Generalized Random Grid and Its Applications in Visual Cryptography

Xiaotian Wu and Wei Sun

***Abstract*—Random grid (RG) is a method to implement visual cryptography (VC) without pixel expansion. However, a reconstructed secret with lower visual quality reveals in RG-based VC due to the fact that average light transmission of a share is fixed at $1/2$. In this work, we introduce the concept of generalized RG, where the light transmission of a share becomes adjustable, and adopt generalized RG to implement different VC schemes. First, a basic algorithm, a $(2, 2)$ generalized RG-based VC, is devised. Based on the $(2, 2)$ scheme, two VC schemes including a $(2, n)$ generalized RG-based VC and a (n, n) XOR-based meaningful VC are constructed. The two derived algorithms are designed to solve different problems in VC. In the $(2, n)$ scheme, recovered image quality is further improved. In the (n, n) method, meaningful shares are constructed so that the management of shadows becomes more efficient, and the chance of suspicion on secret image encryption is reduced. Moreover, superior visual quality of both the shares and recovered secret image is achieved. Theoretical analysis and experimental results are provided as well, demonstrating the effectiveness and advantages of the proposed algorithms.**

***Index Terms*—Visual cryptography, visual secret sharing, random grid, visual quality, meaningful share, XOR.**

I. Introduction

VISUAL cryptography (VC) is a paradigm of cryptography which prevents a secret from being modified or destructed by using the notions of perfect cipher and human visual system. For a general scheme of (k, n) threshold, a secret image is encrypted into n random-looking images which are called shares or shadows. These n shares are then distributed to n associated participants. To visually reveal the secret, any k or more shares are required to stack together. But any k or less shadows give no clue about the secret. Compared with some conventional encryptions such as DES and AES, VC offers unbreakable encryption if a meaningless share contains truly random pixels such that it can be seen as a one-time pad system. Without using a computational device and cryptographic knowledge in decryption, VC technique is effective and suitable for certain practical applications.

Manuscript received April 23, 2013; revised July 12, 2013; accepted July 12, 2013. Date of publication July 26, 2013; date of current version August 19, 2013. This work was supported by the 973 Program (2011CB302400). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Carlo Blundo. *(Corresponding author: W. Sun.)*

W. Sun is with the School of Software, Sun Yat-sen University, Guangzhou 510006, China (e-mail: sunwei@mail.sysu.edu.cn).

X. Wu is with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China (e-mail: wxt.sysu@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2013.2274955

An initial model of VC was proposed by Naor and Shamir [1], where the (k, n) scheme is investigated. Inspired by Naor and Shamir's work, various studies on VC [2] were conducted. Constructing VC scheme for general access structure was investigated in [3], where general access structure is used to implement complicated sharing strategy. Encoding secret images with different formats, such as gray-scale/color images, was studied in [4], [5], [6], [7]. To manage the shadows efficiently and to reduce the chance of suspicion on secret image communication simultaneously, extended VC [8], [9] and halftone VC [10], [11] were proposed, where shadows with meaningful contents are constructed. For the aim of improving the reconstructed secret image quality, methods for obtaining optimal contrast [12], [13] were introduced. However, some deficiencies still remain in the above-mentioned VC, as described as follows.

- Pixel expansion. The generated shadow is $m \geq 2$ times as big as the original secret image, where m is referred to pixel expansion. Pixel expansion further burdens the data transmission and storage.
- Tailor-made codebook required. A codebook is needed to encrypt the secret. But designing codebooks for different thresholds is not trivial.

To generate size invariant shadows, probabilistic VC and random grid-based (RG-based) VC are adopted. For probabilistic VC, Ito *et al.* [14] presented an approach to encode a black/white pixel by using a column selected from the corresponding black/white basis matrix with equal probabilities. Yang [15] proposed constructions of probabilistic VC for different thresholds. A secret pixel is correctly reconstructed with certain probability. Cimato *et al.* [16] further extended the probabilistic VC model to form a generalization, where the generalization is a mixed model of both the classical deterministic model and the probabilistic model. When the pixel expansion $m = 1$, their model reduces to one of Yang's constructions. For big enough values of m, their model reduces to the classical deterministic model if such a deterministic scheme exists.

The concept of RG was initially introduced by Kafri and Keren [17] to encrypt a secret image into two noise-like images, where each image is referred as a RG. The size of a RG is the same as that of the secret image. Moreover, three distinct encryption algorithms were also presented. Inspired by Kafri and Keren, enhanced algorithms for encrypting gray-scale and color images were proposed by Shyu [18], as well as the (n, n) scheme [19]. Follow-up investigations on RG-based VC were discussed for constituting the $(2, n)$[20], (k, n)[21] and access structure [22], [23] schemes. Further, other studies such as improving the visual quality of RG-based VC [24], [25] , constructing RG-based VC with abilities of both OR and XOR de-

cryptions [26] and user-friendly RG-based VC [27] were presented as well.

Conventionally, the average light transmission of a share in RG-based VC is fixed at $1/2$. When more shares are stacked, reconstructed secret with lower visual quality reveals due to the fact that the recovered image becomes darker. On the other hand, XOR-based VC [28], [29] [30], [31] is a significant branch of VC that can reconstruct the secret without darkening the background when more shares are utilized. XOR-based VC system has good color, contrast and resolution properties since the secret decryption can be done with a small, cheap and lightweight decryption display. Moreover, handheld devices, such as cell phone and personal digital assistant (PDA), are popularly utilized in practical applications. XOR-based VC becomes more feasible since the decryption has low computation complexity and can be done by such handheld devices. XOR-based VC is an effective methodology that can increase the reconstructed image quality at the expense of sacrificing the accessibility. However, random-looking shares still used in the above-mentioned XOR-based VC schemes. These noise-like shares are hard to identify and increase the chance of suspicion on secret image encryption.

In this paper, the concept of generalized RG is first introduced and adopted to design a $(2, 2)$ VC scheme. Additionally, the average light transmission of a share becomes adjustable. Based on the $(2, 2)$ method, two VC algorithms including the $(2, n)$ generalized RG-based VC and (n, n) XOR-based meaningful VC are derived. Theoretical analysis and simulation results are provided to demonstrate the effectiveness and advantages of the proposed algorithms.

The remaining part of this paper is organized as follows. The concept of generalized RG is given in Section II. The model of $(2, 2)$ generalized RG-based VC is introduced in Section III. Section IV proposes two derived VC algorithms, which are designed for different application scenarios. Experimental results and discussions are illustrated in Section V. Section VI gives some concluding remarks.

II. Generalized Random Grid

In general, a RG is defined as a transparency comprising a two-dimensional array of pixels [17], where each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. Half of the pixels in a RG are white, and the remaining pixels are black. Prior to formulating our algorithms, some definitions on RG are given, which are partially borrowed from [18], [20], [24], [25]. In addition, notations used in this work are demonstrated in Table I.

Definition 1 (Average Light Transmission) [18]: For a certain pixel r in a binary image $\mathbf{R}$ whose size is $M \times N$, the light transmission of a white pixel is defined as $T(\mathrm{r}) = 1$. Whereas, $T(\mathrm{r}) = 0$ for r is a black pixel. Totally, the average light transmission of $\mathbf{R}$ is defined as

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

Definition 2 (Area Representation) [18]: Let $\mathbf{S}(0)$ (resp. $\mathbf{S}(1)$) be the area of all the white (resp. black) pixels in secret image $\mathbf{S}$ where $\mathbf{S} = \mathbf{S}(0) \cup \mathbf{S}(1)$ and $\mathbf{S}(0) \cap \mathbf{S}(1) = \emptyset$. Therefore, $\mathbf{R}[\mathbf{S}(0)]$ (resp. $\mathbf{R}[\mathbf{S}(1)]$) is the corresponding area of all the white (resp. black) pixels in image $\mathbf{R}$.

TABLE I
Notations Used in This Work

Notation	Decryption
0	A white pixel.
1	A black pixel.
$R_1, \cdots, R_n$	Shares generated by VC schemes.
S	The secret image.
$\otimes$	Stacking (OR) operation.
$R_{\{\otimes,i_1,\cdots,i_t\}}$	Stacked result by shares $R_{i_1}, \cdots, R_{i_t}$.
$\oplus$	XOR operation.
$R_{\{\oplus,i_1,\cdots,i_t\}}$	XOR-ed result by shares $R_{i_1}, \cdots, R_{i_t}$.
α	Contrast of the recovered image.
$\sigma_{4,4}, \sigma_{4,3}, \sigma_{4,2}, \sigma_{4,1}, \sigma_{4,0}$	Variances of the recovered image.

Definition 3 (Contrast) [18], [21]: The contrast of the reconstructed secret image $\mathbf{R}_{\{\otimes,1,\ldots,n\}} = \mathbf{R}_1 \otimes \cdots \otimes \mathbf{R}_n$ with respect to the original secret image $\mathbf{S}$ is

$$\alpha = \frac{T(\mathbf{R}_{\{\otimes,1,\ldots,n\}}[\mathbf{S}(0)]) - T(\mathbf{R}_{\{\otimes,1,\ldots,n\}}[\mathbf{S}(1)])}{1 + T(\mathbf{R}_{\{\otimes,1,\ldots,n\}}[\mathbf{S}(1)])} \tag{2}$$

where symbol $\otimes$ denotes the Boolean OR operation.

The visual quality of revealed secret image is evaluated by contrast. It is expected to be as large as possible so that better visual quality can be obtained. Further, variance is adopted to evaluate the visual quality of the reconstructed secret image as well [24], [25] . When the contrast is fixed, the variance is expected to be as small as possible. Small variance indicates that a more even reconstructed secret image is achieved. The definition of variance is given in Definition 4.

Definition 4 (Variance) [24], [25]: Suppose $B_{t,b}$ is a type of block in the secret image, where it contains t pixels and has b black pixels. The secret image is separated into nonoverlapping blocks, where each block contains t pixels. Let M be the number of blocks in the secret image which belong to $B_{t,b}$. The M secret blocks are encrypted by RG-based VC, and M blocks in the same locations of the recovered image are obtained. Denote the corresponding M blocks in the recovered image as RS_1, ..., RS_M. Variance $\sigma_{t,b}$ of the darkness levels of $B_{t,b}$ is calculated by

$$\sigma_{t,b} = \frac{\sum_{i=1}^{M}[\mu_{t,b} - H(RS_i)]^2}{M} \tag{3}$$

where function H calculates the darkness levels (the number of black pixels) of block RS_i, and $\mu_{t,b}$ is the average darkness levels of the M blocks, as computed by

$$\mu_{t,b} = \frac{\sum_{i=1}^{M} H(RS_i)}{M}. \tag{4}$$

In this paper, t is set to be 4, and the size of the block is set to be 2×2. These are the same as those in [24], [25] . In total, five variances $\sigma_{4,4} \ldots \sigma_{4,0}$ are employed for evaluating the evenness of the recovered secret image. Contrast and variance are measurements for the reconstructed image quality. But contrast serves as the primary measurement, and variance acts as the secondary measurement. Contrast is more significant than variance. Reconstructed secret images with different contrasts and different variances are illustrated in Fig. 1, where Fig. 1(a) is

(a) (b) (c)

Fig. 1. Reconstructed secret images with different contrasts and different variances. (a) $\alpha = 0.2514, \sigma_{4,4} = 0, \sigma_{4,3} = 0.1928, \sigma_{4,2} = 0.3963, \sigma_{4,1} = 0.5590, \sigma_{4,0} = 0.7549$. (b) $\alpha = 0.5012, \sigma_{4,4} = 0, \sigma_{4,3} = 0.2500, \sigma_{4,2} = 0.4962, \sigma_{4,1} = 0.7272, \sigma_{4,0} = 0.9950$. (c) $\alpha = 0.5012, \sigma_{4,4} = 0, \sigma_{4,3} = 0.2498, \sigma_{4,2} = 0.3737, \sigma_{4,1} = 0.4669, \sigma_{4,0} = 0.7124$.

with smaller contrast and Figs. 1(b) and 1(c) are with larger contrasts. Competitive image quality is obtained in Fig. 1(c) since larger contrast and smaller variances are obtained. Note that, variances can be utilized to measure the image quality objectively only when approximate or the same contrasts are achieved (like Figs. 1(b) and 1(c)).

In reported RG-based VC, the number of white pixels in a share is approximately half of the total number. Herein, we introduce the concept of generalized RG, where the probability for a pixel in a share to be white becomes adjustable. A generalized RG is constructed by a random bit generator whose definition is given in Definition 5.

Definition 5 (Random bit Generator): A random bit generator $b = g(x)$ is defined as a bit which is assigned the value 0 (resp. 1) with probability x (resp. $1 - x$), as given by

$$g(x) : Prob(b = 0) = x,\ Prob(b = 1) = 1 - x,$$

where procedure $Prob(A)$ represents the probability when event A is true and $0 < x < 1$.

III. The Basic Algorithm

Based on the random bit generator, a basic VC algorithm, namely a $(2, 2)$ generalized RG-based VC, is constructed, as formulated in Algorithm 1.

Algorithm 1 Generalized RG-Based VC for $(2, 2)$ case.

Input: a binary secret image $\boldsymbol{S}$ with $M \times N$ pixels, and three parameters u, v and d.
Output: two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.
Step 1: For each position (i, j) in the secret image, Steps $2 - 3$ are performed to generate two shared pixels $\boldsymbol{R}_1(i, j)$ and $\boldsymbol{R}_2(i, j)$.
Step 2: Construct a shared pixel $\boldsymbol{R}_1(i, j)$ by

$$\boldsymbol{R}_1(i, j) = g(\frac{u}{v}). \tag{5}$$

Step 3: Construct the other shared pixel $\boldsymbol{R}_2(i, j)$ by

$$\boldsymbol{R}_2(i,j) = \begin{cases} \boldsymbol{R}_1(i,j), & \text{if } \boldsymbol{S}(i,j) = 0, \\ g(\frac{u}{v-d}), & \text{if } \boldsymbol{S}(i,j) = 1 \text{ and } \boldsymbol{R}_1(i,j) = 1, \\ g(\frac{u-d}{v-d}), & \text{if } \boldsymbol{S}(i,j) = 1 \text{ and } \boldsymbol{R}_1(i,j) = 0, \end{cases} . \tag{6}$$

Step 4: Output the two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$.

The three parameters u, v and d used in the $(2, 2)$ scheme must satisfy the following conditions:

$$\begin{cases} d \geq 0, u > 0, v > 0, \\ v > u \geq d, \\ v \geq u + d. \end{cases} . \tag{7}$$

A. Theoretical Analysis

In this subsection, we firstly prove that the $(2, 2)$ algorithm is a valid construction of VC by Theorem 1 when stacking decryption is applied. Usually, a valid construction means that the proposed method satisfies two conditions: security condition and contrast condition. Security condition indicates that insufficient shares give no clue about secret, and contrast condition implies that sufficient shares reveal the secret. Moreover, the contrast of the revealed secret image by stacking decryption is given in Theorem 2. Theoretical analysis is given as follows.

Lemma 1: Given two shares $\mathbf{R}_1$ and $\mathbf{R}_2$ generated from Algorithm 1, every share is a generalized RG, and gives no clue about the secret: $T(\mathbf{R}_k[\mathbf{S}(0)]) = T(\mathbf{R}_k[\mathbf{S}(1)]) = u/v$ where $k = 1, 2$.

Proof: Based on (5), we get $Prob(\mathbf{R}_1(i, j) = 0) = u/v$ no matter the secret pixel is white or black. By Definition 1, we have $T(\mathbf{R}_1[S(0)]) = T(\mathbf{R}_1[S(1)]) = u/v$. According to (6), when $\mathbf{S}(i, j) = 0$, $Prob(\mathbf{R}_2(i, j) = 0) = Prob(\mathbf{R}_1(i, j) = 0) = u/v$. When $\mathbf{S}(i, j) = 1$, $Prob(\mathbf{R}_2(i, j) = 0) = Prob(\mathbf{R}_2(i, j) = 0 \wedge \mathbf{R}_1(i, j) = 0) + Prob(\mathbf{R}_2(i, j) = 0 \wedge \mathbf{R}_1(i, j) = 1) = (u - d)/(v - d) \times u/v + u/(v - d) \times (1 - u/v) = u/v$. Hence, $Prob(\mathbf{R}_2(i, j) = 0) = u/v$ is obtained no matter the secret pixel is white or black. By Definition 1, $T(\mathbf{R}_2[\mathbf{S}(0)]) = T(\mathbf{R}_2[\mathbf{S}(1)]) = u/v$ is achieved. Every share cannot disclose any information about the secret. ■

Lemma 2: Given two shares $\mathbf{R}_1$ and $\mathbf{R}_2$ generated from Algorithm 1, the stacked result by the two shares $\mathbf{R}_{\{\otimes,1,2\}} = \mathbf{R}_1 \otimes \mathbf{R}_2$ visually reveals the secret: $T(\mathbf{R}_{\{\otimes,1,2\}}[\mathbf{S}(0)]) > T(\mathbf{R}_{\{\otimes,1,2\}}[\mathbf{S}(1)])$.

Proof: When $\boldsymbol{S}(i, j) = 0$, $\boldsymbol{R}_2(i, j) = \boldsymbol{R}_1(i, j)$. If $\boldsymbol{R}_1(i, j) = 0$, $\boldsymbol{R}_2(i, j) = 0$. The stacked result is white if and only if the two shared pixels are white. Thus, we have $Prob(\boldsymbol{R}_{\{\otimes,1,2\}}(i, j) = 0) = Prob(\boldsymbol{R}_1(i, j) = 0 \wedge \boldsymbol{R}_2(i, j) = 0) = u/v$. By Definition 1, we obtain $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) = u/v$.

When $\boldsymbol{S}(i, j) = 1$, $Prob(\boldsymbol{R}_{\{\otimes,1,2\}}(i, j) = 0) = Prob(\boldsymbol{R}_1(i, j) = 0 \wedge \boldsymbol{R}_2(i, j) = 0) = u/v \times (u - d)/(v - d)$ according to (6). By Definition 1, we obtain $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)]) = u/v \times (u - d)/(v - d)$.

Therefore, $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)]) = u/v - u/v \times (u - d)/(v - d) = u/v \times (v - u)/(v - d)$. Since $v > u \geq d$, we get $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)]) > 0$. As a result, $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)])$. The stacked result reveals the secret. ■

Theorem 1: Algorithm 1 is a valid construction of the generalized RG-based VC for $(2, 2)$ case. It meets the following conditions:

- Every share is a generalized RG and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u/v$ where $k = 1, 2$.

- The stacked result by the two shares $\boldsymbol{R}_{\{\otimes,1,2\}} = \boldsymbol{R}_1 \otimes \boldsymbol{R}_2$ reveals the secret: $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)])$.

Proof: According to Lemmas 1 and 2, the two conditions are satisfied. Algorithm 1 is a valid construction of $(2,2)$ generalized RG-based VC. ■

Theorem 2: Contrast of the reconstructed secret image by stacking the two shares generated from Algorithm 1 is

$$\alpha = \frac{u}{v+u-d}. \tag{8}$$

Proof: Obtained from the proof of Lemma 2, we have $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) = u/v$ and $T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)]) = u/v \times (u-d)/(v-d)$. According to Definition 3, the contrast of the reconstructed secret image is calculated by

$$\begin{aligned}\alpha &= \frac{T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(0)]) - T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)])}{1+T(\boldsymbol{R}_{\{\otimes,1,2\}}[\boldsymbol{S}(1)])} \\ &= \frac{\left[\frac{u}{v} - \frac{u}{v}\times\frac{u-d}{v-d}\right]}{\left[1+\frac{u}{v}\times\frac{u-d}{v-d}\right]} \\ &= \frac{u}{v+u-d}.\end{aligned} \tag{9}$$

■

When the average light transmission of a shadow is fixed (u, v are determined), parameter d is expected to be as large as possible so that larger contrast is achieved. The following two cases are considered: (1) $u \le v/2$ and (2) $u > v/2$. When $u \le v/2$, the largest value of d is $d = u$. When $u > v/2$, the largest value of d is $d = v - u$. We further prove that the $(2,2)$ algorithm is a valid construction of XOR-based VC by Theorem 3. In this paper, symbol $\oplus$ denotes the Boolean XOR operation. The analysis is given below.

Lemma 3: Given two shares $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$ generated from Algorithm 1, the XOR-ed result by the two shares $\boldsymbol{R}_{\{\oplus,1,2\}} = \boldsymbol{R}_1 \oplus \boldsymbol{R}_2$ visually reveals the secret: $T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(1)])$.

Proof: When $\boldsymbol{S}(i,j) = 0$, $\boldsymbol{R}_2(i,j) = \boldsymbol{R}_1(i,j)$. When $\boldsymbol{R}_1(i,j) = 0, \boldsymbol{R}_2(i,j) = 0$ or $\boldsymbol{R}_1(i,j) = 1, \boldsymbol{R}_2(i,j) = 1$, the XOR-ed result is 0. The probability for $\boldsymbol{R}_1(i,j) = 0$ and $\boldsymbol{R}_2(i,j) = 0$ is u/v. And the probability for $\boldsymbol{R}_1(i,j) = 1$ and $\boldsymbol{R}_2(i,j) = 1$ is $(1-u/v)$. Thus, we have $Prob(\boldsymbol{R}_{\{\oplus,1,2\}}(i,j) = 0) = u/v + 1 - u/v = 1$. By Definition 1, we obtain $T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(0)]) = 1$.

When $\boldsymbol{S}(i,j) = 1$, the probability for $\boldsymbol{R}_1(i,j) = 0$ and $\boldsymbol{R}_2(i,j) = 0$ is $u/v \times (u-d)/(v-d)$. And the probability for $\boldsymbol{R}_1(i,j) = 1$ and $\boldsymbol{R}_2(i,j) = 1$ is $(1-u/v) \times [1-u/(v-d)]$. Thus, we have $Prob(\boldsymbol{R}_{\{\oplus,1,2\}}(i,j) = 0) = (u/v)[(u-d)/(v-d)] + (1-u/v)[1-u/(v-d)]$. By Definition 1, we obtain $T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(0)]) = (u/v)[(u-d)/(v-d)] + (1-u/v)[1-u/(v-d)]$.

Since $d \le u < v$, $u - d < v - d$ is obtained. We have $0 \le (u-d)/(v-d) < 1$. Further, since $v \ge u + d$, we get $v - d \ge u$. And $0 < u/(v-d) < 1$ is achieved. As a result, we obtain $(u/v)[(u-d)/(v-d)] + (1-u/v)[1-u/(v-d)] < (u/v) + (1-u/v) = 1$. Finally, $T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(1)])$ is achieved. The XOR-ed result reveals the secret. ■

Theorem 3: Algorithm 1 is a valid construction of XOR-based VC for $(2,2)$ case. It satisfies the following conditions:

- Every share gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u/v$ where $k = 1, 2$.
- The XOR-ed result by the two shares $\boldsymbol{R}_{\{\oplus,1,2\}} = \boldsymbol{R}_1 \oplus \boldsymbol{R}_2$ reveals the secret: $T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus,1,2\}}[\boldsymbol{S}(1)])$.

Proof: According to Lemmas 1 and 3, the two conditions are met. Algorithm 1 is a valid construction of XOR-based VC for $(2,2)$ case. ■

The above-mentioned analysis is further utilized to substantiate the analysis on the derived algorithms described in Section IV.

IV. Two Derived Algorithms

Based on the $(2,2)$ algorithm, two derived VC schemes, including a $(2,n)$ generalized RG-based VC and a XOR-based meaningful VC, are constructed. The two VC algorithms are designed for different application scenarios and solve different problems in VC. The $(2,n)$ algorithm aims to improve the recovered image quality by manipulating the average light transmission of a share. The XOR-based meaningful VC solves the share management problem by offering meaningful shares. In addition, the meaningful shares decrease the chance of suspicion on secret image encryption. Moreover, superior image quality is provided by the XOR-based meaningful VC as well.

A. $(2,n)$ Generalized RG-Based VC

In reported RG-based VC, the visual quality of the recovered secret image is not satisfactory due to the fact that the average light transmission of a shadow is equal or less than $1/2$. Even worse, when more shares are stacked, the background of reconstructed secret image becomes darker, and leads to terrible visual quality.

To improve the visual quality, we devise that the average light transmission of a share can be manipulated. For different $(2,n)$ thresholds, different average light transmissions are utilized, and those light transmissions which lead to pleasing visual quality can be chosen to construct the $(2,n)$ generalized RG-based VC. Formulation on the proposed $(2,n)$ scheme is given in Algorithm 2.

Algorithm 2 Generalized RG-based VC for $(2,n)$ case.

Input: a binary secret image S with $M \times N$ pixels, and two parameters u and v.
Output: n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.
Step 1: For each position (i,j) in the secret image, Steps 2–4 are performed to construct n shared pixels $\boldsymbol{R}_1(i,j), \ldots, \boldsymbol{R}_n(i,j)$.
Step 2: Generate a shared pixel $\boldsymbol{R}_1(i,j)$ by

$$\boldsymbol{R}_1(i,j) = g(\frac{u}{v}). \tag{10}$$

Step 3: When $\boldsymbol{S}(i,j)=0$, the remaining $n-1$ shared pixels are constructed by

$$\begin{cases} \boldsymbol{R}_2(i,j)=\boldsymbol{R}_1(i,j), \\ \vdots \\ \boldsymbol{R}_n(i,j)=\boldsymbol{R}_1(i,j). \end{cases} \quad (11)$$

Step 4: When $\boldsymbol{S}(i,j)=1$, the $n-1$ shared pixels $\boldsymbol{R}_k(i,j)(2\le k\le n)$ are constructed by

$$\boldsymbol{R}_k(i,j)=g(\frac{u}{v}). \quad (12)$$

Step 5: Output the n shares $\boldsymbol{R}_1,\ldots,\boldsymbol{R}_n$.

By superimposing any two or more shares together, the secret can be visually revealed. Further, theoretical analysis on the $(2,n)$ scheme is given as follows. The analysis is utilized to prove Theorems 4 and 5, where Theorem 4 describes that the $(2,n)$ scheme is a valid construction of VC when stacking decryption is applied and Theorem 5 gives the contrast of the $(2,n)$ scheme.

Lemma 4: Given n shares $\boldsymbol{R}_1,\ldots,\boldsymbol{R}_n$ generated from Algorithm 2, every share is a generalized RG and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)])=T(\boldsymbol{R}_k[\boldsymbol{S}(1)])=u/v$ where $k=1,\ldots,n$.

Proof: According to (10), the shared pixel $\boldsymbol{R}_1(i,j)$ is independent of the secret pixel. No matter the secret pixel is white or black, $Prob(\boldsymbol{R}_1(i,j)=0)=u/v$ is obtained. As a result, $T(\boldsymbol{R}_1[\boldsymbol{S}(0)])=T(\boldsymbol{R}_1[\boldsymbol{S}(1)])=u/v$ is achieved by Definition 1.

Based on (11), the average light transmission of the second shared pixel is $Prob(\boldsymbol{R}_2(i,j)=0)=Prob(\boldsymbol{R}_1(i,j)=0)=u/v$ when the secret pixel is white, i.e., $\boldsymbol{S}(i,j)=0$. On the other hand, when the secret pixel is black, i.e., $\boldsymbol{S}(i,j)=1$, the average light transmission of the second shared pixel $\boldsymbol{R}_2(i,j)$ is u/v according to (12). Hence, the average light transmission of the second shared pixel $\boldsymbol{R}_2(i,j)$ is u/v no matter the secret pixel is black or white. Further, the same conclusion still holds for shared pixels $\boldsymbol{R}_3(i,j),\ldots,\boldsymbol{R}_n(i,j)$.

Therefore, $T(\boldsymbol{R}_k[\boldsymbol{S}(0)])=T(\boldsymbol{R}_k[\boldsymbol{S}(1)])=u/v$ for $2\le k\le n$ is achieved by Definition 1. Finally, Lemma 4 is proved to be met. ■

Lemma 5: Given n shares $\boldsymbol{R}_1,\ldots,\boldsymbol{R}_n$ constructed from Algorithm 2, the stacked result by any $t\ge 2$ shares $\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}=\boldsymbol{R}_{x_1}\otimes\cdots\otimes\boldsymbol{R}_{x_t}$ visually reveals the secret: $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(0)])>T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(1)])$.

Proof: When the secret pixel is white, i.e., $\boldsymbol{S}(i,j)=0$, the n shared pixels are

$$\boldsymbol{R}_n(i,j)=\cdots=\boldsymbol{R}_2(i,j)=\boldsymbol{R}_1(i,j). \quad (13)$$

And $\boldsymbol{R}_1(i,j)$ is constructed by $\boldsymbol{R}_1(i,j)=g(u/v)$ according to (10). The stacked result by the t shared pixels is white if and only if the t shared pixels are white. The probability for the t shared pixels to be white is u/v. Hence, the average light transmission of the stacked result by any t shared pixels are u/v. By Definition 1, we have $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(0)])=u/v$.

When the secret pixel is black, i.e., $\boldsymbol{S}(i,j)=1$, the n shared pixels are constructed by (10) and (12). The n shared pixels are independent of each other. The stacked result by the t shared pixels is white if and only if the t shared pixels are white. The probability for the t shared pixels to be white is $(u/v)^t$. Therefore, the average light transmission of the stacked result by any t shared pixels are $(u/v)^t$. Based on Definition 1, we achieve $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(1)])=(u/v)^t$.

Since $0<u/v<1$ and $t\ge 2$, we get $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(0)])>T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(1)])$. Lemma 5 is proved to be satisfied. ■

Theorem 4: Algorithm 2 is a valid construction of the generalized RG-based VC for $(2,n)$ case. The following conditions are satisfied:

- Every share is a generalized RG and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)])=T(\boldsymbol{R}_k[\boldsymbol{S}(1)])=u/v$ where $k=1,\ldots,n$.
- The stacked result by any $t\ge 2$ shares $\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}=\boldsymbol{R}_{x_1}\otimes\cdots\otimes\boldsymbol{R}_{x_t}$ reveals the secret: $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(0)])>T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(1)])$.

Proof: The two conditions are met based on Lemmas 4 and 5. Algorithm 2 is a valid construction of $(2,n)$ generalized RG-based VC. ■

Theorem 5: Contrast of the reconstructed secret image by stacking any t shares constructed by Algorithm 2 is

$$\alpha=\frac{\frac{u}{v}-(\frac{u}{v})^t}{1+(\frac{u}{v})^t}. \quad (14)$$

Proof: From the proof of Lemma 5, we obtain $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(0)])=u/v$ and $T(\boldsymbol{R}_{\{\otimes,x_1,\ldots,x_t\}}[\boldsymbol{S}(1)])=(u/v)^t$. According to Definition 3, the contrast of the reconstructed secret image is

$$\alpha=\frac{\frac{u}{v}-(\frac{u}{v})^t}{1+(\frac{u}{v})^t}. \quad (15)$$

■

Obviously, when $u/v=1/2$, the proposed method reduces to Chen and Tsao's (2,n) scheme [20]. For a certain t, different values of u/v can be adopted to calculate the contrast.

B. XOR-Based Meaningful VC

In conventional VC, participants are required to stack their share for revealing the secret. Reconstructed secret image with low image quality reveals due to the stacking operation. XOR-based VC is a new branch of VC system that offers better visual quality by adopting XOR operation to decrypt the secret. In the decryption phase, only some small, cheap and lightweight computational devices are needed, which makes the XOR-based VC become feasible. However, the reported XOR-based VC [28] suffers from the following deficiencies:

- Pixel expansion. The generated share is larger than the original secret image.
- Meaningless appearance of the share. The random-looking further increases the chance of suspicion on secret communication and imposes difficulty for managing the shares.

To solve the above-mentioned two problems, a (n,n) XOR-based meaningful VC is introduced. To construct the meaningful scheme, two methods are devised, namely a (n,n) gener-

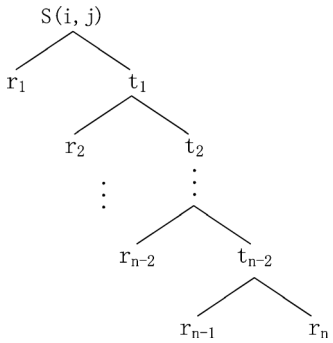


Fig. 2. Diagram of share construction for Algorithm 3.

alized RG-based VC and a synthesizing algorithm. In the (n, n) generalized RG-based VC, the n shares are constructed by recursively applying the $(2, 2)$ scheme for $n-1$ times. Diagram of the share construction is illustrated in Fig. 2. Description on the (n, n) generalized RG-based VC is given below.

Algorithm 3 Generalized RG-based VC for (n, n) Case.

Input: a binary secret image $\boldsymbol{S}$ with $M \times N$ pixels, and three parameters u, v, d.
Output: n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.
Step 1: For each position (i, j) in the secret image, Steps 2 and 3 are performed to generate n shared pixels $\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_n(i, j)$.
Step 2: By recursively applying the $(2, 2)$ generalized RG-based VC for $n-1$ times, n pixels $r_1, r_2, \ldots, r_n$ are constructed by

$$\begin{cases} r_1, t_1 = GRG[(2,2), \boldsymbol{S}(i,j), u, v, d], \\ r_2, t_2 = GRG[(2,2), t_1, u, v, d], \\ \quad \vdots \\ r_{n-2}, t_{n-2} = GRG[(2,2), t_{n-3}, u, v, d], \\ r_{n-1}, r_n = GRG[(2,2), t_{n-2}, u, v, d], \end{cases} \tag{16}$$

where procedure GRG is implemented by generalized RG-based VC, $(2, 2)$ is the desired threshold, $S(i, j), t_1, \ldots, t_{n-2}$ are the input pixels, and u, v, d are the three parameters. Indeed, the $n-1$ pixels$r_1, r_2, \ldots, r_{n-1}$ are generated by the random bit generator $g(u/v)$ in the $(2, 2)$ scheme.
Step 4: The order of the n pixels$r_1, \ldots, r_n$ are rearranged and the rearranged n pixels are assigned to $\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_n(i, j)$.
Step 5: Output the n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.

We further prove that the (n, n) generalized RG-based VC is a valid construction of XOR-based VC scheme by Theorem 6. Insight analysis is given as follows.

Lemma 6: Given n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$ generated from Algorithm 3, every share is a generalized RG and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u/v$ where $k = 1, \ldots, n$.

Proof: According to Algorithm 3, the n shared pixels $r_1, \ldots, r_n$ are constructed by recursively applying the $(2, 2)$ scheme. Based on Lemma 1, every shared pixel is a generalized random pixel and cannot reveal any information about the secret pixel. Thus, we have $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u/v$ for $k = 1, \ldots, n$. ■

Lemma 7: Given n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$ constructed from Algorithm 3, the XOR-ed result by any $k < n$ shares $\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}} = \boldsymbol{R}_{x_1} \oplus \cdots \oplus \boldsymbol{R}_{x_k}$ gives no clue about the secret: $T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(1)])$.

Proof: Assume k shared pixels, denoted as $r_{x_1}, \ldots, r_{x_k}$, are collected from the n shared pixels $r_1, \ldots, r_n$, i.e., $\{x_1, \ldots, x_k\} \in \{1, \ldots, n\}$. To prove that the XOR-ed result by any $k < n$ shared pixels do not reveal the secret pixel $S(i, j)$, two cases are considered: (1)$n \in \{x_1, \ldots, x_k\}$ and (2)$n \notin \{x_1, \ldots, x_k\}$.

(1) $n \in \{x_1, \ldots, x_k\}$. We consider $r_n \oplus r_g \oplus \cdots \oplus r_h$ with $g, \ldots, h$ being the indices in $\{x_1, \ldots, x_k\}$ besides n. Since the value t_{n-2} can be recovered by $r_{n-1} \oplus r_n$, assume that $n-1 \in \{x_1, \ldots, x_k\}$. We obtain

$$\begin{aligned} r_n \oplus r_g \oplus \cdots \oplus r_h &= r_n \oplus r_{n-1} \oplus r_g \oplus \cdots \oplus r_{h-1} \\ &= t^R_{n-2} \oplus r_g \oplus \cdots \oplus r_{h-1} \end{aligned} \tag{17}$$

with $g, \ldots, h-1$ being the indices in $\{x_1, \ldots, x_k\}$ besides n and $n-1$, where t^R_{n-2} resembles t_{n-2} but meaningless.

Likewise, assume that $n-2, n-3, \ldots, n-k \in \{x_1, \ldots, x_k\}$, then

$$\begin{aligned} r_n \oplus r_g \oplus \cdots \oplus r_h &= t^R_{n-2} \oplus r_g \oplus \cdots \oplus r_{h-1} \\ &= t^R_{n-1} \oplus r_g \oplus \cdots \oplus r_{h-2} \\ &= \ldots = t^R_{n-k} \end{aligned} \tag{18}$$

is achieved where t^R_{n-k} resembles t_{n-k} visually but meaningless. Since $k < n$, the XOR-ed result by k shared pixels do not reveal the secret pixel. And it at most reveals a value t_{n-k} which is meaningless.

(2) $n \notin \{x_1, \ldots, x_k\}$. Since the k shared pixels are constructed by the random bit generator, the XOR-ed result by any k shared pixels give no clue about the associated secret pixel.

Based on the above analysis, the secret pixel cannot be recovered by conducting XOR operation on any $k < n$ shared pixels. As a result, the XOR-ed result of any $k < n$ shares $\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}} = \boldsymbol{R}_{x_1} \oplus \cdots \oplus \boldsymbol{R}_{x_k}$ gives no clue about the secret: $T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(1)])$. ■

Lemma 8: Given n shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$ constructed from Algorithm 3, the XOR-ed result of n shares visually reveals the secret: $T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(1)])$.

Proof: Let $\boldsymbol{S}(i, j)$ be the secret pixel and let $r_1, \ldots, r_n$ be the n generated shared pixels. We first consider t_{n-2} which can be recovered from r_{n-1} and r_n. Let $t^R_{n-2} = r_{n-1} \oplus r_n$ be the reconstructed pixel. When $t_{n-2} = 0$, the probability for t^R_{n-2} to be 0 is 1. When $t_{n-2} = 1$, the probability for t^R_{n-2} to be 0 is $(u/v)[(u-d)/(v-d)] + (1-u/v)[1-u/(v-d)] < 1$.

Simply, we calculate the average light transmission of t^R_{n-2} by using another approach. Since r_{n-1} is generated by the random bit generator, we consider r_n. Let r^R_n be the reconstructed pixel which looks like r_n. Suppose that P^0_n (resp. P^1_n) is the probability for r^R_n to be 0 when r_n is 0 (resp. 1). Therefore, we have $Prob(r^R_n = 0) = Prob(r_n = 0) \times P^0_n$

and $Prob(r_n^R = 1) = Prob(r_n = 1) \times (1 - P_n^1)$. Since r_n is a leaf node in the construction tree, we have $r_n^R = r_n$, which indicates that $P_n^0 = 1$ and $P_n^1 = 0$. Based on P_n^0 and P_n^1, we calculate the average light transmission of t_{n-2}^R. t_{n-2}^R can be represented by $t_{n-2}^R = r_{n-1} \oplus r_n^R$. When $t_{n-2} = 0$, the average light transmission of t_{n-2}^R is computed by

$$\begin{aligned} &T(t_{n-2}^R[t_{n-2} = 0]) \\ &\quad = Prob(r_{n-1} = 0) \times Prob(r_n^R = 0) \\ &\qquad + Prob(r_{n-1} = 1) \\ &\qquad \times Prob(r_n^R = 1) \\ &\quad = Prob(r_{n-1} = 0) \times Prob(r_n = 0) \\ &\qquad \times P_n^0 + Prob(r_{n-1} = 1) \\ &\qquad \times Prob(r_n = 1) \times (1 - P_n^1) \\ &\quad = Prob(r_{n-1} = 0) \times Prob(r_n = 0) \times 1 \\ &\qquad + Prob(r_{n-1} = 1) \\ &\qquad \times Prob(r_n = 1) \times 1 \\ &\quad = 1. \end{aligned} \tag{19}$$

Similarly, when $t_{n-2} = 1$, the average light transmission of t_{n-2}^R is calculated by

$$\begin{aligned} &T(t_{n-2}^R[t_{n-2} = 1]) \\ &\quad = Prob(r_{n-1} = 0) \times Prob(r_n^R = 0) \\ &\qquad + Prob(r_{n-1} = 1) \\ &\qquad \times Prob(r_n^R = 1) \\ &\quad = Prob(r_{n-1} = 0) \times Prob(r_n = 0) \times P_n^0 \\ &\qquad + Prob(r_{n-1} = 1) \\ &\qquad \times Prob(r_n = 1) \times (1 - P_n^1) \\ &\quad = Prob(r_{n-1}=0) \times Prob(r_n=0) \times 1 + Prob(r_{n-1}=1) \\ &\qquad \times Prob(r_n = 1) \times 1 \\ &\quad = \left(\frac{u}{v}\right)\left(\frac{u-d}{v-d}\right) \\ &\qquad + \left(1 - \frac{u}{v}\right)\left(1 - \frac{u}{v-d}\right). \end{aligned} \tag{20}$$

Further, let P_{n-2}^0 (resp. P_{n-2}^1) be the probability for t_{n-2}^R to be 0 when t_{n-2} is 0 (resp. 1). Actually, P_{n-2}^0 and P_{n-2}^1 are $T(t_{n-2}^R[t_{n-2} = 0])$ and $T(t_{n-2}^R[t_{n-2} = 1])$, respectively. Similarly, when $t_{n-3} = 0$, the average light transmission of t_{n-3}^R is calculated by

$$\begin{aligned} &T(t_{n-3}^R[t_{n-3} = 0]) \\ &\quad = Prob(r_{n-2} = 0) \times Prob(t_{n-2}^R = 0) \\ &\qquad + Prob(r_{n-2} = 1) \\ &\qquad \times Prob(t_{n-2}^R = 1) \\ &\quad = Prob(r_{n-2} = 0) \times Prob(t_{n-2} = 0) \times P_{n-2}^0 \\ &\qquad + Prob(r_{n-2} = 1) \times Prob(t_{n-2} = 1) \times (1 - P_{n-2}^1) \\ &\quad = \left(\frac{u}{v}\right) P_{n-2}^0 + \left(1 - \frac{u}{v}\right)(1 - P_{n-2}^1). \end{aligned} \tag{21}$$

When $t_{n-3} = 1$, the average light transmission of t_{n-3}^R is calculated by

$$\begin{aligned} &T(t_{n-3}^R[t_{n-3} = 1]) \\ &\quad = Prob(r_{n-2} = 0) \times Prob(t_{n-2}^R = 0) \\ &\qquad + Prob(r_{n-2} = 1) \\ &\qquad \times Prob(t_{n-2}^R = 1) \\ &\quad = Prob(r_{n-2} = 0) \\ &\qquad \times Prob(t_{n-2} = 0) \times P_{n-2}^0 \\ &\qquad + Prob(r_{n-2} = 1) \\ &\qquad \times Prob(t_{n-2} = 1) \times (1 - P_{n-2}^1) \\ &\quad = \left(\frac{u}{v}\right)\left(\frac{u-d}{v-d}\right) P_{n-2}^0 \\ &\qquad + \left(1 - \frac{u}{v}\right)\left(1 - \frac{u}{v-d}\right)(1 - P_{n-2}^1). \end{aligned} \tag{22}$$

Since $0 \le (u-d)/(v-d) < 1$ and $0 < 1 - u/(v-d) \le 1$, we have $(u/v)[(u-d)/(v-d)]P_{n-2}^0 < (u/v)P_{n-2}^0$ and $(1-u/v)[1-u/(v-d)](1-P_{n-2}^1) \le (1-u/v)(1-P_{n-2}^1)$. Therefore, $T(t_{n-3}^R[t_{n-3} = 0]) > T(t_{n-3}^R[t_{n-3} = 1])$ is obtained.

By the same method, we get $T(t_{n-4}^R[t_{n-4} = 0]) > T(t_{n-4}^R[t_{n-4} = 1]), \ldots, T(\boldsymbol{S}^R(i,j)[\boldsymbol{S}(i,j) = 0]) > T(\boldsymbol{S}^R(i,j)[\boldsymbol{S}(i,j) = 1])$ where $t_{n-4}^R, \ldots, \boldsymbol{S}^R(i,j)$ are the reconstructed pixels. Based on Definition 1, $T(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)])$ is obtained. The XOR-ed result by the n shares reveals the secret. ■

Theorem 6: Algorithm 3 is a valid construction of (n, n) XOR-based VC. The following conditions are satisfied:

- Every share is a generalized RG and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u/v$ where $k = 1, \ldots, n$.
- The XOR-ed result by any $k < n$ shares $\boldsymbol{R}_{\{\oplus,x_1,\ldots,x_k\}} = \boldsymbol{R}_{x_1} \oplus \cdots \oplus \boldsymbol{R}_{x_k}$ gives no clue about the secret: $T(\boldsymbol{R}_{\{\oplus,x_1,\ldots,x_k\}}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{\{\oplus,x_1,\ldots,x_k\}}[\boldsymbol{S}(1)])$.
- The XOR-ed result by n shares visually reveals the secret: $T(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)])$.

Proof: Based on Lemmas 6, 7 and 8, the mentioned three conditions are satisfied. Algorithm 3 is a valid construction of (n, n) XOR-based VC. ■

In conventional VC and XOR-based VC, the shared pixels only carry the secret information. Hence the shares are noise-like. Herein, we generate the shares with respect to a cover image. Two different light transmissions in a share are utilized to represent the white and black colors in the cover image. Specifically, we synthesize two (n, n) generalized RG-based VC schemes with two different average light transmissions into one for generating meaningful shares. The (n, n) XOR-based meaningful VC by synthesizing two (n, n) algorithms is described as follows.

Algorithm 4 OR-based meaningful VC for (n, n) Case.

Input: a binary secret image $\boldsymbol{S}$ and a cover image, both with $M \times N$ pixels, and six parameters u_0, v_0, d_0 and u_1, v_1, d_1.

Output: n meaningful shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.

Step 1: For each position (i, j) in the secret image, Step 2 or 3 is performed to generate n shared pixels $\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_2(i, j)$.

Step 2: When the corresponding cover image pixel $\boldsymbol{C}(i, j) = 0$, the n shared pixels are constructed by

$$[\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_n(i, j)] = GRG[(n, n), \boldsymbol{S}(i, j), u_0, v_0, d_0], \tag{23}$$

where procedure GRG is implemented by generalized RG-based VC, (n, n) is the desired threshold, $\boldsymbol{S}(i, j)$ is the secret pixel, and u_0, v_0, d_0 are the three parameters.

Step 3: When the corresponding cover image pixel $\boldsymbol{C}(i, j) = 1$, the n shared pixels are constructed by

$$[\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_n(i, j)] = GRG[(n, n), \boldsymbol{S}(i, j), u_1, v_1, d_1]. \tag{24}$$

Step 4: Output the n meaningful shares $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$.

To make sure that the generated shares resemble the cover image with the correct colors, the parameters must satisfy the following condition:

$$0 < \frac{u_1}{v_1} < \frac{u_0}{v_0} < 1. \tag{25}$$

The following Theorem 7 indicates that the (n, n) XOR-based meaningful VC is a valid construction of VC when XOR decryption is applied.

Theorem 7: Let $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_n$ be the n shares generated from Algorithm 4, Algorithm 4 is a valid construction of XOR-based meaningful VC for (n, n) case. The following conditions are satisfied:

- Every share is a meaningful image which looks like the cover image : $T(\boldsymbol{R}_k[\boldsymbol{C}(0)]) > T(\boldsymbol{R}_k[\boldsymbol{C}(1)])$, and gives no clue about the secret: $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)])$, where $k = 1, \ldots, n$.
- The XOR-ed result by any $k < n$ shares $\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}} = \boldsymbol{R}_{x_1} \oplus \cdots \oplus \boldsymbol{R}_{x_k}$ cannot disclose the secret: $T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(1)])$.
- The XOR-ed result by n shares visually reveals the secret: $T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(1)])$.

Proof: When the cover image pixel $\boldsymbol{C}(i, j) = 0$ (resp. $\boldsymbol{C}(i, j) = 1$), the average light transmissions of the n shared pixels $\boldsymbol{R}_1(i, j), \ldots, \boldsymbol{R}_n(i, j)$ are u_0/v_0 (resp. u_1/v_1). Since $u_0/v_0 > u_1/v_1$, we have $T(\boldsymbol{R}_k(i, j)[\boldsymbol{C}(i, j) = 0]) > T(\boldsymbol{R}_k(i, j)[\boldsymbol{C}(i, j) = 1])$ where $k = 1, \ldots, n$. By Definition 1, $T(\boldsymbol{R}_k[\boldsymbol{C}(0)]) > T(\boldsymbol{R}_k[\boldsymbol{C}(1)])$ is obtained. Every share is a meaningful image which resembles the cover image.

For the white area of the cover image, we calculate the corresponding average light transmissions of every share based on the first condition of Theorem 6, as denoted by $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u_0/v_0, k = 1, \ldots, n$. For the black area of the cover image, we also get $T(\boldsymbol{R}_k[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_k[\boldsymbol{S}(1)]) = u_1/v_1, k = 1, \ldots, n$. As a result, every single share gives no clue about the secret.

Based on the second condition of Theorem 6, the average light transmissions of the XOR-ed result by any $k < n$ shares are $T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(0)]) = T(\boldsymbol{R}_{\{\oplus, x_1, \ldots, x_k\}}[\boldsymbol{S}(1)])$ when these XOR-ed pixels are corresponding to the white area of the cover image. Similarly, the same conclusion holds when these XOR-ed pixels are corresponding to the black area of the cover image. Hence, the XOR-ed result by any k shares do not reveal any information about the secret.

According to the third condition of Theorem 6, the average light transmissions of the XOR-ed result by n shares are $T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(0)]) > T(\boldsymbol{R}_{\{\oplus, 1, \ldots, n\}}[\boldsymbol{S}(1)])$ when these XOR-ed pixels belong to the white area of the cover image. And the same result holds as well when these XOR-ed pixels belong to the black area of the cover image. Thus, the XOR-ed result by n shares visually reveals the secret. ■

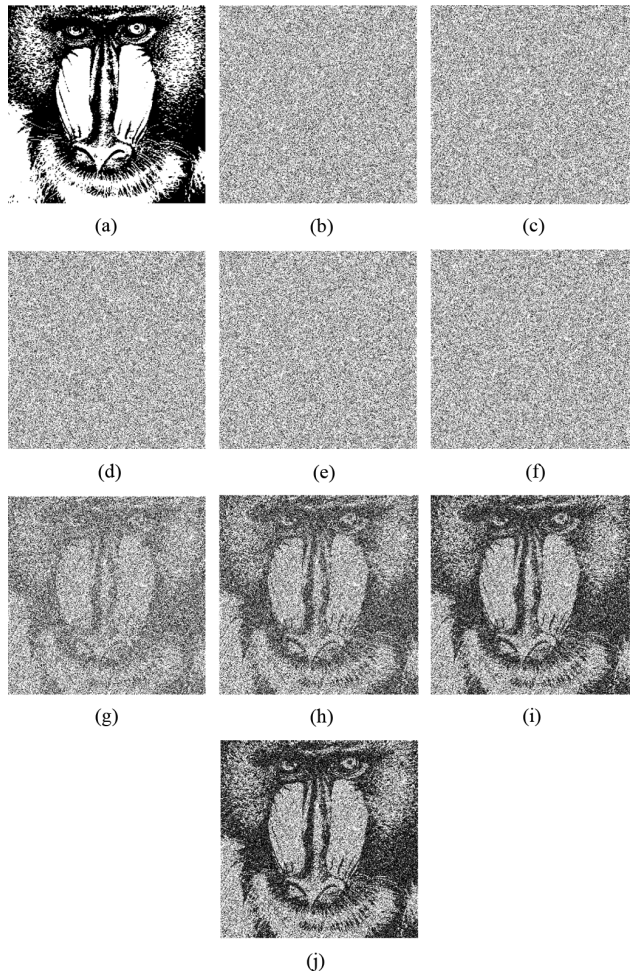


Fig. 3. Simulation results of the $(2, 5)$ case by Algorithm 2. (a) The secret image; (b)–(f) four generated shares; (g)–(j) stacked results by two, three, four, and five shares, respectively.

V. Experimental Results and Discussions

Extensive experimental results by the $(2, n)$ generalized RG-based VC and (n, n) XOR-based meaningful VC are illustrated in this section. Moreover, some comparisons and further discussions on the two algorithms are provided as well.

A. Simulations for the $(2, n)$ Generalized Rg-based VC

A $(2, 5)$ generalized RG-based VC by Algorithm 2 is demonstrated in Fig. 3, where $u = 3, v = 4, d = 1$. The secret image is shown in Fig. 3(a) and the five generated shares are illustrated in Figs. 3(b)–3(f). By stacking any two or more shares, the secret

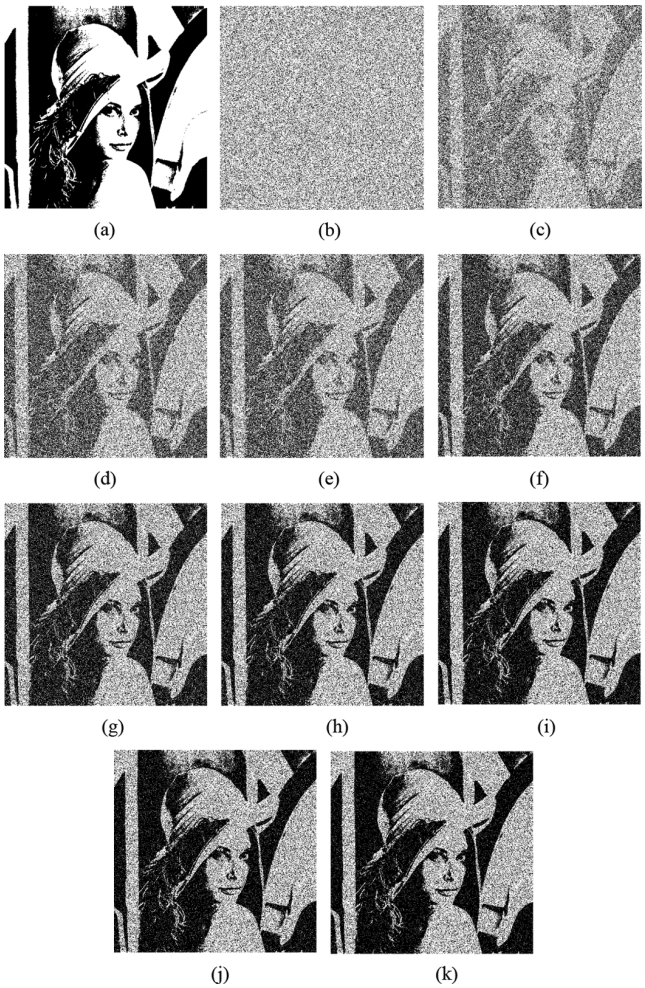


Fig. 4. Simulation results of the $(2, 10)$ case by Algorithm 2. (a) The secret image; (b) one of the generated shares, (c)–(k) stacked results by two, three, four, five, six, seven, eight, nine, and ten shares, respectively.

image is visually revealed, as demonstrated in Figs. 3(g)–3(j). Another experiment by Algorithm 2 for the $(2, 10)$ case is exhibited in Fig. 4 with parameters $u = 3, v = 4, d = 1$, where the secret image is shown in Fig. 4(a) and one of the generated shares is demonstrated in Fig. 4(b). The secret image is visually reconstructed by superimposing any two or more shares together, where the revealed secret images are illustrated in Figs. 4(c)–4(k).

B. Simulations for the (n, n) XOR-Based Meaningful VC

Simulation results by Algorithm 4 for constructing XOR-based meaningful VC are provided in Figs. 5 and 6, where Figs. 5 and 6 show the $(2, 2)$ and $(3, 3)$ schemes, respectively. In the $(2, 2)$ scheme, the six parameters are with the following configurations: $u_0 = 3, v_0 = 4, d_0 = 1$, and $u_1 = 1, v_1 = 4, d_1 = 1$. The secret image and cover image are illustrated in Figs. 5(a) and 5(b). Two generated meaningful shares which look like the cover image are demonstrated in Figs. 5(c) and 5(d). The XOR-ed result by the two shares is shown in Fig. 5(e), which reveals the secret.

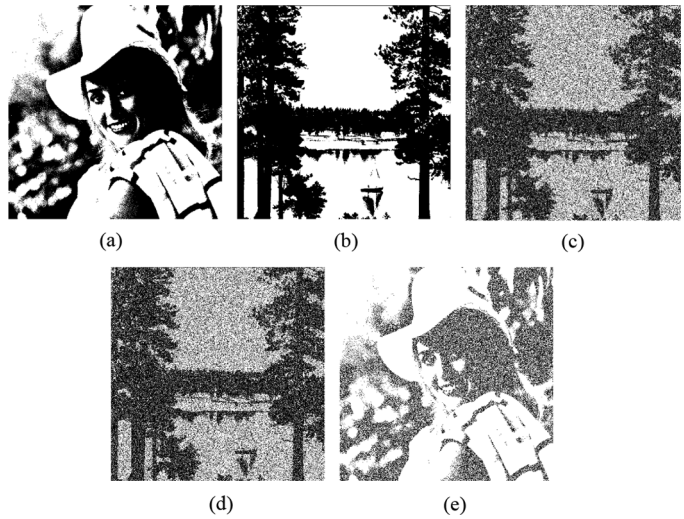


Fig. 5. Simulation results of the $(2, 2)$ XOR-based meaningful VC by Algorithm 4. (a) The secret image; (b) the cover image; (c)–(d) two meaningful shares; (e) XOR-ed result by two shares.

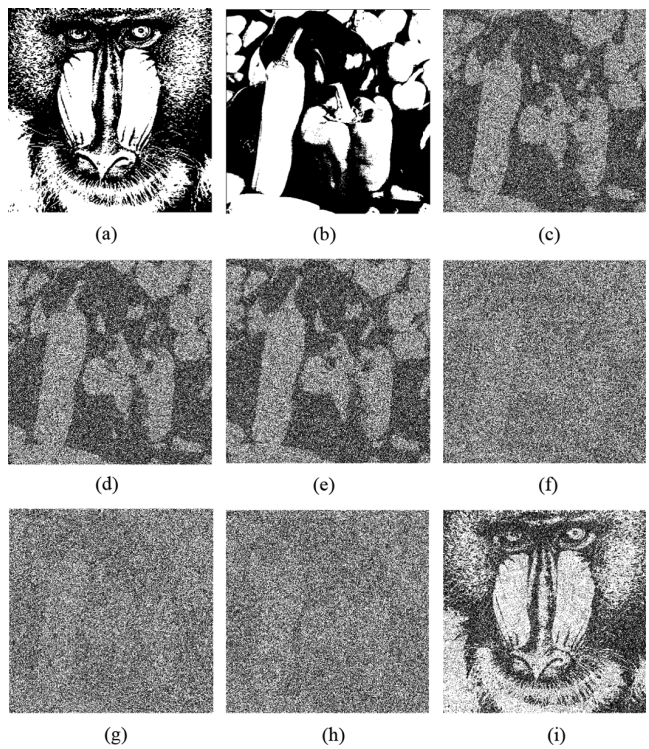


Fig. 6. Simulation results of the $(3, 3)$ XOR-based meaningful VC by Algorithm 4. (a) The secret image; (b) the cover image; (c)–(e) two meaningful shares; (f)–(h) XOR-ed results by any two of the three shares; (i) XOR-ed result by three shares.

The six parameters used in the $(3, 3)$ scheme are configured as $u_0 = 2.5, v_0 = 4, d_0 = 1.5$, and $u_1 = 1.5, v_1 = 4, d_1 = 1.5$.Figs. 6(a) and 6(b) show the secret image and cover image used in the $(3, 3)$ scheme, respectively. The meaningful shares are demonstrated in Figs. 6(c)–6(e).The XOR-ed results by any two of the three shares are illustrated in Figs. 6(f)–6(h), which give no clue about the secret. The secret is reconstructed by conducting XOR operation on the three shares, as shown in Fig. 6(i).

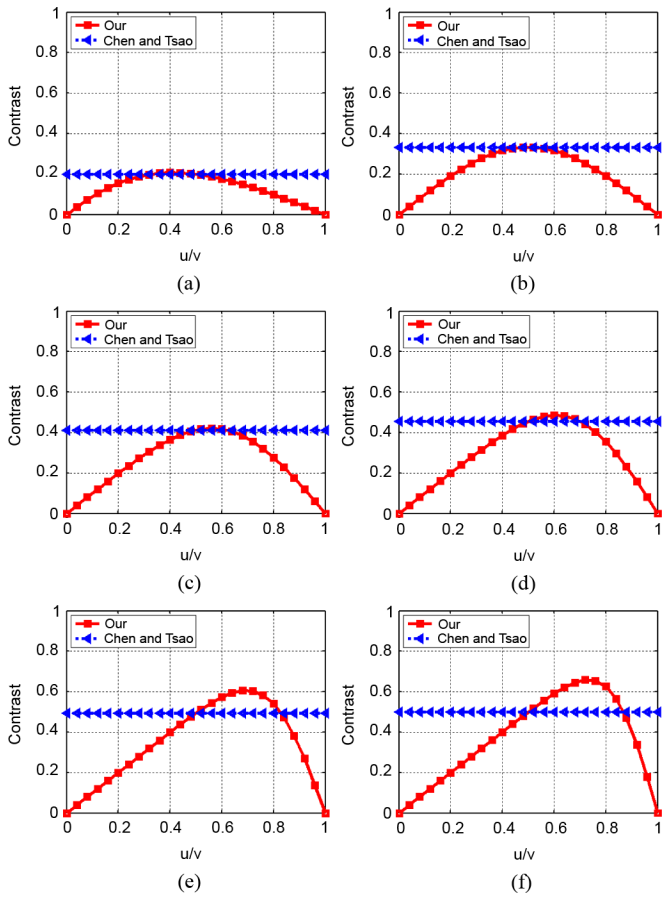


Fig. 7. Contrast curves of Algorithm 2 and Chen and Tsao's $(2, n)$ method [20] when possible values of u/v are used. (a) The $(2, 2)$ scheme; (b) the $(2, 3)$ scheme; (c) the $(2, 4)$ scheme; (d) the $(2, 5)$ scheme; (e) the $(2, 8)$ scheme; (f) the $(2, 10)$ scheme.

C. Visual Performance of the $(2, n)$ Generalized RG-Based VC

Herein, we investigate the visual performance of the proposed $(2, n)$ generalized RG-based VC. The contrast of the recovered secret image are utilized to evaluate the visual quality. Further, Chen and Tsao's $(2, n)$ scheme [20] is adopted for comparisons.

As formulated in Theorem 5, the contrast of the reconstructed secret image in Algorithm 2 is calculated by

$$\alpha = \frac{\frac{u}{v} - (\frac{u}{v})^n}{1 + (\frac{u}{v})^n} \tag{26}$$

where u/v is the average light transmission of a share. For a specific threshold, e.g., (2,2), we can calculate the possible contrasts by using different values of u/v. And the contrast of Chen and Tsao's method [20] can be computed by

$$\alpha = \frac{\frac{1}{2} - (\frac{1}{2})^n}{1 + (\frac{1}{2})^n}. \tag{27}$$

Fig. 7 shows the contrast curves of Algorithm 2 and Chen and Tsao's $(2, n)$ method [20] by using possible values of u/v. Except for the $(2, 3)$ scheme, larger contrasts can be obtained by Algorithm 2 when appropriate values of u/v are selected, according to Fig. 7. For example, larger contrast is achieved by Algorithm 2 for the $(2, 2)$ scheme, when $u/v = 0.4$ based on Fig. 7(a). The associated contrast is 0.2069, while the contrast by Chen and Tsao's method [20] is 0.2. Moreover, optimal contrasts are obtained as well by Algorithm 2 for the $(2, 4), (2, 5), (2, 8)$ and $(2, 10)$ schemes, when $u/v = 0.6$ based on Figs. 7(c)–7(f). We further discuss the contrast when n is big enough. Fig. 8 demonstrates the contrast curves of Algorithm 2 and Chen and Tsao's $(2, n)$ method [20] when $n = 20$ and $n = 100$. In these cases, Algorithm 2 offers better visual quality as well when appropriate values of u/v are adopted, e.g., $u/v = 0.6$.

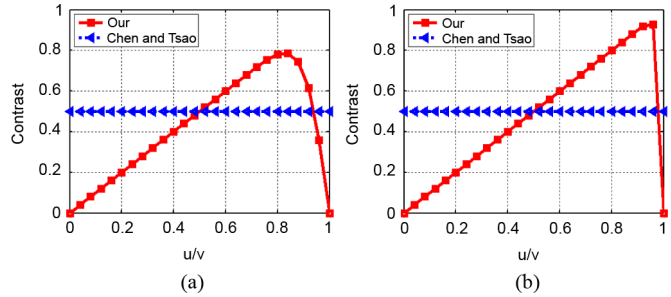


Fig. 8. Contrast curves of Algorithm 2 and Chen and Tsao's $(2, n)$ method [20] for large n, when possible values of u/v are used. (a) The $(2, 20)$ scheme; (b) the (2,100) scheme.

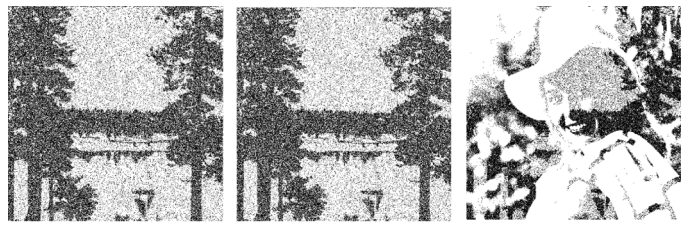


Fig. 9. Example of $(2, 2)$ XOR-based meaningful VC, where the recovered secret image is not homogeneous. (a)–(b) Two meaningful shares; (c) the XOR-ed result by two shares.

D. Available Values for u_0/v_0 and u_1/v_1

The proposed XOR-based meaningful VC is constructed by synthesizing two XOR-based VC schemes with different values of u/v. But different values of u/v would introduce different light transmissions of the reconstructed result. These light transmissions may vary from each other significantly, and lead to a consequence that the reconstructed secret image is not homogeneous. An example is shown in Fig. 9 with the six parameters configured as $u_0 = 9, v_0 = 10, d_0 = 1$, and $u_1 = 4, v_1 = 10, d_1 = 4$. Obviously, some reconstructed pixels which belong to the black area of the original secret image are darker than the others. The reason of resulting in inhomogeneous recovered secret image is that the light transmissions $(T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)])$ and $T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]))$ of the recovered secret image by value u_0/v_0 are significantly different from the light transmissions $(T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)])$ and $T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]))$ by value u_1/v_1. In this example, $T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) = T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) = 0$, but $T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]) = 0.8$ and $T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]) = 0.2$. $T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)])$ is dramatically different from $T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)])$.

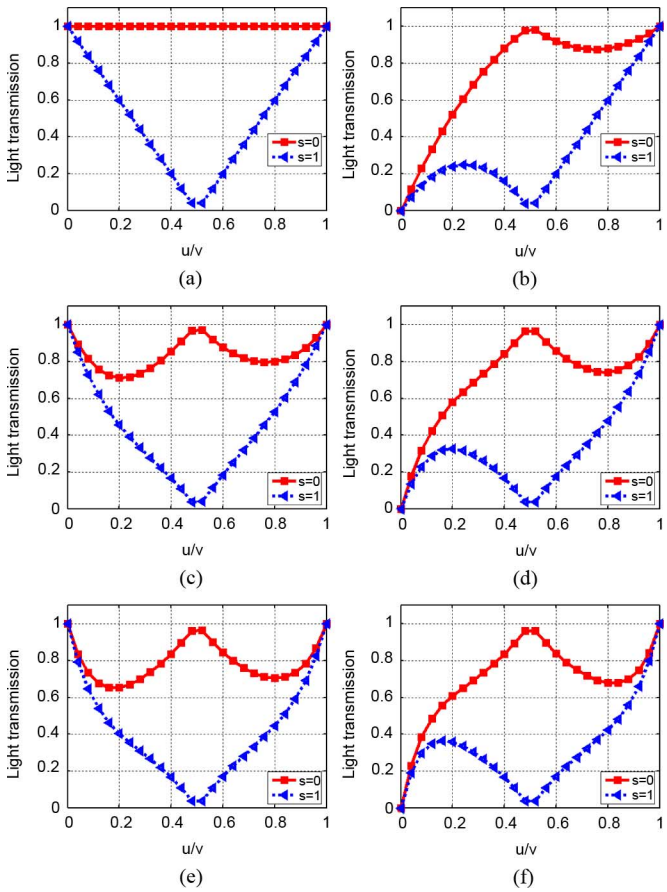


Fig. 10. Average light transmission curves of Algorithm 3 with different values of u/v. (a) The $(2,2)$ scheme; (b) the $(3,3)$ scheme; (c) the $(4,4)$ scheme; (d) the $(5,5)$ scheme; (e) the $(6,6)$ scheme; (f) the $(7,7)$ scheme.

For obtaining homogeneous recovered secret image for the (n,n) XOR-based meaningful VC, the four light transmissions should satisfy the following conditions:

$$T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) \approx T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(0)]) \tag{28}$$

and

$$T^{u_0/v_0}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]) \approx T^{u_1/v_1}(\boldsymbol{R}_{\{\oplus,1,\ldots,n\}}[\boldsymbol{S}(1)]). \tag{29}$$

Based on the analysis provided in the proof of Theorem 8, the average light transmissions of reconstructed results by n shares can be calculated iteratively. Herein, possible values of u/v are adopted to compute the light transmissions of XOR-ed result by n shares in Algorithm 3, as demonstrated in Fig. 10. Specifically, Fig. 10(a) illustrates the average light transmission curves of the XOR-ed result by two shares in the $(2,2)$ scheme, when possible values of u/v are utilized. To satisfy the homogeneous conditions, the values of u_0/v_0 and u_1/v_1 can be

$$\frac{u_0}{v_0} = 0.5 + t \text{ and } \frac{u_1}{v_1} = 0.5 - t \tag{30}$$

where $0 < t < 0.5$.

We further analyze the light transmission curves for schemes such as $(3,3),\ldots,(7,7)$, as shown in Figs. 10(b)–10(f). We notice that the curves in the $(3,3)$, $(5,5)$ and $(7,7)$ scheme are similar. To meet the homogeneous conditions, the values of u_0/v_0 and u_1/v_1 can be 0.6 and 0.4, respectively. For the $(4,4)$ and $(6,6)$, values for u_0/v_0 and u_1/v_1 are suggested to be 0.6 and 0.4 as well. We further investigate the light transmission curves when n is much bigger, as demonstrated in Fig. 11. We conclude from the light transmission curves that suggested values for u_0/v_0 and u_1/v_1 to meet the homogeneous conditions are

$$\frac{u_0}{v_0} = \begin{cases} 0.5+t, & \text{if } n=2, \\ 0.6, & \text{otherwise,} \end{cases} \tag{31}$$

and

$$\frac{u_1}{v_1} = \begin{cases} 0.5-t, & \text{if } n=2, \\ 0.4, & \text{otherwise} \end{cases} \tag{32}$$

where $0 < t < 0.5$. Note that, the 0.6 and 0.4 are suggested values, some values near 0.6 and 0.4 are applicable as well.

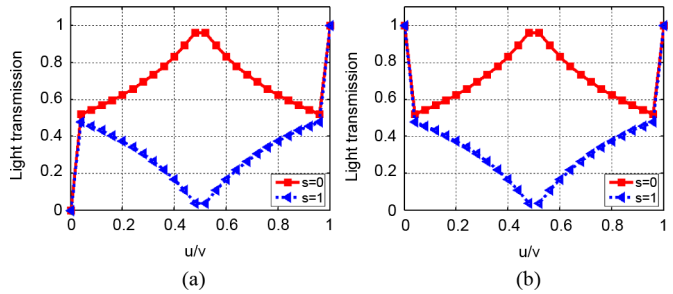


Fig. 11. Average light transmission curves of Algorithm 3 with different values of u/v, when large n is applied. (a) The $(99,99)$ scheme; (b) the (100,100) scheme.

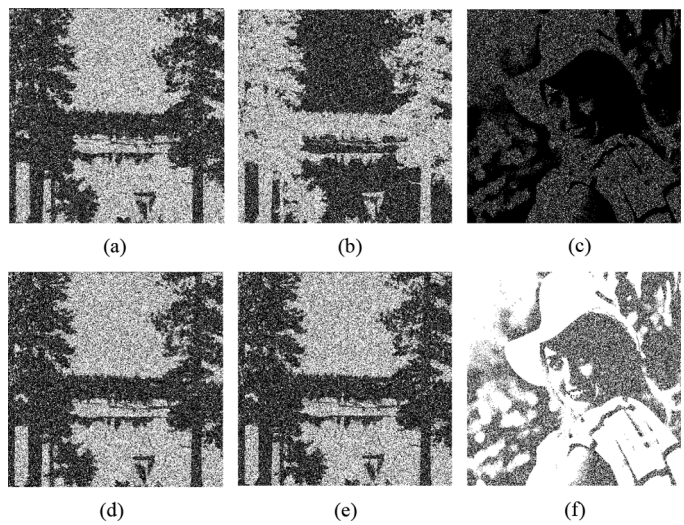


Fig. 12. Comparison of visual quality between Algorithm 4 and Chen and Tsao's meaningful RG-based VC [27], where complementary shares are used in Chen and Tsao's method. (a)–(b) Two shares generated from [27]; (c) the recovered secret image by (a) and (b); (d)–(e) two shares generated from Algorithm 4; (f) the recovered secret image by (d) and (e).

E. Comparisons for XOR-Based Meaningful VC

Comparison of visual quality between Algorithm 4 and Chen and Tsao's meaningful RG-based VC [27] is demonstrated in Fig. 12, where complementary shares are used in Chen and Tsao's approach. In their method [27], the parameter which defines the portion of shared pixels in the meaningful share is set to be 0.5. In Algorithm 4, the six parameters are configured as

TABLE II
COMPARISON OF CONTRAST AND VARIANCE FOR THE $(2, 2)$ CASE BETWEEN ALGORITHM 4 AND CHEN AND TSAO'S APPROACH [27], WHERE COMPLEMENTARY SHARES ARE USED IN CHEN AND TSAO'S APPROACH

Methods	Images	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [27]	Share 1	0.3994	0.7566	0.7762	0.7674	0.7442	0.7443
	Share 2	-	-	-	-	-	-
	Recovered Secret	0.2506	0	0.1851	0.3778	0.5396	0.7559
Algorithm 4	Share 1	0.3963	0.7506	0.7285	0.7669	0.6966	0.7611
	Share 2	0.4008	0.7473	0.7168	0.7460	0.7461	0.7510
	Recovered Secret	0.3340	0.9964	0.7686	0.5093	0.2499	0

TABLE III
COMPARISON OF CONTRAST AND VARIANCE FOR THE $(2, 2)$ CASE BETWEEN ALGORITHM 4 AND CHEN AND TSAO'S APPROACH [27], WHERE COMPLEMENTARY SHARES ARE NOT USED IN CHEN AND TSAO'S APPROACH

Methods	Images	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [27]	Share 1	0.1986	0.7520	0.8329	0.8591	0.9019	0.9976
	Share 2	0.1997	0.7397	0.8005	0.8585	0.9094	1.0015
	Recovered Secret	0.2510	0	0.1916	0.3698	0.5619	0.7504
Algorithm 4	Share 1	0.3963	0.7506	0.7285	0.7669	0.6966	0.7611
	Share 2	0.4008	0.7473	0.7168	0.7460	0.7461	0.7510
	Recovered Secret	0.3340	0.9964	0.7686	0.5093	0.2499	0

TABLE IV
COMPARISON OF FEATURE AMONG ALGORITHM 4 AND RELATED METHODS

Schemes	Features					
	Meaningful Share	Pixel Expansion	Code book Needed	Decryption	Visual Quality	Type of VSS
Ref.[28]	No	Yes	Yes	XOR	High	(k,n)
Ref.[21]	No	No	No	Stack	Low	(k,n)
Ref.[27]	Yes	No	No	Stack	Low	(2,n),(n,n)
Algorithm 4	Yes	No	No	XOR	High	(n,n)

$u_0 = 3, v_0 = 4, d_0 = 1$, and $u_1 = 1, v_1 = 4, d_1 = 1$. Contrasts and variances calculated from the shares and recovered secret image in this experiment are provided in Table II. When the contrasts of shared image quality is approximately the same, larger contrast of the reconstructed image is obtained by Algorithm 4. Variance serves as the secondary measurement to evaluate the image quality when the contrasts of shares are nearly the same. In this experiment, the variances are approximately the same for the shares. But adopting complementary shares is not suitable for practical applications, since the complementary share do not resemble natural image.

More comparisons of visual quality between Algorithm 4 and Chen and Tsao's scheme [27] are exhibited in Fig. 13 and Table IIII, where complementary shares are not used in their approach [27]. Obviously, larger contrasts of both the meaningful shares and reconstructed secret image are provided by Algorithm 4. Moreover, smaller variances of the shares are achieved by Algorithm 4 as well. Superior visual quality is obtained.

Feature comparison among Algorithm 4 and related methods is shown in Table IV. Major advantages of Algorithm 4 are that (1) shares are with meaningful contents and (2) superior visual quality is achieved. Meanwhile, merits such as no pixel expansion and no code book required are also maintained.

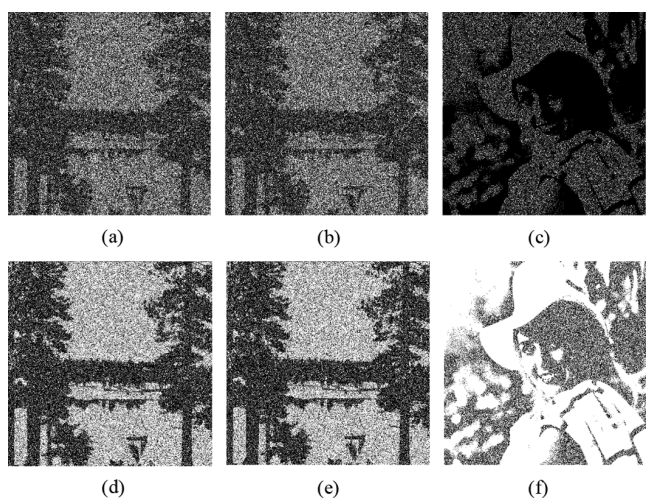


Fig. 13. Comparison of visual quality between Algorithm 4 and Chen and Tsao's meaningful RG-based VC [27], where complementary shares are not used in Chen and Tsao's method. (a)–(b) Two shares generated from [27]; (c) the recovered secret image by (a) and (b); (d)–(e) two shares generated from Algorithm 4; (f) the recovered secret image by (d) and (e).

VI. CONCLUSIONS

This paper firstly introduces the concept of generalized RG. By adopting the generalized RG, a basic VC algorithm, $(2, 2)$ generalized RG-based VC, is constructed. The average light transmission of a share becomes adjustable. Inspired by basic algorithm, two VC schemes, including a $(2, n)$ generalized RG-based VC and a (n, n) XOR-based meaningful VC, are derived for different application scenarios. For the $(2, n)$ generalized RG-based VC, better visual quality of the recovered secret image is obtained. For the XOR-based meaningful VC, shares with meaningful contents are constructed, where the

meaningful shares ease the management of shadows and reduce the chance of suspicion on secret image communication. Furthermore, superior visual quality is provided by the meaningful method as well.

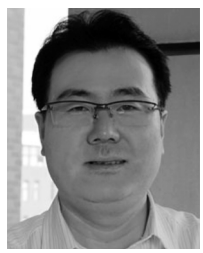
ACKNOWLEDGMENT

The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have greatly improved this work.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes Comput. Sci.*, vol. 950, no. 1, pp. 1–12, 1995.
[2] J. W. Yan, "A comprehensive study of visual cryptography," *Trans. Data Hiding and Multimedia Security V*, pp. 70–105, 2010.
[3] G. Ateniese, C. Blundo, A. De Santis, and D. Stinson, "Visual cryptography for general access structures," *Inf. Computat.*, vol. 129, no. 2, pp. 86–106, 1996.
[4] C. Lin and W. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, no. 1-3, pp. 349–358, 2003.
[5] Y. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003.
[6] D. Jin, W.-Q Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *J. of Electron. Imag.*, vol. 14, no. 3, p. 033019, 2005.
[7] I. Kang, G. Arce, and H. Lee, "Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132–145, Jan. 2011.
[8] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, no. 1-2, pp. 143–161, 2001.
[9] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.
[10] Z. Zhou, G. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
[11] Z. Wang, G. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[12] C. Blundo, A. DeSantis, and D. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptol.*, vol. 12, no. 4, pp. 241–289, 1999.
[13] T. Hofmeister, M. Krause, and H. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Comput. Sci.*, vol. 240, no. 2, pp. 471–485, 2000.
[14] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fund. Electron., Commun., Comput. Sci.*, vol. 82, no. 10, pp. 2172–2177, 1999.
[15] C. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 486–494, 2004.
[16] S. Cimato, R. DePrisco, and A. De Santis, "Probabilistic visual cryptography schemes," *The Comput. J.*, vol. 49, no. 1, pp. 97–107, 2006.
[17] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, pp. 377–379, 1987.
[18] S. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014–1031, 2007.
[19] S. Shyu, "Image encryption by multiple random grids," *Pattern Recognit.*, vol. 42, no. 7, pp. 1582–1596, 2009.
[20] T. Chen and K. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognit.*, vol. 42, no. 9, pp. 2203–2217, 2009.
[21] T. Chen and K. Tsao, "Threshold visual secret sharing by random grids," *J. Syst. Softw.*, vol. 84, pp. 1197–1208, 2011.
[22] X. Wu and W. Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," *J. Syst. Softw.*, vol. 85, no. 5, pp. 1119–1134, 2011.
[23] X. Wu and W. Sun, "Visual secret sharing for general access structures by random grids," *IET Inf. Security*, vol. 6, no. 4, pp. 299–309, 2012.
[24] X. Wu and W. Sun, "Improving the visual quality of random grid-based visual secret sharing," *Signal Process.*, vol. 93, no. 5, pp. 977–995, 2013.
[25] X. Wu, T. Liu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing via error diffusion," *J. Vis. Commun. Image Representat.*, vol. 24, no. 5, pp. 552–566, 2013.
[26] X. Wu and W. Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions," *J. Vis. Commun. Image Representat.*, vol. 24, no. 1, pp. 48–62, 2013.
[27] T. Chen and K. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693–1703, Nov. 2011.
[28] P. Tuyls, H. Hollmann, J. Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Designs, Codes, Cryptography*, vol. 37, no. 1, pp. 169–186, 2005.
[29] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognit.*, vol. 40, no. 10, pp. 2776–2785, 2007.
[30] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[31] T. Chen and C. Wu, "Efficient multi-secret image sharing based on Boolean operations," *Signal Process.*, vol. 91, no. 1, pp. 90–97, 2011.

Xiaotian Wu received the Ph.D. degree in computer science from the School of Information Science and Technology, Sun Yat-sen University, in 2013. He also received the Bachelor degree in software engineering from the School of Software, Sun Yat-sen University, in 2008. His research interests include visual cryptography, information hiding, and multimedia security.



Wei Sun received the Ph.D. degree in computer science from Sun Yat-sen University, in 2004. He is currently a professor with the School of Software, Sun Yat-sen University, China. His current research interests include information security, digital watermarking, and computer graphics.