_{i_1 \otimes \cdots \otimes i_t}[s = 0]) = T(r_{i_1 \otimes \cdots \otimes i_t}[s = 1]) = \left(\frac{1}{2}\right)^t, \quad t < p$$

Proof: Two cases are considered: (i) $p \in \{i_1, \ldots, i_t\}$, (ii) $p \notin \{i_1, \ldots, i_t\}$.

(i) $p \in \{i_1, \ldots, i_t\}$. Since $t < p$ and $p \in \{i_1, \ldots, i_t\}$, a set $W = \{u, \ldots, v\}$ whose elements $u, \ldots, v \in \{1, \ldots, p\}$ and $u, \ldots, v \notin \{i_1, \ldots, i_t\}$ can be found. Let $r_{u \oplus \ldots \oplus v} = r_u \oplus \ldots \oplus r_v$, we obtain $r_p = s \oplus r_g \oplus \ldots \oplus r_h \oplus r_{u \oplus \ldots \oplus v}$ where $g, \ldots, h$ are the indices in $\{1, \ldots, p\}$ beside $u, \ldots, v$. When s, $r_g, \ldots, r_h$ are determined, r_p is decided by $r_{u \oplus \ldots \oplus v}$. By Lemma 2, we have $\text{Prob}(r_{u \oplus \ldots \oplus v} = 0) = \text{Prob}(r_{u \oplus \ldots \oplus v} = 1) = 1/2$. When $s \oplus r_g \oplus \ldots \oplus r_h = 0$, $r_p = r_{u \oplus \ldots \oplus v}$. We have $\text{Prob}(r_p = 0) = \text{Prob}(r_p = 1) = 1/2$. When $s \oplus_g \oplus \ldots \oplus r_h = 1$, $r_p = \overline{r_{u \oplus \cdots \oplus v}}$. We obtain $\text{Prob}(r_p = 0) = \text{Prob}(r_p = 1) = 1/2$. By Lemma 3, $\text{Prob}(s \oplus r_g \oplus \ldots \oplus r_h = 0) = \text{Prob}(s \oplus r_g \oplus \ldots \oplus r_h = 1) = 1/2$. As a result, $\text{Prob}(r_p = 0) = \text{Prob}(r_p = 1) = 1/2$ and r_p is independent of $s, r_g, \ldots, r_h$.

Light transmissions are obtained as

$$T(r_{i_1 \otimes \cdots \otimes i_t}[s = 0]) = T(r_{j \otimes \cdots \otimes k} \otimes r_p[s = 0]) = \left(\frac{1}{2}\right)^{t-1} \frac{1}{2} = \frac{1^t}{2}$$

and

$$T(r_{i_1 \otimes \cdots \otimes i_t}[s = 1]) = T(r_{j \otimes \cdots \otimes k} \otimes r_p[s = 1]) = \left(\frac{1}{2}\right)^{t-1} \frac{1}{2} = \left(\frac{1}{2}\right)^t$$

by Lemma 1.

(ii) $p \notin \{i_1, \ldots, i_t\}$. Since t bits are randomly generated, they are independent of the secret pixel s. Light transmissions of the stacked result of the t bits are $T(r_{i_1 \otimes \cdots \otimes i_t}[s=0]) = T(r_{i_1 \otimes \cdots \otimes i_t}[s=1]) = (1/2)^t$ by Lemma 1. □

Lemma 5: Given a secret pixel s and p bits $r_1, \ldots, r_p$, $p-1$ bits $r_1, \ldots, r_{p-1}$ are randomly assigned value 0 or 1 and $r_p = s \oplus r_1 \oplus \ldots \oplus r_{p-1}$. By stacking p bits $r_1, \ldots, r_p$ to form $r_{1 \otimes \ldots \otimes p}$, the light transmission is $T(r_{1 \otimes \ldots \otimes p}[s=0]) = (1/2)^{p-1}$ for the secret pixel is white. Whereas, the light transmission is $T(r_{1 \otimes \ldots \otimes p}[s=1]) = 0$ for the secret pixel is black.

Proof: When the secret pixel is white ($s=0$), $r_p = s \oplus r_1 \oplus \ldots \oplus r_{p-1} = r_1 \oplus \ldots \oplus r_{p-1}$. The stacked result of the p bits is white, if and only if, all the p bits are white. On the other hand, when the $p-1$ bits are all white, r_p is certainly white. The probability for the $p-1$ bits to be white is $\text{Prob}(r_1 = 0 \cup \ldots \cup r_{p-1} = 0) = (1/2)^{p-1}$. Hence, the light transmission is $T(r_{1 \otimes \ldots \otimes p}[s=0]) = (1/2)^{p-1}$.

When the secret pixel is black ($s=1$), $r_p = s \oplus r_1 \oplus \cdots \oplus r_{p-1} = \overline{r_1 \oplus \cdots \oplus r_{p-1}}$. The stacked result is white, if and only if, all the p bits are white. However, when the $p-1$ bits are white, r_p is black. The probability for the stack result to be white is zero. Therefore we obtain $T(r_{1 \otimes \ldots \otimes p}[s=1]) = 0$. □

Lemma 6: Given a secret pixel s and a minimal qualified set $Q = \{i_1, \ldots, i_p\}$ where $Q \subset \{1, \ldots, n\}$, $n-1$ bits $r_{i_1}, \ldots, r_{i_{p-1}}, r_g, \ldots, r_h$ are randomly assigned 0 or 1, where $g, \ldots, h$ are the $n-p$ indices in $\{1, \ldots, n\} - \{i_1, \ldots, i_p\}$ and $r_{i_p} = s \oplus r_{i_1} \oplus \cdots \oplus r_{i_{p-1}}$. By stacking t bits $r_{j_1}, \ldots, r_{j_t}$ to form $r_{j_1 \otimes \cdots \otimes j_t}$,

(i) for $Q \subseteq \{j_1, \ldots, j_t\}$, the light transmissions of the stacked result are

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = \left(\frac{1}{2}\right)^{t-1}$$

and

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = 0$$

(ii) For $Q \not\subseteq \{j_1, \ldots, j_t\}$, the light transmissions of the stacked result are

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = \left(\frac{1}{2}\right)^{t}$$

Proof: (i) $Q \subseteq \{j_1, \ldots, j_t\}$. $r_{j_1 \otimes \cdots \otimes j_t} = r_{g \otimes \cdots \otimes h} \otimes r_{i_1 \otimes \cdots \otimes i_p}$ where $g, \ldots, h$ are the $t-p$ indices in $\{j_1, \ldots, j_t\} - \{i_1, \ldots, i_p\}$. Since $r_g, \ldots, r_h$ are randomly generated, they are independent of the secret pixel. By Lemma 1, we have

$$T(r_{g \otimes \cdots \otimes h}[s=0]) = T(r_{g \otimes \cdots \otimes h}[s=1]) = \left(\frac{1}{2}\right)^{t-p}$$

By Lemma 5, we obtain $T(r_{i_1 \otimes \cdots \otimes i_p}[s=0]) = (1/2)^{p-1}$ and $T(r_{i_1 \otimes \cdots \otimes i_p}[s=1]) = 0$. As a result, we obtain

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = T(r_{g \otimes \cdots \otimes h}[s=0])\, T(r_{i_1 \otimes \cdots \otimes i_p}[s=0]) = \left(\frac{1}{2}\right)^{t-p}\left(\frac{1}{2}\right)^{p-1} = \left(\frac{1}{2}\right)^{t-1}$$

and

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = T(r_{g \otimes \cdots \otimes h}[s=1])T(r_{i_1 \otimes \cdots \otimes i_p}[s=1]) = \left(\frac{1}{2}\right)^{t-p} 0 = 0$$

(ii) $Q \not\subseteq \{j_1, \ldots, j_t\}$. For the t bits, $e < p$ bits are selected from $Q = \{i_1, \ldots, i_p\}$ and $f = t - e$ bits are selected from $\{1, \ldots, n\} - \{i_1, \ldots, i_p\}$. By Lemma 4, we obtain

$$T(r_{u \otimes \cdots \otimes v}[s=0]) = T(r_{u \otimes \cdots \otimes v}[s=1]) = \left(\frac{1}{2}\right)^{e}$$

where $u, \ldots, v$ are any e indices in Q. The f bits are randomly generated. By Lemma 1, we have

$$T(r_{g \otimes \cdots \otimes h}[s=0]) = T(r_{g \otimes \cdots \otimes h}[s=1]) = \left(\frac{1}{2}\right)^{f}$$

where $g, \ldots, h$ are any f indices in $\{1, \ldots, n\} - \{i_1, \ldots, i_p\}$. Hence, we obtain

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = T(r_{u \otimes \cdots \otimes v}[s=0])\, T(r_{g \otimes \cdots \otimes h}[s=0]) = \left(\frac{1}{2}\right)^{e}\left(\frac{1}{2}\right)^{f} = \left(\frac{1}{2}\right)^{t}$$

and

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = T(r_{u \otimes \cdots \otimes v}[s=1])\, T(r_{g \otimes \cdots \otimes h}[s=1]) = \left(\frac{1}{2}\right)^{e}\left(\frac{1}{2}\right)^{f} = \left(\frac{1}{2}\right)^{t}$$

□

Lemma 7: Given a secret pixel s and a strong access structure $\{\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}\}$, n bits $r_1, \ldots, r_n$ are generated by the proposed Algorithm 4. Denote Γ_0 is the basis of access structure. $k = |\Gamma_0|$ is the number of minimal qualified sets in Γ_0. Let $X \in 2^P$ be a set which contains t participants $\{j_1, \ldots, j_t\}$. Suppose that elements in X can form d ($0 \le d \le k$) minimal qualified sets. By stacking the t bits $r_{j_1}, \ldots, r_{j_t}$ to form $r_{j_1 \otimes \cdots \otimes j_t}$, the light transmissions of the stacked result are

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = \frac{d}{k}\left(\frac{1}{2}\right)^{t-1} + \left(1 - \frac{d}{k}\right)\left(\frac{1}{2}\right)^{t}$$

and

$$T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = \left(1 - \frac{d}{k}\right)\left(\frac{1}{2}\right)^{t}$$

Proof: Assume that Q is a minimal qualified set. If $Q \subseteq X$, light transmissions of the stacked result of the t bits are $T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = (1/2)^{t-1}$ and $T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = 0$ by Lemma 6. If $Q \not\subseteq X$, light transmissions of the stacked result of the t bits are $T(r_{j_1 \otimes \cdots \otimes j_t}[s=0]) = T(r_{j_1 \otimes \cdots \otimes j_t}[s=1]) = (1/2)^t$ by Lemma 6. The probability for the chosen minimal qualified set $Q \subseteq X$ is d/k and the probability for the chosen qualified set is $1 - d/k$.

doi: 10.1049/iet-ifs.2012.0046

Therefore the light transmissions of the stacked result are

$$T(r_{j_1\otimes\cdots\otimes j_t}[s=0]) = \frac{d}{k}\left(\frac{1}{2}\right)^{t-1} + \left(1-\frac{d}{k}\right)\left(\frac{1}{2}\right)^{t}$$

and

$$T(r_{j_1\otimes\cdots\otimes j_t}[s=1]) = \left(1-\frac{d}{k}\right)\left(\frac{1}{2}\right)^{t}$$

□

Theorem 1: Given a secret image $\boldsymbol{S}$ and a strong access structure $\{\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}\}$, n shares are generated by the proposed Algorithm 4. Algorithm 4 is a valid construction for a $\{\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}\}$ VSS scheme by RGs. It meets the following three conditions:

(i) For $1 \le i \le n$, R_i is a RG with $T(\boldsymbol{R}_i[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_i[\boldsymbol{S}(1)]) = 1/2$.
(ii) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\text{Qual}}$ (i.e. if X is a qualified set), by stacking the p shares to form $\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}$, the secret image is visually revealed. That is

$$T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])$$

(iii) If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\text{Forb}}$ (i.e. if X is a forbidden set), by stacking the p shares to form $\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}$, the stacked result gives no clue about the secret. That is

$$T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])$$

Proof: By Lemma 3, we have $T(r_i[s=0]) = T(r_i[s=1])$, $1 \le i \le n$. By Definition 1, we obtain $T(\boldsymbol{R}_i[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_i[\boldsymbol{S}(1)]) = 1/2$, $1 \le i \le n$. Each share generated by Algorithm 4 is an RG.

Denote Γ_0 is the basis of access structure. $k = |\Gamma_0|$ is the number of minimal qualified sets in Γ_0. Assume that elements in X can form d $(0 \le d \le k)$ minimal qualified sets. Light transmissions of the stacked result of the p bits are $T(r_{i_1\otimes\cdots\otimes i_p}[s=0]) = (d/k)(1/2)^{p-1} + (1-d/k)(1/2)^p$ and $T(r_{i_1\otimes\cdots\otimes i_p}[s=1]) = (1-d/k)(1/2)^p$ by Lemma 7. By Difinition 1, we have $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) = (d/k)(1/2)^{p-1} + (1-d/k)(1/2)^p$ and $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)]) = (1-d/k)(1/2)^p$.

If X is a qualified set, $d \ge 1$. We obtain $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)]) = (d/k)(1/2)^{p-1} > 0$. It is easy to know that $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])$.

If X is a forbidden set, $d = 0$. We obtain $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)]) = (d/k)(1/2)^{p-1} = 0$. Finally, we have $T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])$ □

In Theorem 1, the first condition guarantees that the n shares generated by Algorithm 4 are RGs. The second condition is also called contrast condition which makes sure that qualified sets can visually reveal the secret image. The third condition, which is referred to the security condition, ensures that forbidden sets cannot disclose any information of the secret image.

Theorem 2: Let Γ_0 be the basis of access structure. $k = |\Gamma_0|$ is the number of minimal qualified sets in Γ_0. $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\text{Qual}}$ is a qualified set whose elements can form d $(1 \le d \le k)$ minimal qualified sets, contrast of the stacked result of $\boldsymbol{R}_{i_1}, \ldots, \boldsymbol{R}_{i_p}$ is

$$\alpha = \frac{2d}{(2^p+1)k - d}$$

Proof: By Lemma 7, light transmissions of the stacked result of the p bits are

$$T(r_{i_1\otimes\cdots\otimes i_p}[s=0]) = \frac{d}{k}\left(\frac{1}{2}\right)^{p-1} + \left(1-\frac{d}{k}\right)\left(\frac{1}{2}\right)^{p}$$

and

$$T(r_{i_1\otimes\cdots\otimes i_p}[s=1]) = \left(1-\frac{d}{k}\right)\left(\frac{1}{2}\right)^{p}$$

Therefore

$$\frac{T(r_{i_1\otimes\cdots\otimes i_p}[s=0]) - T(r_{i_1\otimes\cdots\otimes i_p}[s=1])}{1 + T(r_{i_1\otimes\cdots\otimes i_p}[s=1])} = \frac{(d/k)(1/2)^{p-1}}{1 + (1-d/k)(1/2)^p} = \frac{2d}{(2^p+1)k - d}$$

By Definition 1, we have

$$\alpha = \frac{T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])}{1 + T(\boldsymbol{R}_{i_1\otimes\cdots\otimes i_p}[\boldsymbol{S}(1)])} = \frac{2d}{(2^p+1)k - d}$$

□

Theorem 3: The RG-based (p, n)-threshold VSS scheme presented in [21] is the special case of the proposed RG-based scheme with the contrast

$$\alpha = \frac{2\binom{t}{p}}{(2^p+1)\binom{n}{p} - \binom{t}{p}}$$

when t $(p \le t \le n)$ shares are stacked together.

Proof: For (p, n)-threshold VSS, every p shares form a minimal qualified set. The number of minimal qualified sets is $k = \binom{n}{p}$. The number of minimal qualified sets of the t shares is $d = \binom{t}{p}$. By Theorem 2, we have

$$\alpha = \frac{2\binom{t}{p}}{(2^p+1)\binom{n}{p} - \binom{t}{p}}$$

□

4 Experimental results and discussions

In this section, experiments of the proposed scheme are demonstrated in the illustrations. All the images used in this section are of size 1024 × 1024.

4.1 Two cases for binary images

Two experiments for encoding binary images with text are provided, demonstrating that the proposed scheme is feasible to be used in practical applications.

The first experiment by the proposed scheme for binary images is demonstrated in Fig. 7. Four participants $P = \{1, 2, 3, 4\}$ are involved in this example. The basis of the access structure is $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$. Set of qualified sets is $\Gamma_{\text{Qual}} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\}$ and set of forbidden sets is $\Gamma_{\text{Forb}} = 2^P - \Gamma_{\text{Qual}}$. The binary secret image and four RGs are illustrated in Figs. 7*a*–*e*. The four RGs are delivered to four associated participants. One participant only holds one RG, and will present the same RG for reconstructing the secret in different sets, which contain the current participant.

The reconstructed results of sets {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4} and {3, 4} are illustrated in Figs. 7*f*–*k*, respectively. Further, the superimposed results of sets {1, 2, 3}, {1, 2, 4}, {1, 3, 4} and {2, 3, 4} are shown in Figs. 7*l*–*o*. The stacked result of set {1, 2, 3, 4} is illustrated in Fig. 7*p*. Only qualified sets {1, 2, 3} (Fig. 7*l*), {1, 2, 4} (Fig. 7*m*) and {1, 2, 3, 4} (Fig. 7*p*) can visually reveal the secret image. Note that, for any one set which contains the *i*th participant, the same share R_i is presented by the *i*th participant for revealing the secret. For example, the shares in Figs. 7*b*–*e* are the same for the two different qualified sets {1, 2, 3} and {1, 2, 4}. Contrasts of the three reconstructed secret images are $\alpha_{\{1,2,3\}} = 2/17$, $\alpha_{\{1,2,4\}} = 2/17$ and $\alpha_{\{1,2,3,4\}} = 1/8$.

The second experiment for binary images is illustrated in Fig. 8. Fig. 8*a* shows the binary secret image. Basis of the access structure is $\Gamma_0 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$. Set of the qualified sets is $\Gamma_{\text{Qual}} = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$ and set of forbidden sets is $\Gamma_{\text{Forb}} = 2^P - \Gamma_{\text{Qual}}$. The four output RGs are shown in Figs. 8*b*–*e*, which are delivered to four associated participants. Similar to the first experiment, the same share R_i is presented by the *i*th participant for

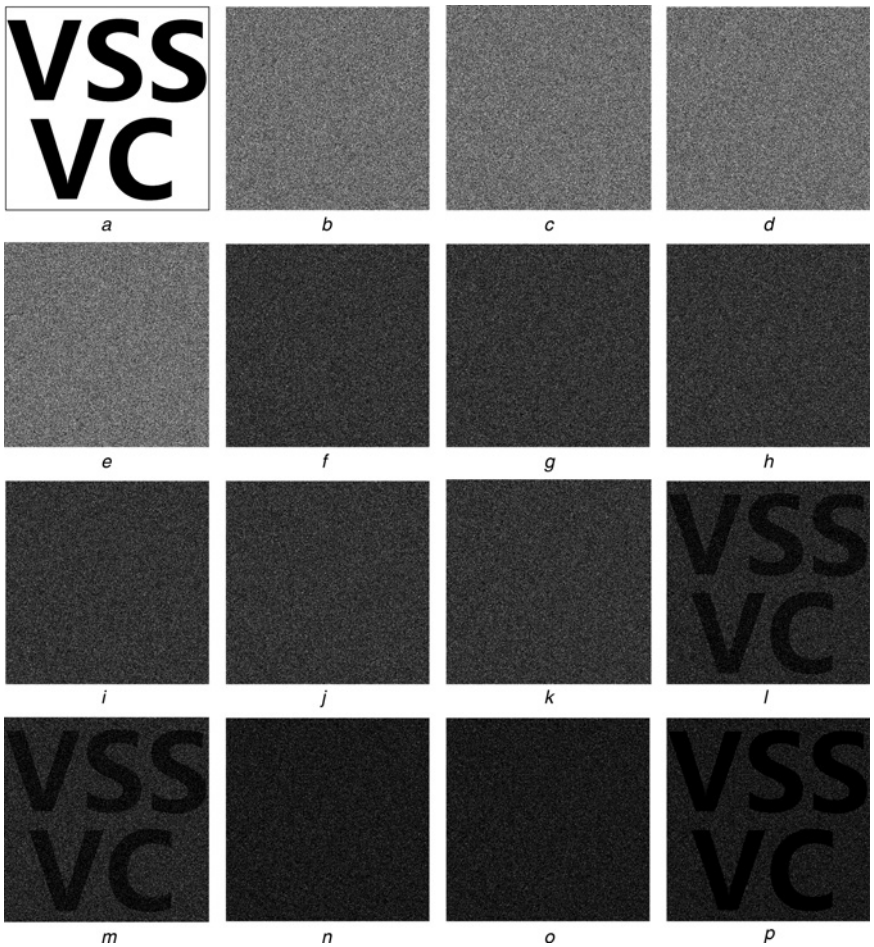

Fig. 7 *First experiment by the proposed scheme for binary images, $\Gamma_0 = \{\{1, 2, 3\}, \{1, 2, 4\}\}$*

a Secret image
b–*e* Four RGs, R_1, R_2, R_3 and R_4
f $R_1 \otimes R_2$
g $R_1 \otimes R_3$
h $R_1 \otimes R_4$
i $R_2 \otimes R_3$
j $R_2 \otimes R_4$
k $R_3 \otimes R_4$
l $R_1 \otimes R_2 \otimes R_3$, $\alpha_{\{1,2,3\}} = 2/17$
m $R_1 \otimes R_2 \otimes R_4$, $\alpha_{\{1,2,4\}} = 2/17$
n $R_1 \otimes R_3 \otimes R_4$
o $R_2 \otimes R_3 \otimes R_4$
p $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, $\alpha_{\{1,2,3,4\}} = 1/8$

IET Inf. Secur., 2012, Vol. 6, Iss. 4, pp. 299–309
doi: 10.1049/iet-ifs.2012.0046

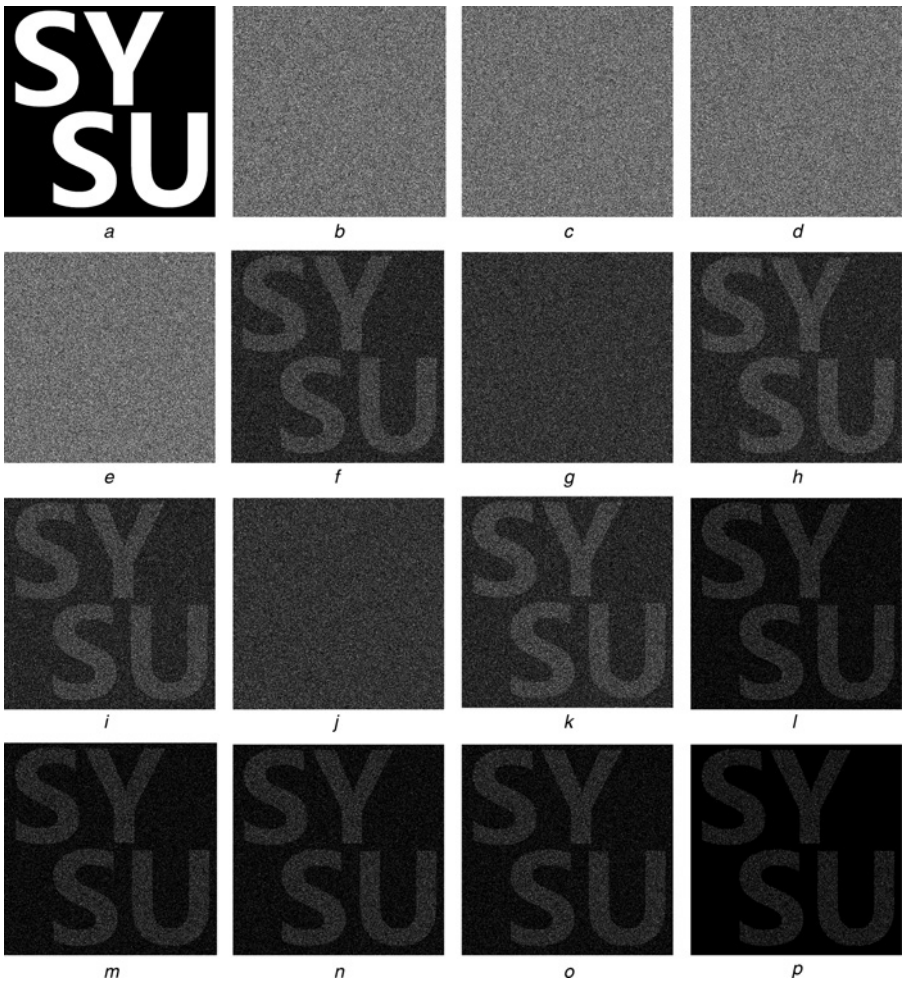

Fig. 8 *Second experiment by the proposed scheme for binary images,* $\Gamma_0 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}\}$

a Secret image
b–e Four RGs, R_1, R_2, R_3 and R_4
f $R_1 \otimes R_2$, $\alpha_{\{1,2\}} = 2/19$
g $R_1 \otimes R_3$
h $R_1 \otimes R_4$, $\alpha_{\{1,4\}} = 2/19$
i $R_2 \otimes R_3$, $\alpha_{\{2,3\}} = 2/19$
j $R_2 \otimes R_4$
k $R_3 \otimes R_4$, $\alpha_{\{3,4\}} = 2/19$
l $R_1 \otimes R_2 \otimes R_3$, $\alpha_{\{1,2,3\}} = 2/17$
m $R_1 \otimes R_2 \otimes R_4$, $\alpha_{\{1,2,4\}} = 2/17$
n $R_1 \otimes R_3 \otimes R_4$, $\alpha_{\{1,3,4\}} = 2/17$
o $R_2 \otimes R_3 \otimes R_4$, $\alpha_{\{2,3,4\}} = 2/17$
p $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, $\alpha_{\{1,2,3,4\}} = 1/8$

revealing the secret when the current set contains the *i*th participant. The stacked results of sets {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4} and {3, 4} are illustrated in Figs. 8*f–k*. The reconstructed results by sets {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4} are shown in Figs. 8*l–o*. The reconstructed result by set {1, 2, 3, 4} is illustrated in Fig. 8*p*. As demonstrated in Fig. 8, only the nine qualified sets can reconstruct the secret image visually, where the revealed secret images are illustrated in Fig. 8*f* (by set {1, 2}), Fig. 8*h* (by set {1, 4}), Fig. 8*i* (by set {2, 3}), Fig. 8*k* (by set {3, 4}), Fig. 8*l* (by set {1, 2, 3}), Fig. 8*m* (by set {1, 2, 4}), Fig. 8*n* (by set {1, 3, 4}), Fig. 8*o* (by set {2, 3, 4}) and Fig. 8*p* (by set {1, 2, 3, 4}). Contrasts of the nine stacked results by the nine qualified sets are $\alpha_{\{1,2\}} = \alpha_{\{1,4\}} = \alpha_{\{2,3\}} = \alpha_{\{3,4\}} = (2/19)$, $\alpha_{\{1,2,3\}} = \alpha_{\{1,2,4\}} = \alpha_{\{1,3,4\}} = \alpha_{\{2,3,4\}} = (2/17)$ and $\alpha_{\{1,2,3,4\}} = (1/8)$.

Table 1 Feature comparisons among the proposed scheme and other VSS methods

Schemes	Features			
	Pixel expansion	Code book needed	Shape distortion	Type of VSS
[3]	yes	yes	yes	(*k*, *n*)
[12]	no	yes	no	(*k*, *n*)
[13]	no	yes	no	(*k*, *n*)
[17]	no	no	no	(2, 2)
[18]	no	no	no	(2, 2)
[19]	no	no	no	(*n*, *n*)
[20]	no	no	no	(2, *n*),(*n*, *n*)
[21]	no	no	no	(*k*, *n*)
ours	no	no	no	access structure

Table 2 Comparisons of contrast among the proposed scheme and related non-expansible methods for different threshold cases

Schemes	Threshold cases			
	(2, 2)	(2, n)	(n, n)	(k, n)
[13]	(1/2)	$\geq[n/(5n-6)]$(even), $\geq[(n+1)/(5n-1)]$(odd), $(1/n)$	$[1/(2^{(n-1)})]$	–
[17]	(1/2, 1/5, 1/4)	–	–	–
[18]	(1/2, 1/5, 1/4)	–	–	–
[19]	(1/2, 1/5, 1/4)	–	$[1/(2^{(n-1)})$, $1/(2^n+1)$, $1/(2^n)]$	–
[20]	(1/2, 1/5, 1/4)	$[(2^{t-1}-1)/(2^t+1)]$	$[1/(2^{(n-1)})$, $1/(2^n+1)$, $(1/(2^n)]$	–
[21]	(1/2)	$\left(\left(2\binom{t}{2}\right)/\left((2^t+1)\binom{n}{2}-\binom{t}{2}\right)\right)$	$[1/(2^{(n-1)})]$	$\left(\left(2\binom{t}{k}\right)/\left((2^t+1)\binom{n}{k}-\binom{t}{k}\right)\right)$
ours	(1/2)	$\left(\left(2\binom{t}{2}\right)/\left((2^t+1)\binom{n}{2}-\binom{t}{2}\right)\right)$	$[1/(2^{(n-1)})]$	$\left(\left(2\binom{t}{k}\right)/\left((2^t+1)\binom{n}{k}-\binom{t}{k}\right)\right)$

4.2 Comparisons

Feature comparisons among the proposed scheme and related VSS schemes are demonstrated in Table 1. Merits of RG-based VSS, such as no pixel expansion, no code book required and no shape distortion, are preserved in the proposed scheme. Meanwhile, the proposed scheme is a generalisation of the RG-based threshold schemes [18–21]. These threshold schemes are the special cases of the proposed scheme. It is feasible for users to implement complicated sharing strategy via access structures.

Contrast of the revealed secret image serves as a measurement to evaluate the visual performance of the VSS scheme. It determines how well human eye can recognise the information in the reconstructed secret image. Usually, contrast is considered to be as large as possible. Herein, we compare the contrasts among the proposed scheme and related methods. Ito *et al.*'s method [12] encodes a black/white pixel by selecting one column in the black/white basis matrix. Contrast of their method is completely determined by the basis matrices. However, how to construct the basis matrices is not mentioned in their work. Different basis matrices would lead to different contrast. As a result, it is difficult to give a deterministic analysis on contrast of their work. In Yang's method [13], code book constructions for threshold cases such as (2, 2), (2, n), (n, n) and (k, n) are given. Nevertheless, the construction for (k, n) threshold is also based on the basis matrices used in conventional VSS. For the same reason, contrast of the (k, n)-threshold is hard to be determined as well. Therefore Ito *et al.*'s method [12] and the (k, n) case of Yang's method [13] are not included for contrast comparisons.

Table 2 shows the comparisons of contrast among the proposed scheme and related non-expansible methods for different threshold cases, where t is the number of stacked shares. From Theorem 3, when the access structures are reduced to threshold cases, contrast of the proposed scheme is reduced to Chen and Tsao's method [21]. Note that, there would be several contrasts for a threshold case in some schemes, since different share construction algorithms are proposed in these schemes. Especially in the (2, n)-threshold of Yang's method [13], there are two approaches to construct the shares. For the first approach, the contrast by stacking any two shares is $(n/(5n-6))$ when n is even, and it is $((n+1)/(5n-1))$ when n is odd. When n is fixed, the contrast increases when the number of stacked shares are increases according to their approach. For the second approach, the contrast is $1/n$. From Table 2, we know that optimal contrast is achieved by the proposed scheme in threshold cases such as (2, 2), (n, n) and (k, n). For the (2, n) case, contrast of the proposed scheme is slightly lower than the others.

5 Conclusions

This paper proposes RG-based VSS scheme for general access structures. Existing RG-based threshold schemes are special cases of the proposed schemes. Complicated sharing strategy can be implemented by the proposed method, which is fit for practical applications. Furthermore, advanced merits of RG-based VSS such as no pixel expansion, no code book required and no image distortion are maintained in the proposed method as well.

6 Acknowledgments

The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation. And they are especially grateful to Professor Carlo Blundo for his kind help during the review process of this paper. This work was supported by Science and Technology Development Fund of Macao Special Administrative Region under Contract no. 006/2001/A

7 References

1 Blakley, G.R.: 'Safeguarding cryptographic keys'. Proc. National Computer Conf., 1979, vol. 48, pp. 313–317
2 Shamir, A.: 'How to share a secret', *Commun. ACM*, 1979, **22**, (11), pp. 612–613
3 Naor, M., Shamir, A.: 'Visual cryptography', *Lect. Notes Comput. Sci.*, 1995, **950**, (1), pp. 1–12
4 Ateniese, G., Blundo, C., De Santis, A., Stinson, D.: 'Visual cryptography for general access structures', *Inf. Comput.*, 1996, **129**, (2), pp. 86–106
5 Ateniese, G., Blundo, C., Santis, A., Stinson, D.: 'Extended capabilities for visual cryptography', *Theor. Comput. Sci.*, 2001, **250**, (1–2), pp. 143–161
6 Blundo, C., De Santis, A., Stinson, D.: 'On the contrast in visual cryptography schemes', *J. Cryptol.*, 1999, **12**, (4), pp. 261–289
7 Hofmeister, T., Krause, M., Simon, H.: 'Contrast-optimal k out of n secret sharing schemes in visual cryptography', *Comput. Comb.*, 1997, **1276**, pp. 176–185
8 Verheul, E., Van Tilborg, H.: 'Constructions and properties of k out of n visual secret sharing schemes', *Des. Codes Cryptogr.*, 1997, **11**, (2), pp. 179–196
9 Blundo, C., De Santis, A., Naor, M.: 'Visual cryptography for grey level images', *Inf. Process. Lett.*, 2000, **75**, (6), pp. 255–259
10 Hou, Y.: 'Visual cryptography for color images', *Pattern Recognit.*, 2003, **36**, (7), pp. 1619–1629

doi: 10.1049/iet-ifs.2012.0046

11 Shyu, S.: 'Efficient visual secret sharing scheme for color images', *Pattern Recognit.*, 2006, **39**, (5), pp. 866–880
12 Ito, R., Kuwakado, H., Tanaka, H.: 'Image size invariant visual cryptography', *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, 1999, **82**, (10), pp. 2172–2177
13 Yang, C.: 'New visual secret sharing schemes using probabilistic method', *Pattern Recognit. Lett.*, 2004, **25**, (4), pp. 481–494
14 Cimato, S., De Prisco, R., De Santis, A.: 'Probabilistic visual cryptography schemes', *Comput. J.*, 2006, **49**, (1), pp. 97–107
15 Yang, C., Chen, T.: 'Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion', *Pattern Recognit. Lett.*, 2005, **26**, (2), pp. 193–206
16 Yang, C., Chen, T.: 'Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation', *Pattern Recognit.*, 2006, **39**, (7), pp. 1300–1314
17 Kafri, O., Keren, E.: 'Encryption of pictures and shapes by random grids', *Opt. Lett.*, 1987, **12**, (6), pp. 377–379
18 Shyu, S.: 'Image encryption by random grids', *Pattern Recognit.*, 2007, **40**, (3), pp. 1014–1031
19 Shyu, S.: 'Image encryption by multiple random grids', *Pattern Recognit.*, 2009, **42**, (7), pp. 1582–1596
20 Chen, T., Tsao, K.: 'Visual secret sharing by random grids revisited', *Pattern Recognit.*, 2009, **42**, (9), pp. 2203–2217
21 Chen, T., Tsao, K.: 'Threshold visual secret sharing by random grids', *J. Syst. Softw.*, 2011, **84**, pp. 1197–1208