J. Vis. Commun. Image R. 24 (2013) 48–62

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Random grid-based visual secret sharing with abilities of OR and XOR decryptions

Xiaotian Wu [a], Wei Sun [b,*]

[a] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
[b] School of Software, Sun Yat-sen University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 15 August 2012
Accepted 24 October 2012
Available online 16 November 2012

Keywords:
Visual secret sharing
Visual cryptography
Random grid
OR
XOR
Decryption
Visual quality
Contrast

ABSTRACT

Random grid (RG) is a methodology to construct visual secret sharing (VSS) scheme without pixel expansion. In some reported RG-based VSS schemes, a secret image can be visually reconstructed only by stacking operation, even thought some light-weight computational devices are available. In this paper, a novel RG-based VSS is developed, where the secret image can be recovered in two situations: (1) when computational devices are not available, the secret image can be reconstructed by stacking the shares directly, and (2) when some light-weight computational devices are available, the secret image can be decrypted by XOR operation. Further, the decrypted secret image quality by stacking operation is approximately the same as that of conventional RG-based VSS. But better visual quality is obtained by XOR operation.

1. Introduction

Sensitive information kept in one single information-carrier would be easily lost or destructed. Secret sharing is one alternative method which has been proposed in 1979 [1,2] for addressing the above problem. In a (k,n) threshold secret sharing scheme, a secret message is encoded into n pieces (called shares or shadows) that can be delivered to n associated participants. The secret message can be decoded from k or more shadows, whereas, the knowledge of any $k-1$ or fewer shadows gives no clue about the secret.

Visual secret sharing (VSS) is a novel type of secret sharing that focuses on protecting images. The basic principles of VSS were introduced by Naor and Shamir [3], where n random-looking shares are constructed from a secret image and distributed to n participants in a (k,n) threshold VSS. The secret image can be visually reconstructed when any k or more participants present their shares and stack them together. The advantage of VSS is that the decryption of secret image is completely based on human visual system without the aid of any computational devices. Based on the pioneer work of Naor and Shamir [3], extensive investigations on VSS were conducted. Most of the studies focus on the following issues.

- *Contrast*. The visual quality of the recovered secret image is evaluated by contrast, where contrast is expected to be as large as possible so that human eyes can easily identify the secret information in the stacked result.
- *Pixel expansion*. In conventional VSS schemes, one secret pixel is replaced by $m \geqslant 2$ shared pixels in each shadow. Pixel expansion indicates that each generated share is m times as big as the original secret image.

Studies on enhancing the visual quality of decrypted secret image can be found in [4,5]. They claimed that secret information in the stacked result can be easily identified when the black secret pixels are perfectly reconstructed. Further, better image quality can be obtained as well, by applying the XOR-based VSS schemes [6,7]. Usually, the stacking operation in VSS can be denote by Boolean OR operation. The background of reconstructed secret image is inevitably darken when more shadows are stacked together. But in XOR-based VSS, this can be avoided. However, decryption in XOR-based VSS requires some light-weight computational devices, which makes it useless when such devices are not available. Further, pixel expansion problem still exists in XOR-based VSS [7].

To solve the pixel expansion problem, image size invariant VSS schemes including the probabilistic VSS and random grid-based (RG-based) VSS were employed. In probabilistic VSS [8–10], each secret pixel is encoded by column matrices, and hence, non-expansible shadows are obtained. But code book is still required in the encryption phase. Sometimes, designing a code book is not trivial. Differ from probabilistic VSS, a code book is not required in the encoding phase of RG-based VSS. Basic model of RG-based VSS was first proposed by Kafir and Keren [11]. Meanwhile, three distinct algorithms for the (2,2) VSS were presented as well. Inspired by Kafri and Keren, Shyu [12] introduced an enhanced algorithm to share grayscale/color images. The same author further

[*] Corresponding author.
E-mail address: sunwei@mail.sysu.edu.cn (W. Sun).

1047-3203/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jvcir.2012.11.001

extended Kafri and Keren's model to accomplish the (n,n) threshold case [13]. Chen and Tsao [14] proposed algorithms for the $(2,n)$ and (n,n) cases. A more generalized model, the (k,n) threshold scheme, was also introduced by Chen and Tsao [15].

In this paper, a model for constructing (k,n) RG-based VSS with abilities of OR and XOR decryptions is proposed. When computational devices are not available, the secret image can be decrypted by stacking sufficient shares. When light-weight computational devices are available, the secret image can be reconstructed via XOR operation. Pixel expansion problem is solved by the proposed method, and competitive visual quality of the recovered secret image is obtained by XOR decryption according to the provided experiments.

The remaining part of this paper is organized as follows. The $(2,n)$ RG-based VSS scheme is described in Section 2, as well as the (k,n) scheme. Section 3 introduces the proposed method. Meanwhile, theoretical analysis on the proposed method is also presented. Experimental results and discussions are provided in Section 4. Section 5 concludes our work.

2. Related works

The proposed method employs the $(2,n)$ and (k,n) RG-based VSS schemes. Hence, the two methods are briefly described in this section, as well as some basic definitions on random grid.

A random grid (RG) [11] is defined as a transparency comprising a two-dimensional array of pixels, where each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a random process with an equal probability. Different RG-based VSS schemes such as (n,n) [13], $(2,n)$ [14] and (k,n) [15] have been proposed in the last five years. Among them, the $(2,n)$ scheme provides competitive image quality and the (k,n) scheme gives a generalized model for constructing flexible sharing strategy. In this paper, digits 0 and 1 are used to denote the white and black pixels, respectively. Symbols $\otimes$ and $\oplus$ represent the Boolean OR and XOR operations, respectively. Detailed description of the two methods is formulated as follows.

(2,n) RG-based VSS

```
Input: A $M \times N$ binary secret image $S$.
Output: $n$ shares $R_1, \ldots, R_n$.
Step 1: For each position $(i,j) \in \{(i,j) | 1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N\}$,
    Step 2 or 3 is applied according to the color of the current
    processing secret pixel.
Step 2: If $S(i,j) = 0$, one random bit $b$ is generated by assigning
    $b$ the value 0 or 1. The $n$ shared pixels are constructed by
    $R_1(i,j) = \cdots = R_n(i,j) = b$.
Step 3: If $S(i,j) = 1$, $n$ shared pixels $R_1(i,j), \ldots, R_n(i,j)$ are
    generated by randomly assigning each of them the value 0
    or 1.
Step 4: Output the $n$ shares $R_1, \ldots, R_n$.
```

(k,n) RG-based VSS

```
Input: A $M \times N$ binary secret image $S$.
Output: $n$ shares $R_1, \ldots, R_n$.
Step 1: For each position $(i,j) \in \{(i,j) | 1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N\}$,
    repeat Steps 2–5.
Step 2: Generate $k-1$ bits $b_u$ $(1 \leqslant u \leqslant k-1)$ by randomly
    assigning value 0 or 1 to $b_u$.
Step 3: Compute the $k$-th bit $b_k$ by
```

(*continued*)

(k,n) RG-based VSS

```
$b_k = S(i,j) \oplus b_1 \oplus \cdots \oplus b_{k-1}$
where $\oplus$ denotes the Boolean XOR operation.
Step 4: Generate $n-k$ bits $b_v$ $(k+1 \leqslant v \leqslant n)$ by randomly
    assigning value 0 or 1 to $b_v$.
Step 5: Randomly assign the $n$ bits $b_1, \cdots, b_n$ to $n$ random grids
    $R_1(i,j), \ldots, R_n(i,j)$.
Step 6: Output the $n$ shares $R_1, \ldots, R_n$.
```

For the $(2,n)$ (resp. (k,n)) scheme, the secret image is revealed by stacking any two (resp. k) or more shares. To analyze the RG-based VSS, some definitions which are obtained from [12,14] are adopted, as described as follows.

Definition 1 (Average light transmission [12,14]). For a certain pixel p in a binary image R whose size is $M \times N$, the light transmission of a white pixel is defined as $T(p) = 1$. Whereas, $T(p) = 0$ for p is a black pixel. Totally, the average light transmission of R is defined as

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

Definition 2 (Area representation [12]). Let $S(0)$ (resp. $S(1)$) be the area of all the white (resp. black) pixels in secret image S where $S = S(0) \cup S(1)$ and $S(0) \cap S(1) = \emptyset$. Therefore, $R[S(0)]$ (resp. $R[S(1)]$) is the corresponding area of all the white (resp. black) pixels in the random grid R.

Definition 3 (Contrast [12]). The contrast of the reconstructed secret image $S^R_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ with respect to the original secret image S is

$$\alpha = \frac{T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(0)]) - T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(1)])}{1 + T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(1)])}.$$

Definition 4 (Visual recognition [14]). The revealed secret image $S^R_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ is visual recognizable as the original secret image S by contrast $\alpha > 0$. Precisely, it is $T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(0)]) > T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(1)])$. Whereas, it gives no clue about the secret image when $\alpha = 0$.

Definition 3 on the contrast, which is borrowed from [12], has been widely accepted and used in some reported RG-based VSS schemes [12–17]. Other definition on contrast used in some RG-based VSS [18] and probabilistic VSS [9] is given by

$$\alpha = T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(0)]) - T(S^R_{i_1 \otimes \cdots \otimes i_k}[S(1)]),$$

where it evaluates the absolute difference of light transmission rate between secret and background. For a (k,n) conventional deterministic VSS, the contrast in most of the VSS is defined as

$$\alpha = \frac{h - l}{m},$$

where m is referred to the pixel expansion, h (resp. l) represents the number of zeros of the OR-ed result by any k rows in the corresponding basis matrix B_0 (resp. B_1). The definition of contrast used in [18,9] is similar with that used in most conventional deterministic VSS [3,19]. It merely calculates the deference. Some reconstructed secret images may be with the same difference, but those with darker reconstructed black pixels show better visual quality [4] since human eyes can identify darker reconstructed black pixels easily. That means, when the same difference is achieved, better image quality is obtained when $T(S^R_{i_1\otimes\cdots\otimes i_k}[S(1)]$ becomes smaller. As a result, Definition 3 is more reasonable for evaluating the contrast of RG-based VSS.

For conventional deterministic VSS and probabilistic VSS, whether the secret image can be revealed or not can be determined by the contrast. When the contrast is bigger than zero (the difference is bigger than zero), the secret image is disclosed. Such definition is the same as Definition 4, since the contrast of RG-based VSS is bigger than zero if and only if the difference is bigger than zero.

3. The proposed method

In some reported RG-based VSS schemes, the secret image is revealed only by stacking sufficient shares together. The visual quality of the stacked decrypted secret image is not satisfactory due to the background of the recovered secret image becomes darken when more shares are superimposed. On the other hand, some RG-based VSS schemes cannot recovered the secret image even though some light-weight computational devices are available. XOR-based VSS is another methodology to carry out visual secret sharing via Boolean XOR operation, where better visual quality of the reconstructed secret image is achieved. However, secret image in XOR-based VSS cannot be recovered without the aid of computational devices, which provide the XOR operation.

RG-based VSS and XOR-based VSS have some limitations. For RG-based VSS, the visual quality of the reconstructed secret image is not competitive since the background becomes darker when more shares are stacked together. Further, a pixel-wise alignment is preferred for decrypting the secret image quickly and correctly. For XOR-based VSS, a computational device is needed to perform the secret image decryption. When such a computational device is not available, XOR-based VSS becomes useless.

XOR-based VSS is an alternative approach to solve the problems of RG-based VSS. And RG-based VSS can dispose the concerns in XOR-based VSS. It is desired to integrate both the conventional VSS and XOR-based VSS together. Herein, the proposed method with two decoding abilities serves as a supplementary tool for both the RG-based VSS and XOR-based VSS. The application scenario for the proposed scheme can be considered as follows. When computational devices are not available, the secret image can be decrypted by stacking the shares directly. The deficiency of XOR-based VSS is solved. For the alignment problem, some additional marks can be made on the shares. When these marks are aligned, the shares are aligned and the secret image can be reconstructed. But these marks should be removable and not damage the shares. When some computational devices can be used, the secret image can be recovered with better visual quality via Boolean XOR operation. Since the shares are processed by computational devices, the alignment problem is solved as well. The proposed method exhibits the abilities of both stacking and XOR decryptions, which can deal with the problems occurred in RG-based VSS and XOR-based VSS.

According to the reported (k,n) RG-based VSS, the XOR operation is utilized in the share construction. On the other hand, recovering the secret image via XOR operation seems possible. For example, when $k = n$, the share construction is completely based on XOR operation. The secret image can be lossless recovered from the n shares by using XOR operation. However, the secret image cannot be reconstructed via XOR operation in the (k,n) scheme when $k < n$. We aim to constitute a XOR-based VSS algorithm by adopting the processing mentioned in RG-based VSS. Provided that such a XOR-based VSS is a valid construction, the secret image can be reconstructed by XOR operation. Since the shares are constructed by utilizing the processing mentioned in RG-based VSS, the secret image can be reconstructed by stacking operation possibly. As a result, such a VSS scheme maintains the abilities of stacking and XOR decryptions.

Diagram of share construction for the proposed method is illustrated in Fig. 1. The proposed method utilizes existing RG-based VSS for generating the shares. For each secret pixel, a number t is randomly chosen from the set $\{k, k+1, \ldots, n\}$. Then, n bits $b_1, b_2, \ldots, b_n$ are constructed by the (t,n) threshold RG-based VSS with respect to the current secret pixel. The n generated bits are rearranged and assigned to the n shares. Detailed description of the share construction for the proposed method is given below.

The proposed (k,n) VSS with abilities of OR and XOR decryptions

```
Input: A $M \times N$ binary secret image $S$.
Output: $n$ shares $R_1, \ldots, R_n$.
Step 1: For each position $(i,j) \in \{(i,j)|1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N\}$,
    repeat Steps 2–4.
Step 2: Randomly select a number $t$ from $\{k, k+1, \ldots, n\}$.
Step 3: Generate $n$ bits $b_1, b_2, \ldots, b_n$ by

    $[b_1, b_2, \ldots, b_n] = Random\_Grid(S(i,j), t, n)$

    where $S(i,j)$ is the current processing secret pixel, $(t,n)$ is the
    desired threshold, and procedure $Random\_Grid$ is
    implemented by reported RG-based VSS. More specifically,
    when $t = 2$, the procedure is implemented by Chen and
    Tsao's $(2,n)$ method [14]. When $t > 2$, the procedure is
    implemented by Chen and Tsao's $(k,n)$ method [15].
Step 4: The order of the $n$ bits $b_1, b_2, \ldots, b_n$ are randomly
    rearranged, and the rearranged $n$ bits are assigned to the $n$
    shares $R_1(i,j), R_2(i,j), \cdots, R_n(i,j)$.
Step 5: Output the $n$ shares $R_1, \ldots, R_n$.
```

When computational devices are not available, the secret image can be reconstructed by stacking k or more shares. When some light-weight computational devices are available, the secret image can be revealed by applying XOR operation on k or more shares. Theoretical analysis on the proposed method is provided as follows.

Lemma 1. *Given a secret pixel s and n shared pixels $r_1, \ldots, r_n$ generated by the proposed method, let o be the stacked result of any d pixels from $r_1, \ldots, r_n$. When $s = 0$, the average light transmission of the stacked result is*

$$T^{OR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=0]) + \cdots + T^{OR,d}_{(n,n)}(o[s=0])\right],$$

where $T^{OR,d}_{(k,n)}, \ldots, T^{OR,d}_{(n,n)}$ are the average light transmissions of the stacked results by d pixels in the $(k,n), \ldots, (n,n)$ threshold RG-based VSS schemes [14,15]. When $s = 1$, the average light transmission of the stacked result is

$$T^{OR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=1]) + \cdots + T^{OR,d}_{(n,n)}(o[s=1])\right].$$

Proof. In the proposed method, the n pixels are generated by one of the $n-k+1$ RG-based VSS schemes such as (k,n), $(k+1,n), \ldots, (n,n)$. When the n pixels are generated by a specific (t,n) RG-based VSS, where $k \leqslant t \leqslant n$, the average light transmissions are $T^{OR,d}_{(t,n)}(o[s=0])$ and $T^{OR,d}_{(t,n)}(o[s=1])$. The probability for the (t,n) RG-based VSS being chosen is $\frac{1}{n-k+1}$. Hence, the average light transmissions of the stacked result are

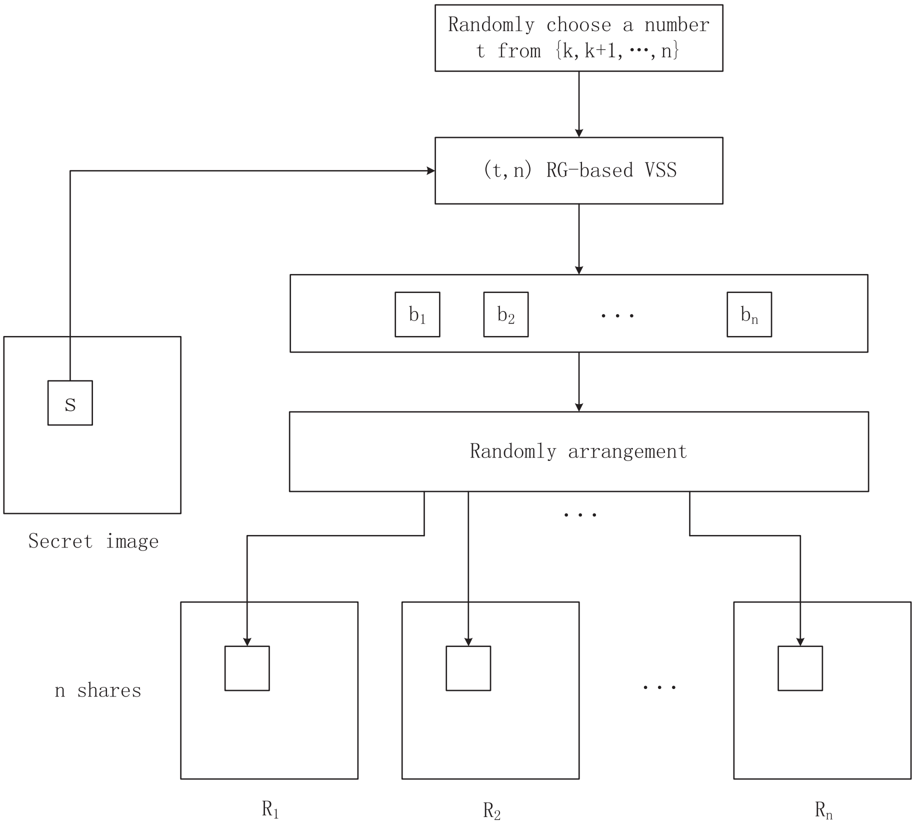

Fig. 1. Diagram of share construction of the proposed scheme.

$$T^{OR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=0]) + \cdots + T^{OR,d}_{(n,n)}(o[s=0])\right]$$

and

$$T^{OR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=1]) + \cdots + T^{OR,d}_{(n,n)}(o[s=1])\right]. \qquad \square$$

Theorem 1. *Given a secret image S and n shares $R_1, \ldots, R_n$ generated by the proposed method, let O be the stacked result of any d shares from $R_1, \ldots, R_n$. The proposed method is a valid construction of (k,n) threshold RG-based VSS when OR decryption is applied, which satisfies the following three conditions.*

- *Each share is a RG, as denoted by*
$$T^{OR,1}(R_i[S(0)]) = T^{OR,1}(R_i[S(1)]), \quad 1 \leqslant i \leqslant n.$$
- *When $d < k$, the stacked result gives no clue about the secret, as represented by*
$$T^{OR,d}(O[S(0)]) = T^{OR,d}(O[S(1)]).$$
- *When $d \geqslant k$, the stacked result reveals the secret, as represented by*
$$T^{OR,d}(O[S(0)]) > T^{OR,d}(O[S(1)]).$$

Proof. Given a secret pixel s and n shared pixels $r_1, \ldots, r_n$ generated by the proposed method, let o be the stacked result of any d pixels from $r_1, \ldots, r_n$. According to Lemma 1, we have

$$T^{OR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=0]) + \cdots + T^{OR,d}_{(n,n)}(o[s=0])\right]$$

and

$$T^{OR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{OR,d}_{(k,n)}(o[s=1]) + \cdots + T^{OR,d}_{(n,n)}(o[s=1])\right].$$

When $d = 1$, the stacked result o reduces to a random grid pixel, where $o = r_i, 1 \leqslant i \leqslant n$. We get

$$T^{OR,1}(r_i[s=0]) = \frac{1}{(n-k+1)}\left[T^{OR,1}_{(k,n)}(r_i[s=0]) + \cdots + T^{OR,1}_{(n,n)}(r_i[s=0])\right], \quad 1 \leqslant i \leqslant n,$$

and

$$T^{OR,1}(r_i[s=1]) = \frac{1}{(n-k+1)}\left[T^{OR,1}_{(k,n)}(r_i[s=1]) + \cdots + T^{OR,1}_{(n,n)}(r_i[s=1])\right], \quad 1 \leqslant i \leqslant n.$$

In the $(2,n)$ and (k,n) RG-based VSS schemes [14,15], each generated random grid pixel give no clue about the secret pixel, as denoted by

$$T^{OR,1}_{(k,n)}(r_i[s=0]) = T^{OR,1}_{(k,n)}(r_i[s=1]), \ldots, T^{OR,1}_{(n,n)}(r_i[s=0]) = T^{OR,1}_{(n,n)}(r_i[s=1]).$$

As a result, we obtain

$$T^{OR,1}(r_i[s=0]) = T^{OR,1}(r_i[s=1]), \quad 1 \leqslant i \leqslant n.$$

According to Definition 1, $T^{OR,1}(R_i[S(0)]) = T^{OR,1}(R_i[S(1)]),\ 1 \leqslant i \leqslant n$. The first condition is met.

In the $(2,n)$ and (k,n) RG-based VSS [14,15], insufficient number of random grid pixels cannot disclose the secret pixel, as represented by

$$T^{OR,d}_{(k,n)}(o[s=0]) = T^{OR,d}_{(k,n)}(o[s=1]), \cdots, T^{OR,d}_{(n,n)}(o[s=0]) = T^{OR,d}_{(n,n)}(o[s=1]),$$

where $d < k$. Hence, we achieve

$$T^{OR,d}(o[s=0]) = T^{OR,d}(o[s=1]).$$

Based on Definition 1, $T^{OR,d}(O[S(0)]) = T^{OR,d}(O[S(1)])$. The second condition is satisfied.

In the $(2,n)$ and (k,n) RG-based VSS [14,15], the secret pixel can be revealed by sufficient number of random grid pixels, as denoted by

$$T^{OR,d}_{(k,n)}(o[s=0]) > T^{OR,d}_{(k,n)}(o[s=1]), \ldots, T^{OR,d}_{(n,n)}(o[s=0]) > T^{OR,d}_{(n,n)}(o[s=1]),$$

where $d \geqslant k$. Hence, we achieve

$$T^{OR,d}(o[s=0]) > T^{OR,d}(o[s=1]).$$

Based on Definition 1, $T^{OR,d}(O[S(0)]) > T^{OR,d}(O[S(1)])$. The third condition is satisfied.

In general, the proposed method is a valid construction of the RG-based VSS when OR decryption is applied. □

Lemma 2. *Given d binary pixels $r_1, \ldots, r_d$ generated randomly, let $o = r_1 \oplus \cdots \oplus r_d$ be the XOR-ed result of the d pixels. The average light transmission of o is*

$$T^{XOR,d}(o) = \frac{1}{2}.$$

Proof. By induction on d, (1) when $d = 2$, $o = r_1 \oplus r_2$. If $r_1 = 0,\ r_2 = 0$ or $r_1 = 1,\ r_2 = 1$, $o = 0$. If $r_1 = 0,\ r_2 = 1$ or $r_1 = 1,\ r_2 = 0$, $o = 1$. Let procedure $Prob(A)$ denote the probability of the event A being true. Hence, we have $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$. The light transmission of o is $T^{XOR,2}(o) = \frac{1}{2}$.

(2) Assume that the claim holds for $d-1$, i.e., $T^{XOR,d-1}(o) = \frac{1}{2}$. That is $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$. For $r_1 \oplus \cdots \oplus r_{d-1} \oplus r_d$, if $r_1 \oplus \cdots \oplus r_{d-1} = 0, r_d = 0$ or $r_1 \oplus \cdots \oplus r_{d-1} = 1, r_d = 1$, the XOR result o is 0. If $r_1 \oplus \cdots \oplus r_{d-1} = 1, r_d = 0$ or $r_1 \oplus \cdots \oplus r_{d-1} = 0$, $r_d = 1$, the XOR result o is 1. Therefore, we get $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$. The light transmission is $T^{XOR,d}(o) = \frac{1}{2}$. The claim also holds for d. □

Lemma 3. *Let s be the secret pixel. n random grid pixels $r_1, \ldots, r_n$ are generated by Chen and Tsao's (k,n) RG-based VSS. That is, $n-1$ pixels $r_1, \ldots, r_{k-1}, r_{k+1}, \ldots, r_n$ are generated randomly, and $r_k = s \oplus r_1 \oplus \cdots \oplus r_{k-1}$. Let $o = r_{i_1} \oplus \cdots \oplus r_{i_d}$ be the XOR-ed result of any d pixels, where $d < k$. The light transmissions are*

$$T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}.$$

Proof. Two cases are considered: (1) $k \in \{i_1, \ldots, i_d\}$, and (2) $k \notin \{i_1, \ldots, i_d\}$.

(1) $k \in \{i_1, \ldots, i_d\}$. As $k \in \{i_1, \ldots, i_d\}$, the set $\{i_1, \ldots, i_d\}$ can be denoted as $\{i_1, \ldots, i_{d-1}, k\}$. Let a set $\Gamma_1 = \{u, \ldots, v\} = \{i_1, \ldots, i_{d-1}\} \cap \{1, \ldots, k-1\}$. Moreover, two sets $\Gamma_2 = \{g, \ldots, h\} = \{i_1, \ldots, i_{d-1}\} - \Gamma_1$ and $\Gamma_3 = \{e, \ldots, f\} = \{1, \ldots, k-1\} - \Gamma_1$ can be obtained. In general, $\{i_1, \ldots, i_d\}$ can be represented as $\Gamma_1 \cup \Gamma_2 \cup \{k\}$, and $\{1, \ldots, k\}$ can be denoted as $\Gamma_1 \cup \Gamma_3 \cup \{k\}$. Pixel r_k is generated by $r_k = s \oplus r_1 \oplus \cdots \oplus r_{k-1}$. It can be represented as $r_k = s \oplus r_u \oplus \cdots \oplus r_v \oplus r_e \oplus \cdots \oplus r_f$. The XOR result by any d pixels is represented by

$$\begin{aligned} o &= r_{i_1} \oplus \cdots \oplus r_{i_d} = r_{i_1} \oplus \cdots \oplus r_{i_{d-1}} \oplus r_k \\ &= r_u \oplus \cdots \oplus r_v \oplus r_g \oplus \cdots \oplus r_h \oplus r_k \\ &= s \oplus r_e \oplus \cdots \oplus r_f \oplus r_g \oplus \cdots \oplus r_h. \end{aligned}$$

Let $r = r_e \oplus \cdots \oplus r_f \oplus r_g \oplus \cdots \oplus r_h$ where $r_e, \ldots, r_f, r_g, \ldots, r_h$ are generated randomly. Hence, we get $Prob(r = 0) = Prob(r = 1) = \frac{1}{2}$ by Lemma 2. When $s = 0$, the XOR-ed result of d pixels is given as $o = s \oplus r = r$. We have $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$. When $s = 1, o = s \oplus r = \overline{r}$. We obtain $Prob(o = 1) = Prob(o = 0) = \frac{1}{2}$. As a result, $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$ no matter the secret pixel s is 0 or 1. The light transmissions are $T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}$.

(2) $k \notin \{i_1, \ldots, i_d\}$. The d pixels are randomly generated, they are independent of the secret pixel s. The light transmissions of the XOR-ed result of the d pixels are $T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}$ according to Lemma 2. □

Lemma 4. *Let s be the secret pixel. n random grid pixels $r_1, \ldots, r_n$ are generated by Chen and Tsao's (k,n) RG-based VSS. That is, $n-1$ pixels $r_1, \ldots, r_{k-1}, r_{k+1}, \ldots, r_n$ are generated randomly, and $r_k = s \oplus r_1 \oplus \cdots \oplus r_{k-1}$. Let $o = r_{i_1} \oplus \cdots \oplus r_{i_d}$ be the XOR result of any d pixels, where $d \geqslant k$. The light transmissions are*

$$T^{XOR,d}(o[s=0]) = \begin{cases} \frac{1}{2}\left[1 + \frac{1}{\binom{n}{k}}\right], & \text{if } d = k, \\ \frac{1}{2}, & \text{if } d > k \end{cases}$$

and

$$T^{XOR,d}(o[s=1]) = \begin{cases} \frac{1}{2}\left[1 - \frac{1}{\binom{n}{k}}\right], & \text{if } d = k, \\ \frac{1}{2}, & \text{if } d > k. \end{cases}$$

Proof. For the d generated random grid pixels, α pixels are selected from $r_1, \ldots, r_k$, and β pixels are selected from $r_{k+1}, \ldots, r_n$. The proof considers two cases: (1) $\alpha = k$ and $\beta = d - \alpha$, (2) $\alpha < k$ and $\beta = d - \alpha$. For the description, let o_α and o_β be the XOR-ed results of the α pixels and β pixels, respectively.

(1) $\alpha = k$ and $\beta = d - \alpha$.

When $d = k$, $\alpha = k$ and $\beta = 0$. Only the k pixels $r_1, \ldots, r_k$ are selected. Since $r_k = s \oplus r_1 \oplus \cdots \oplus r_{k-1}$, the XOR-ed result of the d pixels is $o = o_\alpha = s$. The light transmissions are

$$T^{XOR,d}(o[s=0]) = 1$$

and

$$T^{XOR,d}(o[s=1]) = 0.$$

When $d > k, \alpha = k$ and $\beta > 0$. The k pixels $r_1, \ldots, r_k$ are chosen, and β pixels in $r_{k+1}, \ldots, r_n$ are selected. The XOR-ed result of the α pixels is $o_\alpha = s$. Hence, the XOR-ed result of the d pixels is $o = o_\alpha \oplus o_\beta = s \oplus o_\beta$. Since the β pixels are randomly generated, we get $Prob(o_\beta = 0) = Prob(o_\beta = 1) = \frac{1}{2}$ by Lemma 2. When $s = 0, o = s \oplus o_\beta = o_\beta$. $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$ is obtained. When $s = 1, o = s \oplus o_\beta = \overline{o_\beta}$. $Prob(o = 1) = Prob(o = 0) = \frac{1}{2}$ is achieved. As a result, $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$ no matter the secret pixel s is 0 or 1. The light transmissions are

$$T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}.$$

(2) $\alpha < k$ and $\beta = d - \alpha$.

When $d \geqslant k, \alpha > 0$ and $\beta > 0$. α pixels are selected from $r_1, \ldots, r_k$, and β pixels are selected from $r_{k+1}, \ldots, r_n$. Since $\alpha < k$, $Prob(o_\alpha = 0) = Prob(o_\alpha = 1) = \frac{1}{2}$ by Lemma 3, no matter the secret pixel s is 0 or 1. Since the β pixels are randomly generated, we have $Prob(o_\beta = 0) = Prob(o_\beta = 1) = \frac{1}{2}$ no matter the secret pixel s is 0 or 1. As a result, $Prob(o = 0) = Prob(o = 1) = \frac{1}{2}$ no matter the secret pixel s is 0 or 1. The light transmissions are

$$T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}.$$

When $d = k$, the probability of $\alpha = k$ and $\beta = d - \alpha$ is $\frac{1}{\binom{n}{k}}$, and the probability of $\alpha < k$ and $\beta = d - \alpha$ is $1 - \frac{1}{\binom{n}{k}}$. As a result, the light transmissions are

$$T^{XOR,d}(o[s=0]) = 1 \times \frac{1}{\binom{n}{k}} + \frac{1}{2} \times \left[1 - \frac{1}{\binom{n}{k}}\right] = \frac{1}{2}\left[1 + \frac{1}{\binom{n}{k}}\right]$$

and

$$T^{XOR,d}(o[s=1]) = 0 \times \frac{1}{\binom{n}{k}} + \frac{1}{2} \times \left[1 - \frac{1}{\binom{n}{k}}\right] = \frac{1}{2}\left[1 - \frac{1}{\binom{n}{k}}\right].$$

When $d > k$, the light transmissions are $\frac{1}{2}$ for both $\alpha = k,\ \beta = d - \alpha$ and $\alpha < k, \beta = d - \alpha$. As a result, $T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]) = \frac{1}{2}$.

In all, the light transmissions are

$$T^{XOR,d}(o[s=0]) = \begin{cases} \frac{1}{2}\left[1 + \frac{1}{\binom{n}{k}}\right], & \text{if } d = k, \\ \frac{1}{2}, & \text{if } d > k, \end{cases}$$

and

$$T^{XOR,d}(o[s=1]) = \begin{cases} \frac{1}{2}\left[1 - \frac{1}{\binom{n}{k}}\right], & \text{if } d = k, \\ \frac{1}{2}, & \text{if } d > k. \end{cases} \qquad \square$$

Lemma 5. *Let s be the secret pixel. n random grid pixels $r_1, \ldots, r_n$ are generated by Chen and Tsao's $(2, n)$ RG-based VSS. That is, $r_1, \ldots, r_n$ are generated randomly when $s = 1$, whereas, $r_1, \ldots, r_n$ are assigned the same value which is chosen from 0 or 1, when $s = 0$. Let $o = r_{i_1} \oplus \cdots \oplus r_{i_d}$ be the XOR-ed result of any d pixels, where $d \geqslant 2$. The light transmissions are*

$$T^{XOR,d}(o[s=0]) = \begin{cases} 1, & \text{if d is even} \\ \frac{1}{2}, & \text{otherwise} \end{cases}$$

and

$$T^{XOR,d}(o[s=1]) = \frac{1}{2}.$$

Proof. If $s = 0, r_1 = r_2 = \cdots = r_n = r$ where r is randomly assigned the value 0 or 1. When d is even, the XOR-ed result of any d pixels is 0. The light transmission is $T^{XOR,d}(o[s=0]) = 1$. When d is odd, the XOR-ed result of any d pixels is r. Since r is randomly generated, the light transmission is $T^{XOR,d}(o[s=0]) = \frac{1}{2}$.

If $s = 1, r_1, \ldots, r_n$ are randomly generated. The light transmission is $T^{XOR,d}(o[s=1]) = \frac{1}{2}$ by Lemma 2. $\square$

Lemma 6. *Given a secret pixel s and n shared pixels $r_1, \ldots, r_n$ generated by the proposed method, let o be the XOR-ed result of any d pixels from $r_1, \ldots, r_n$. When $s = 0$, the average light transmission of the XOR-ed result is*

$$T^{XOR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=0]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=0])\right],$$

where $T^{XOR,d}_{(k,n)}, \ldots, T^{XOR,d}_{(n,n)}$ are the average light transmissions of the XOR-ed results by d pixels in the $(k,n), \ldots, (n,n)$ threshold RG-based VSS schemes [14,15]. When $s = 1$, the average light transmission of the XOR-ed result is

$$T^{XOR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=1]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=1])\right].$$

Proof. In the proposed method, the n pixels are generated by one of the $n - k + 1$ RG-based VSS schemes such as (k, n), $(k+1, n), \ldots, (n, n)$. When the n pixels are generated by a specific (t, n) RG-based VSS, where $k \leqslant t \leqslant n$, the average light transmissions are $T^{XOR,d}_{(t,n)}(o[s=0])$ and $T^{XOR,d}_{(t,n)}(o[s=1])$. The probability for the (t, n) RG-based VSS being chosen is $\frac{1}{n-k+1}$. Hence, the average light transmissions of the XOR-ed result are

$$T^{XOR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=0]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=0])\right]$$

and

$$T^{XOR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=1]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=1])\right]. \qquad \square$$

Theorem 2. *Given a secret image S and n shares $R_1, \ldots, R_n$ generated by the proposed method, let O be the XOR-ed result of any d shares from $R_1, \ldots, R_n$. The proposed method is a valid construction of the (k, n) threshold RG-based VSS when XOR-ed decryption is applied, which satisfies the following three conditions.*

- *Each share is a RG, as denoted by*

  $$T^{XOR,1}(R_i[S(0)]) = T^{XOR,1}(R_i[S(1)]), \quad 1 \leqslant i \leqslant n.$$

- *When $d < k$, the XOR-ed result gives no clue about the secret, as represented by*

  $$T^{XOR,d}(O[S(0)]) = T^{XOR,d}(O[S(1)]).$$

- *When $d \geqslant k$, the XOR-ed result reveals the secret, as represented by*

  $$T^{XOR,d}(O[S(0)]) > T^{XOR,d}(O[S(1)]).$$

Proof. Given a secret pixel s and n shared pixels $r_1, \ldots, r_n$ generated by the proposed method, let o be the XOR-ed result of any d pixels from $r_1, \ldots, r_n$. According to Lemma 6, we have

$$T^{XOR,d}(o[s=0]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=0]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=0])\right]$$

and

$$T^{XOR,d}(o[s=1]) = \frac{1}{(n-k+1)}\left[T^{XOR,d}_{(k,n)}(o[s=1]) + \cdots + T^{XOR,d}_{(n,n)}(o[s=1])\right].$$

When $d = 1$, the first condition reduces to the first condition of Theorem 1. According to Theorem 1, the first condition is met.

When $k = 2$, the first condition guarantees that the XOR-ed result of any $d < k$ shares gives no clue about the secret.

When $k > 2$, if $d < k$, the light transmissions of the XOR-ed results by any d pixels for the $(k,n),\ldots,(n,n)$ cases satisfy

$$T^{XOR,d}_{(k,n)}(o[s=0]) = T^{XOR,d}_{(k,n)}(o[s=1]),\ldots,T^{XOR,d}_{(n,n)}(o[s=0]) = T^{XOR,d}_{(n,n)}(o[s=1])$$

according to Lemma 3. Hence, we achieve

$$T^{XOR,d}(o[s=0]) = T^{XOR,d}(o[s=1]).$$

Based on Definition 1, $T^{XOR,d}(O[S(0)]) = T^{XOR,d}(O[S(1)])$. The second condition is satisfied.

When $k = 2$, if $d = 2$, the light transmissions of the XOR-ed results by any d pixels for the $(2,n)$ case satisfy

$$T^{XOR,d}_{(2,n)}(o[s=0]) > T^{XOR,d}_{(k,n)}(o[s=1])$$

by Lemma 5. The light transmissions of the XOR-ed results by any d pixels for the $(3,n),\ldots,(n,n)$ cases satisfy

$$T^{XOR,d}_{(3,n)}(o[s=0]) = T^{XOR,d}_{(3,n)}(o[s=1]),\ldots,T^{XOR,d}_{(n,n)}(o[s=0]) = T^{XOR,d}_{(n,n)}(o[s=1])$$

according to Lemma 3. As a result, we have

$$T^{XOR,d}(o[s=0]) > T^{XOR,d}(o[s=1]).$$

Based on Definition 1, $T^{XOR,d}(O[S(0)]) > T^{XOR,d}(O[S(1)])$.

When $k = 2$, if $d > 2$, the light transmissions of the XOR-ed results by any d pixels for the $(2,n)$ case satisfy

$$T^{XOR,d}_{(2,n)}(o[s=0]) \geqslant T^{XOR,d}_{(k,n)}(o[s=1])$$

by Lemma 5. The light transmissions of the XOR-ed results by any d pixels for the $(3,n),\ldots,(d-1,n),(d,n),(d+1,n),\ldots,(n,n)$ cases satisfy

$$\begin{aligned}
&T^{XOR,d}_{(3,n)}(o[s=0]) = T^{XOR,d}_{(3,n)}(o[s=1]),\\
&\ldots\\
&T^{XOR,d}_{(d-1,n)}(o[s=0]) = T^{XOR,d}_{(d-1,n)}(o[s=1]),\\
&T^{XOR,d}_{(d,n)}(o[s=0]) > T^{XOR,d}_{(d,n)}(o[s=1]),\\
&T^{XOR,d}_{(d+1,n)}(o[s=0]) = T^{XOR,d}_{(d+1,n)}(o[s=1]),\\
&\ldots\\
&T^{XOR,d}_{(n,n)}(o[s=0]) = T^{XOR,d}_{(n,n)}(o[s=1]),
\end{aligned}$$

according to Lemma 4. Therefore, we have

$$T^{XOR,d}(o[s=0]) > T^{XOR,d}(o[s=1]).$$

Based on Definition 1, $T^{XOR,d}(O[S(0)]) > T^{XOR,d}(O[S(1)])$.

When $k > 2$, if $d > k$, the light transmissions of the XOR-ed results by any d pixels for the $(k,n),\ldots,(d-1,n),(d,n),(d+1,n),\ldots,(n,n)$ cases satisfy

$$\begin{aligned}
&T^{XOR,d}_{(k,n)}(o[s=0]) = T^{XOR,d}_{(k,n)}(o[s=1]),\\
&\ldots\\
&T^{XOR,d}_{(d-1,n)}(o[s=0]) = T^{XOR,d}_{(d-1,n)}(o[s=1]),\\
&T^{XOR,d}_{(d,n)}(o[s=0]) > T^{XOR,d}_{(d,n)}(o[s=1]),\\
&T^{XOR,d}_{(d+1,n)}(o[s=0]) = T^{XOR,d}_{(d+1,n)}(o[s=1]),\\
&\ldots\\
&T^{XOR,d}_{(n,n)}(o[s=0]) = T^{XOR,d}_{(n,n)}(o[s=1]),
\end{aligned}$$

according to Lemma 4. As a result, we get

$$T^{XOR,d}(o[s=0]) > T^{XOR,d}(o[s=1]).$$

Based on Definition 1, $T^{XOR,d}(O[S(0)]) > T^{XOR,d}(O[S(1)])$. Finally, the third condition is satisfied.

In general, the proposed method is a valid construction of the (k,n) threshold RG-based VSS when XOR decryption is applied. □

Based on Theorems 1 and 2, the proposed scheme is a valid construction of RG-based VSS for both the stacking and XOR decryptions.

3.1. Extension for grayscale/color images

The proposed method can be further extended to share grayscale/color images. For sharing the grayscale images, halftoning methods such as order dithering, error diffusion and dot diffusion are applied to the gray-level image for converting it into binary. Then, the proposed scheme is adopted to construct shares.

To share the color images, techniques including color decomposition, halftone technique and color composition are utilized. The constitution of colors can be described by color model. Totally, two types of color models are used: (1) additive color model, which displays a color by mixing with different colors of light, such as RGB (red–green–blue) model; (2) subtractive color model, which illustrates a color by reflecting light from a surface of an object, such as CMY (cyan–magenta–yellow) model. Since the secret image can be visually decrypted by stacking, the CMY model is utilized in this work. Overall, four steps are conducted to share the color secret image. Firstly, the secret image is decomposed by the CMY model into the C,M,Y images. Secondly, the C, M, Y images are converted into binary images by using the halftoning technique. Thirdly, each converted binary image is processed by the proposed method, and some RGs are constructed. Finally, those corresponding RGs are composed by the CMY color model to form color RGs.

For the stacking decryption, the shares are stacked together directly. For the XOR decryption, the shares are decomposed into the C, M, Y image. Then, the C image of the secret is reconstructed by conducting the XOR operation on the associated C images from the shares. Similarly, the M and Y images of the secret can be reconstructed. Finally, the C, M, Y images are composed and the secret image is reconstructed.

4. Simulation results and discussion

4.1. Three cases by the proposed scheme

Three experiments are shown in the illustrations to demonstrate the feasibility of the proposed scheme. The secret images used in this section are of size 1000 × 1000. The first experiment is a $(2,4)$ case by the proposed method. The secret image and four generated shares are illustrated in Fig. 2. The stacked (OR-ed) results by different combinations of the four shares are shown in Fig. 3. Meanwhile, the XOR-ed results by different combinations of the four shares are demonstrated in Fig. 4. The two types of decryptions exhibit that the proposed scheme is a valid construction of RG-based VSS for OR and XOR decryptions. Furthermore, better visual quality of decrypted secret image is obtained by XOR decryption.

Another experiment is a $(3,4)$ case by the proposed method. The secret image and four generated shares are shown in Fig. 5. The stacked results and XOR-ed results of different combinations of the four shares are illustrated in Figs. 6 and 8, respectively. Note that, visual quality of the decrypted secret image by XOR operation is better than that by OR operation.

Example of a $(2,3)$ case by the proposed method for sharing color images is demonstrated in Fig. 7. The color secret image is

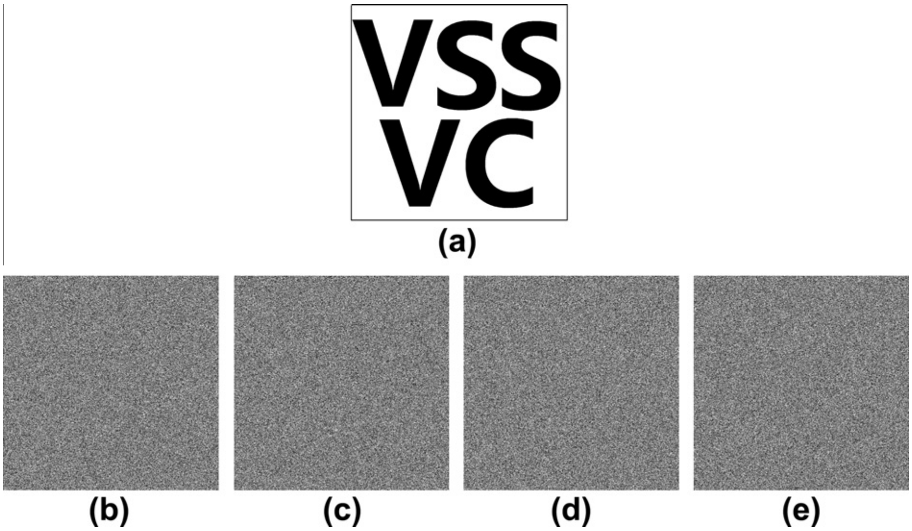

Fig. 2. Secret image and four shares of a (2,4) case by the proposed scheme. (a) Secret image, (b)–(e) four generated shares: R_1, R_2, R_3 and R_4.

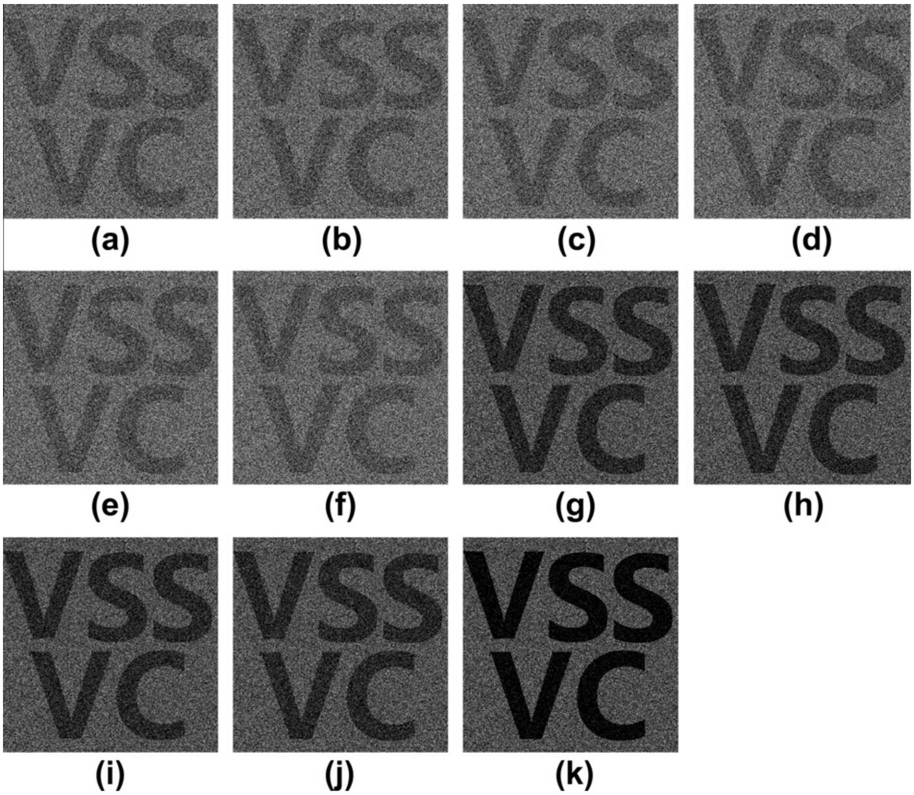

Fig. 3. Stacked results of different combinations of the four shares generated in the (2,4) case by the proposed scheme. (a) $R_1 \otimes R_2$, (b) $R_1 \otimes R_3$, (c) $R_1 \otimes R_4$, (d) $R_2 \otimes R_3$, (e) $R_2 \otimes R_4$, (f) $R_3 \otimes R_4$, (g) $R_1 \otimes R_2 \otimes R_3$, (h) $R_1 \otimes R_2 \otimes R_4$, (i) $R_1 \otimes R_3 \otimes R_4$, (j) $R_2 \otimes R_3 \otimes R_4$, and (k) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

shown in Fig. 7 and the three generated shares are illustrated in Figs. 7(b)–(d). Stacked results by different combinations of three shares are shown in Figs. 7(e)–(h). When the XOR decryption is utilized, the secret images can be reconstructed as well, as demonstrated in Figs. 7(i)–(l). According to Fig. 7, the proposed method can be adopted to share grayscale/color images.

4.2. Security analysis

The security constraint, which is verified based on the visual recognition described in Definition 4, does not take into account the joint multidimensional distribution of neighboring pixels, since certain distribution of neighboring pixels could be exploited to have an estimate of the secret image.

To further evaluate the security of the proposed method, the correlation test is adopted, where such a test has been widely used in secret image sharing [20,21] and image encryption [22–24]. In essence, the correlation test is used to show the confusion and diffusion properties of the proposed scheme. Four kinds of correlations in the original secret image, shares, stacked shares and XOR-ed shares are calculated. They are correlations between two horizontally adjacent pixels, two vertically adjacent pixels, two

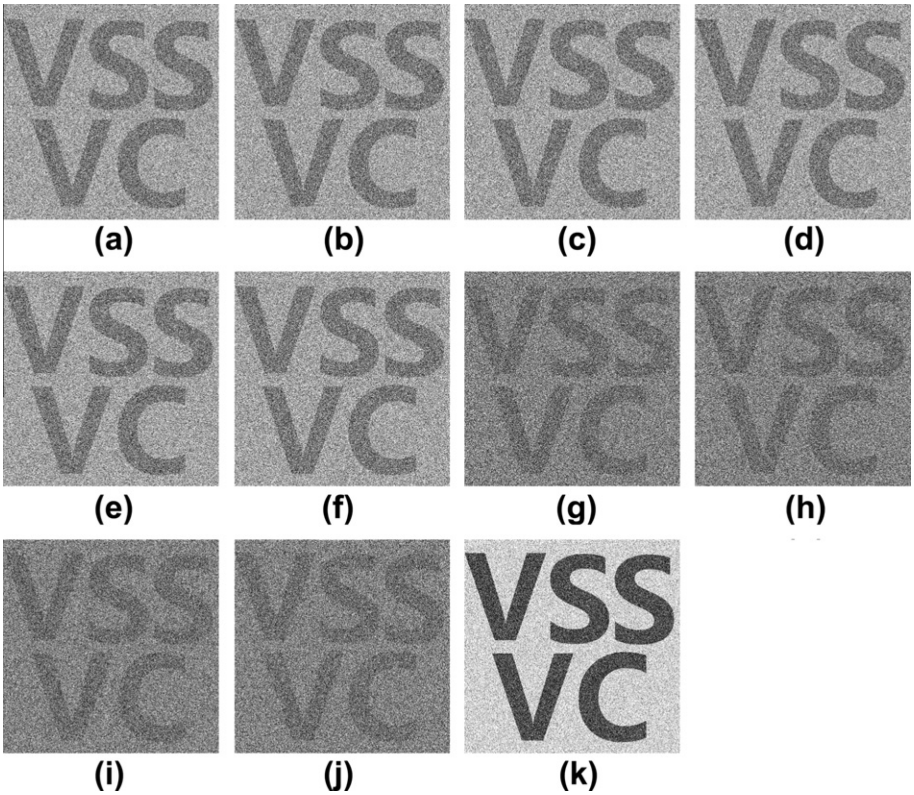

Fig. 4. XOR results of different combinations of the four shares generated in the (2,4) case by the proposed scheme. (a) $R_1 \oplus R_2$, (b) $R_1 \oplus R_3$, (c) $R_1 \oplus R_4$, (d) $R_2 \oplus R_3$, (e) $R_2 \oplus R_4$, (f) $R_3 \oplus R_4$, (g) $R_1 \oplus R_2 \oplus R_3$, (h) $R_1 \oplus R_2 \oplus R_4$, (i) $R_1 \oplus R_3 \oplus R_4$, (j) $R_2 \oplus R_3 \oplus R_4$, and (k) $R_1 \oplus R_2 \oplus R_3 \oplus R_4$.

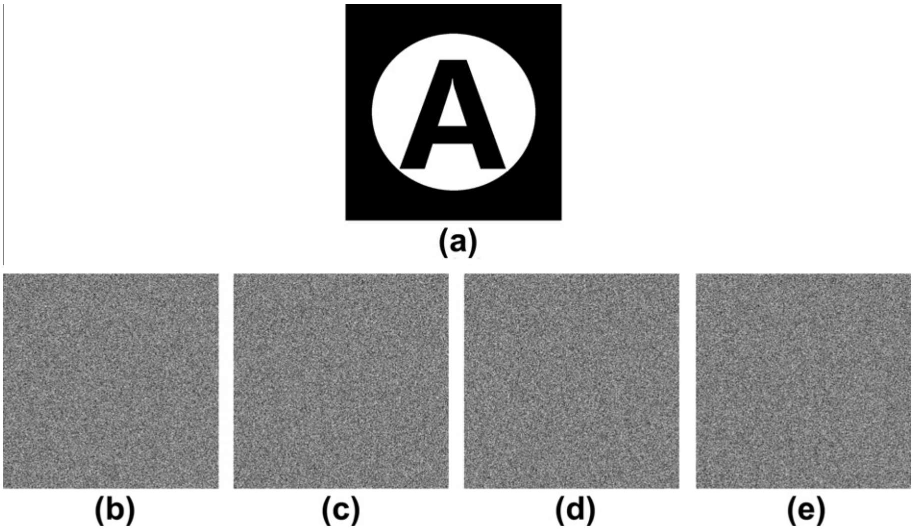

Fig. 5. Secret image and four shares of a (3,4) case by the proposed scheme. (a) Secret image, (b)–(e) four generated shares: R_1, R_2, R_3 and R_4.

diagonal adjacent pixels and two vice-diagonal adjacent pixels, respectively. The correlation coefficient of each pair pixels is calculated by

$$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

where x and y are the values of two adjacent pixels in an image. $cov(x,y), D(x)$ are defined as follows:

$$cov(x,y) = \frac{1}{m \times n}\sum_{i=1}^{m\times n}(x_i - E(x))(y_i - E(y)),$$

$$D(x) = \frac{1}{m \times n}\sum_{i=1}^{m\times n}(x_i - E(x))^2, E(x) = \frac{1}{m \times n}\sum_{i=1}^{m\times n}x_i.$$

In the correlation test, 10,000 pairs of two horizontally adjacent pixels, 10,000 pairs of two vertically adjacent pixels, 10,000 pairs of two diagonal adjacent pixels and 10,000 pairs of two vice-diagonal

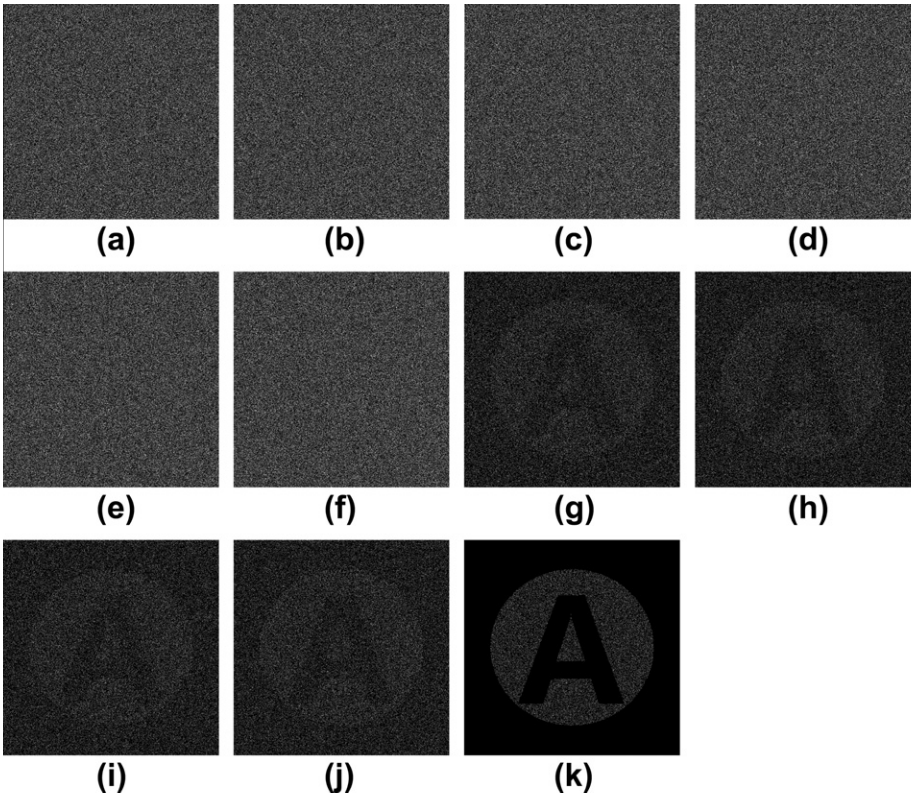

Fig. 6. Stacked results of different combinations of the four shares generated in the (3,4) case by the proposed scheme. (a) $R_1 \otimes R_2$, (b) $R_1 \otimes R_3$, (c) $R_1 \otimes R_4$, (d) $R_2 \otimes R_3$, (e) $R_2 \otimes R_4$, (f) $R_3 \otimes R_4$, (g) $R_1 \otimes R_2 \otimes R_3$, (h) $R_1 \otimes R_2 \otimes R_4$, (i) $R_1 \otimes R_3 \otimes R_4$, (j) $R_2 \otimes R_3 \otimes R_4$, and (k) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

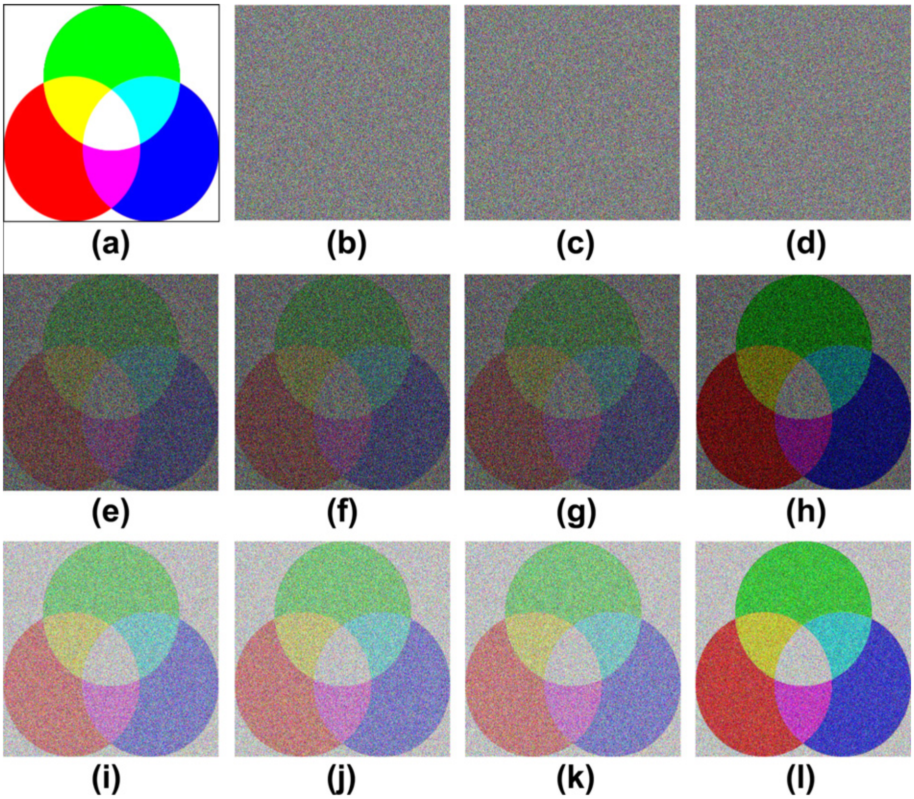

Fig. 7. Experiment of a (2,3) case by the proposed method for sharing color images. (a) color secret image, (b) $R_1 \otimes R_2$, (c) $R_1 \otimes R_3$, (d) $R_2 \otimes R_3$, (e) $R_1 \otimes R_2 \otimes R_3$, (f) $R_1 \oplus R_2$, (g) $R_1 \oplus R_3$, (h) $R_2 \oplus R_3$, and (i) $R_1 \oplus R_2 \oplus R_3$. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

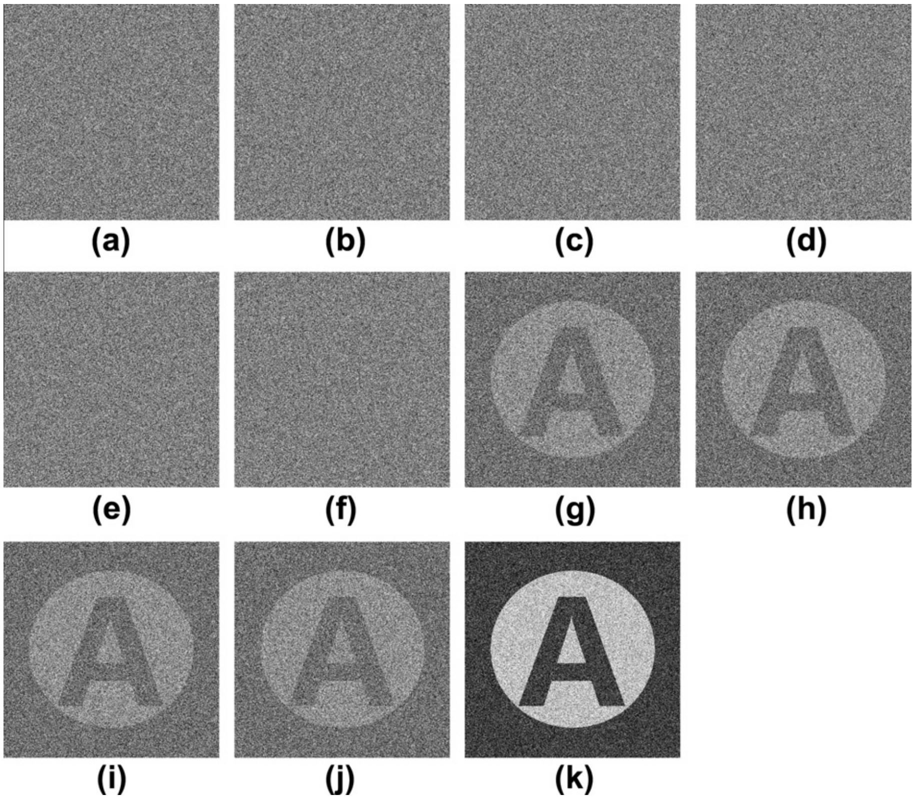

Fig. 8. XOR results of different combinations of the four shares generated in the (3,4) case by the proposed scheme. (a) $R_1 \oplus R_2$, (b) $R_1 \oplus R_3$, (c) $R_1 \oplus R_4$, (d) $R_2 \oplus R_3$, (e) $R_2 \oplus R_4$, (f) $R_3 \oplus R_4$, (g) $R_1 \oplus R_2 \oplus R_3$, (h) $R_1 \oplus R_2 \oplus R_4$, (i) $R_1 \oplus R_3 \oplus R_4$, (j) $R_2 \oplus R_3 \oplus R_4$, and (k) $R_1 \oplus R_2 \oplus R_3 \oplus R_4$.

adjacent pixels are randomly selected in the test image. For the (2,4) case experiment, the four kinds of correlation coefficients are listed in Table 1. Correlations of the original secret image are rather different from the correlations of the shares. The correlation coefficients of the shares are only slight positive or negative. Pixels in the shares are in weak correlations. As a result, the appearance of the generated shares is noise-like and they cannot reveal the secret image. Moreover, correlation coefficients of the original secret image, shares, stacked shares, XOR-ed shares in the (3,4) experiment are illustrated in Table 2. Pixels in the shares, stacked shares and XOR-ed shares are in weak correlations. The secret image cannot be disclosed by insufficient shares.

4.3. Pixel expansion and contrast

Table 3 shows the comparisons of pixel expansion among the proposed method and related schemes [7,13–15]. Note that, Tuyls et al.'s method [7] is a XOR-based VSS which introduces several approaches. Different approaches lead to different pixel expansions. Herein, the minimal pixel expansions for different thresholds are employed for comparisons. Further, schemes such as [13–15] are the RG-based VSS schemes for different thresholds. As illustrated in Table 3, the pixel expansion problem is solved by RG-based VSS schemes including the proposed method. Whereas, the pixel expansion problem remains in Tuyls et al.'s method [7]. The pixel expansion problem becomes more serious when k and n $(k \neq n)$ become bigger.

Table 1
Correlation coefficients of neighboring pixels for the original secret image and shares in the (2,4) experiment.

Images	Correlation coefficients			
	Horizontal	Vertical	Diagonal	Vice-diagonal
Secret	0.9904	0.9918	0.9863	0.9822
R_1	0.0120	0.0089	0.0020	−0.0124
R_2	0.0031	0.0033	0.0128	−0.0024
R_3	0.0072	−0.0186	−0.0092	−0.0074
R_4	0.0025	−0.0033	0.0092	0.0040

Table 2
Correlation coefficients of neighboring pixels for the original secret image, shares, stacked shares and XOR-ed shares in the (3,4) experiment.

Images	Correlation coefficients			
	Horizontal	Vertical	Diagonal	Vice-diagonal
Secret	0.9939	0.9957	0.9907	0.9927
R_1	−0.0088	0.0178	−0.0023	−0.0035
R_2	−0.0026	0.0032	0.0168	0.0224
R_3	0.0120	−0.0110	0.0094	−0.0010
R_4	−0.0012	−0.0040	−0.0043	−0.0098
$R_1 \otimes R_2$	−0.0068	−0.0085	−0.0106	−0.0063
$R_1 \otimes R_3$	0.0176	−0.0155	0.0147	0.0140
$R_1 \otimes R_4$	−0.0036	−0.0092	0.0094	−0.0019
$R_2 \otimes R_3$	−0.0048	0.0022	0.0018	−0.0017
$R_2 \otimes R_4$	−0.0004	0.0104	−0.0012	0.0009
$R_3 \otimes R_4$	−0.0142	0.0065	−0.0090	0.0052
$R_1 \oplus R_2$	−0.0110	0.0070	−0.0101	−0.0117
$R_1 \oplus R_3$	0.0033	−0.0034	−0.0037	−0.0132
$R_1 \oplus R_4$	−0.0157	0.0147	−0.0139	−0.0131
$R_2 \oplus R_3$	0.0006	0.0118	−0.0002	0.0095
$R_2 \oplus R_4$	−0.0053	−0.0035	−0.0140	0.0013
$R_3 \oplus R_4$	0.0058	0.0120	0.0051	-0.0032

Extensive experiments are conducted to evaluate the visual quality of the proposed method. Comparisons of recovered secret image quality for the (2,4) case between the proposed method and Chen and Tsao's (k,n) method [15] are shown in Fig. 9. The visual quality of recovered secret image by the proposed scheme is approximately the same as that of Chen and Tsao's (k,n) method

Table 3
Comparisons of pixel expansion among the proposed scheme and related methods [7,13–15].

Thresholds	Pixel expansion				
	Ref. [7]	Ref. [13]	Ref. [14]	Ref. [15]	Our
(n,n)	1	1	1	1	1
$(2,3)$	2	–	1	1	1
$(2,4)$	2	–	1	1	1
$(3,4)$	6	–	–	1	1
$(3,5)$	8	–	–	1	1
$(4,5)$	15	–	–	1	1

[15], when stacking decryption is applied. Better visual quality is provided by the proposed method when XOR decryption is utilized. The background by XOR decryption is not as dark as that by stacking decryption.

For the $(3,4)$ case, Fig. 10 shows the comparisons of recovered secret image quality between the proposed method and Chen and Tsao's (k,n) method [15]. Better recovered secret image quality is obtained by the proposed method, when XOR operation is adopted. Meanwhile, the visual quality of decrypted secret image of the proposed scheme by stacking decryption is nearly the same as that by Chen and Tsao's (k,n) method [15].

To quantitatively evaluate the visual quality of recovered secret image, the contrast is adopted, as defined in Definition 3. The formal definition of contrast is for the OR decryption, the contrast by XOR operation can be calculated by the same approach. Further, some related VSS schemes [7,13–15] are employed for contrast comparisons as well. Note that, Tuyls et al.'s work [7] introduced several constructions for XOR-based VSS. The contrast of the recovered secret image is calculated when minimal pixel expansion is used.

Table 4 shows the comparisons of contrast among the proposed method and four related schemes [7,13–15]. For the (n,n) case, the proposed method and three other schemes [13–15] reduce to a same VSS model, where the four schemes can be decrypted by both stacking and XOR operations. For this special case, the contrast by stacking decryption of the four schemes is $\frac{1}{2^{n-1}}$ and the contrast by XOR decryption is 1.

Comparisons of contrast for the $(2,3)$ and $(2,4)$ cases among the proposed scheme and related schemes [7,14,15] are provided in Tables 5 and 6, respectively. For the $(2,3)$ case, when two shares are stacked, the contrast by the proposed method is $\frac{1}{10}$ which is less than Chen and Tsao's $(2,n)$ method [14] and Chen and Tsao's (k,n) method [15] by $\frac{1}{10}$ and $\frac{3}{70}$, respectively. When the secret image is reconstructed from two shares by XOR operation, the contrasts of the proposed method and Tuyls et al.'s method [7] are $\frac{1}{6}$ and $\frac{1}{3}$, respectively. When three shares are stacked, the contrast of the proposed method is bigger than Chen and Tsao's (k,n) scheme [15] and is approximately the same as Chen and Tsao's $(2,n)$ scheme [14]. When the secret image is recovered by XOR operation, the largest contrast, which is $\frac{2}{5}$, is obtained by the proposed method among the four approaches.

For the $(2,4)$ case, the contrast of the proposed method by two XOR-ed shares, which is $\frac{1}{6}$, is larger than that of Chen and Tsao's (k,n) method [15] and is smaller than those in [7,14]. When three shares are stacked or XOR-ed, smaller contrasts are provided by the proposed method. Whereas, better visual quality is achieved by the proposed method when four shares are stacked or XOR-ed. The contrasts by stacking and XOR decryptions of the proposed approach are larger than those of Chen and Tsao's (k,n) method [15] by $\frac{39}{392}$ and $\frac{1}{4}$, respectively.

Extensive comparisons of contrast among the proposed method and related methods [7,15] are demonstrated in Tables 7–9. For the

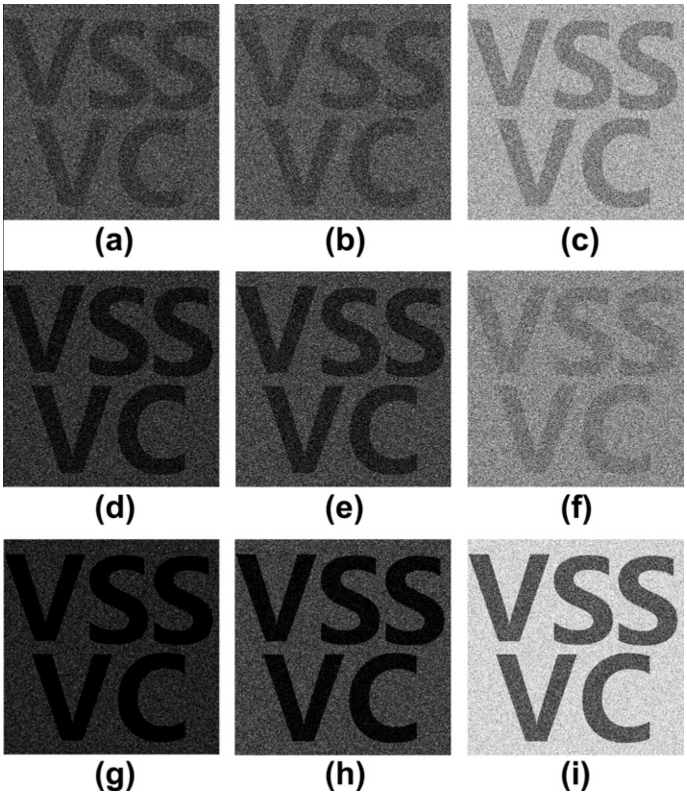

Fig. 9. Comparisons of visual quality of the recovered secret images for the $(2,4)$ case between the proposed method and Chen and Tsao's method [15]. (a), (d), (g) Three secret images reconstructed by stacking two, three, four shares of Chen and Tsao's method, respectively, (b), (e), (h) three secret images reconstructed by stacking two, three, four shares of the proposed method, respectively, (c), (f), (i) three secret images reconstructed by conducting XOR operation on two, three, four shares of the proposed method, respectively.

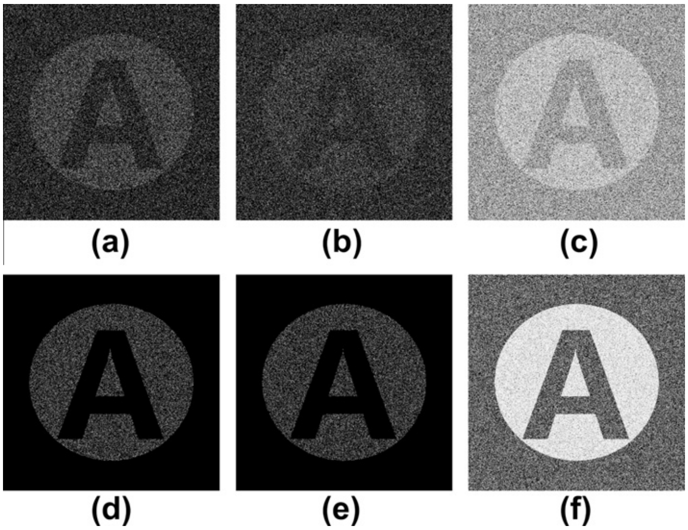

Fig. 10. Comparisons of visual quality of the recovered secret images for the (3,4) case between the proposed method and Chen and Tsao's method [15]. (a), (d) Two secret images reconstructed by stacking three and four shares of Chen and Tsao's method, respectively, (b), (e) two secret images reconstructed by stacking three and four shares of the proposed method, respectively, (c), (f) two secret images reconstructed by conducting XOR operation on three and four shares of the proposed method, respectively.

Table 4
Comparisons of contrast for the (n,n) case among the proposed scheme and related methods [7,13–15].

Schemes	Contrast	
	Stacking	XOR
Ref. [7]	–	1
Ref. [13]	$\frac{1}{2^{n-1}}$	1
Ref. [14]	$\frac{1}{2^{n-1}}$	1
Ref. [15]	$\frac{1}{2^{n-1}}$	1
Our	$\frac{1}{2^{n-1}}$	1

Table 5
Comparisons of contrast for the (2,3) case among the proposed scheme and related methods [7,14,15], where t is the number of shares.

Schemes	t	Contrast	
		Stacking	XOR
Ref. [7]	2	–	$\frac{1}{3}$
Ref. [14]		$\frac{1}{5}$	–
Ref. [15]		$\frac{1}{7}$	–
Our		$\frac{1}{10}$	$\frac{1}{6}$
Ref. [7]	3	–	$\frac{1}{3}$
Ref. [14]		$\frac{3}{10}$	–
Ref. [15]		$\frac{1}{4}$	–
Our		$\frac{5}{17}$	$\frac{2}{5}$

Table 6
Comparisons of contrast for the (2,4) case among the proposed scheme and related methods [7,14,15], where t is the number of shares.

Schemes	t	Contrast	
		Stacking	XOR
Ref. [7]	2	–	$\frac{1}{3}$
Ref. [14]		$\frac{1}{5}$	–
Ref. [15]		$\frac{2}{29}$	–
Our		$\frac{1}{15}$	$\frac{1}{9}$
Ref. [7]	3	–	$\frac{1}{3}$
Ref. [14]		$\frac{3}{10}$	–
Ref. [15]		$\frac{6}{51}$	–
Our		$\frac{14}{107}$	$\frac{2}{57}$
Ref. [7]	4	–	$\frac{1}{3}$
Ref. [14]		$\frac{7}{17}$	–
Ref. [15]		$\frac{1}{8}$	–
Our		$\frac{11}{49}$	$\frac{3}{8}$

Table 7
Comparisons of contrast for the (3,4) case among the proposed scheme and related methods [7,15], where t is the number of shares.

Schemes	t	Contrast	
		Stacking	XOR
Ref. [7]	3	-	$\frac{4}{7}$
Ref. [15]		$\frac{2}{35}$	–
Our		$\frac{2}{71}$	$\frac{2}{23}$
Ref. [7]	4	-	$\frac{4}{7}$
Ref. [15]		$\frac{1}{8}$	–
Our		$\frac{1}{8}$	$\frac{2}{5}$

(3,4) case, best visual quality is achieved by Tuyls et al.'s method [7]. The contrasts of the proposed method by the XOR decryption are larger than those of Chen and Tsao's (k,n) method [15].

For the (3,5) case, the contrast of the proposed method by three XOR-ed shares is nearly the same as that of Chen and Tsao's (k,n) method [15] by three stacked shares. The contrasts of the proposed method by four stacked shares and by four XOR-ed shares are smaller than those of [7,15]. But better visual quality is achieved by the proposed method when five shares are stacked or XOR-ed, where the contrasts by five XOR-ed shares is bigger than that in [15] by $\frac{3}{16}$. For the (4,5) case, larger contrast is obtained by the proposed scheme via XOR decryption, while comparing to Chen and Tsao's (k,n) method [15]. But contrasts of four stacked shares and four XOR-ed shares are small.

Overall, largest contrast is provided by Tuyls et al.'s method [7] but pixel expansion problem still exists in their method. The proposed method obtains larger contrast via XOR decryption in average, while comparing to Chen and Tsao's (k,n) method [15]. Further, some contrasts of the proposed method by stacking

Table 8
Comparisons of contrast for the (3,5) case among the proposed scheme and related methods [7,15], where t is the number of shares.

Schemes	t	Contrast	
		Stacking	XOR
Ref. [7]	3	–	$\frac{2}{5}$
Ref. [15]		$\frac{1}{44}$	–
Our		$\frac{2}{269}$	$\frac{2}{89}$
Ref. [7]	4	–	$\frac{2}{5}$
Ref. [15]		$\frac{4}{83}$	–
Our		$\frac{3}{126}$	$\frac{1}{27}$
Ref. [7]	5	–	$\frac{2}{5}$
Ref. [15]		$\frac{1}{16}$	-
Our		$\frac{1}{16}$	$\frac{1}{4}$

Table 9
Comparisons of contrast for the (4,5) case among the proposed scheme and related methods [7,15], where t is the number of shares.

Schemes	t	Contrast	
		Stacking	XOR
Ref. [7]	4	–	$\frac{4}{9}$
Ref. [15]		$\frac{2}{43}$	–
Our		$\frac{2}{169}$	$\frac{1}{29}$
Ref. [7]	5	–	$\frac{4}{9}$
Ref. [15]		$\frac{1}{16}$	–
Our		$\frac{1}{16}$	$\frac{2}{5}$

decryption are nearly same as those of [15], such as the contrasts of two stacked shares in (2,4), four stacked shares in (3,4), five stacked shares in (3,5) and (4,5). Some contrasts of the proposed method by stacking decryption are larger than those of [15] such as contrasts of three stacked shares in (2,3) and four stacked shares in (2,4).

4.4. More comparisons

It is desired to calculate the computational complexity of the proposed method when different decryptions are applied. When the stacking decryption is used, no computation is conducted since the decryption is completely based on human eyes. Hence, the computational complexity is $O(1)$. When the XOR decryption is adopted, the computation complexity is proportional to the number of XOR-ed shares. Let t be the number of shares, the computational complexity is $O(t)$. Table 10 summaries the comparisons of computational complexity for the decryption among the proposed scheme and related methods [7,13–15].

Further, feature comparisons among the proposed method and related VSS schemes are demonstrated in Table 11. The proposed method not only maintains the advantages of RG-based VSS such as no pixel expansion and no code book required, but also obtains the abilities of stacking and XOR decryptions.

Table 10
Comparisons of computational complexity for the decryption among the proposed scheme and related methods [7,13–15], where t is the number of shares.

Schemes	Computational complexity	
	Stacking	XOR
Ref. [7]	–	$O(t)$
Ref. [13]	$O(1)$	–
Ref. [14]	$O(1)$	–
Ref. [15]	$O(1)$	–
Our	$O(1)$	$O(t)$

Table 11
Feature comparisons among the proposed scheme and related VSS methods.

Schemes	Features				
	Pixel expansion	Code book needed	Type of VSS	Stacking decryption	XOR decryption
Ref. [3]	Yes	Yes	(k,n)	Yes	No
Ref. [11]	No	No	(2,2)	Yes	Yes
Ref. [12]	No	No	(2,2)	Yes	Yes
Ref. [13]	No	No	(n,n)	Yes	Yes
Ref. [14]	No	No	$(2,n),(n,n)$	Yes	No
Ref. [15]	No	No	(k,n)	Yes	No
The proposed method	No	No	(k,n)	Yes	Yes

Note that, when $k = n$, the proposed scheme reduces to Shyu's (n,n) RG-based VSS [13]. Due to the share construction in Shyu's method [13] is based on XOR operation, the secret image can be perfectly reconstructed when XOR operation is used. But Shyu's method is only designed for the (n,n) threshold, more sharing strategies such as $(2,n)$ and (k,n) cannot be implemented. However, the proposed method addresses the above problem by providing general construction for the (k,n) threshold.

5. Conclusions

This paper introduces a (k,n) RG-based VSS with abilities of stacking and XOR decryptions. When computational devices are not available, the secret image can be decrypted by stacking operation. Whereas, the secret image can be recovered by XOR operation as well when light-weight computational devices are used. Some deficiencies existed in RG-based VSS and XOR-based VSS can be solved by the proposed method. Also, the proposed VSS is verified to be a valid construction of (k,n) VSS theoretically and experimentally. Some advantages such as no code book required and no pixel expansion are maintained in the proposed method. Further, the contrasts by using stacking decryption and XOR decryption are calculated and compared to related VSS schemes. According to the comparisons, larger contrast is obtained by the proposed method when XOR decryption is applied.

Acknowledgments

This work was partially supported by Science and Technology Development Fund of Macao Special Administrative Region under Contract 006/2001/A1 and innovative talent training program of Sun Yat-sen University. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612–613.
[2] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, vol. 88, 1979, p. 317.
[3] M. Naor, A. Shamir, Visual cryptography, Lecture Notes in Computer Science 950 (1995) 1–12.
[4] C. Blundo, A. De Santis, Visual cryptography schemes with perfect reconstruction of black pixels, Computers & Graphics 22 (1998) 449–455.
[5] H. Koga, E. Ueda, Basic properties of the (t,n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels, Designs, Codes and Cryptography 40 (2006) 81–102.
[6] D. Wang, L. Zhang, N. Ma, X. Li, Two secret sharing schemes based on Boolean operations, Pattern Recognition 40 (2007) 2776–2785.
[7] P. Tuyls, H. Hollmann, J. Lint, L. Tolhuizen, Xor-based visual cryptography schemes, Designs, Codes and Cryptography 37 (2005) 169–186.
[8] R. Ito, H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 82 (1999) 2172–2177.

[9] C. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters 25 (2004) 486–494.

[10] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, The Computer Journal 49 (2006) 97–107.

[11] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Optics Letters 12 (1987) 377–379.

[12] S. Shyu, Image encryption by random grids, Pattern Recognition 40 (2007) 1014–1031.

[13] S. Shyu, Image encryption by multiple random grids, Pattern Recognition 42 (2009) 1582–1596.

[14] T. Chen, K. Tsao, Visual secret sharing by random grids revisited, Pattern Recognition 42 (2009) 2203–2217.

[15] T. Chen, K. Tsao, Threshold visual secret sharing by random grids, Journal of Systems and Software 84 (2011) 1197–1208.

[16] T. Chen, K. Tsao, User-friendly random-grid-based visual secret sharing, IEEE Transactions on Circuits and Systems for Video Technology 21 (2011) 1693–1703.

[17] S. Chen, S. Lin, Optimal $(2,n)$ and $(2,\infty)$ visual secret sharing by generalized random grids, Journal of Visual Communication and Image Representation 23 (2012) 677–684.

[18] R. Wang, Y. Lan, Y. Lee, S. Huang, S. Shyu, T. Chia, Incrementing visual cryptography using random grids, Optics Communications 283 (2010) 4242–4249.

[19] G. Ateniese, C. Blundo, A. De Santis, D. Stinson, Visual cryptography for general access structures, Information and Computation 129 (1996) 86–106.

[20] G. Alvarez, L. Hernández Encinas, A. Martín del Rey, A multisecret sharing scheme for color images based on cellular automata, Information Sciences 178 (2008) 4382–4395.

[21] C. Chang, C. Lin, C. Lin, Y. Chen, A novel secret image sharing scheme in color images using small shadow images, Information Sciences 178 (2008) 2433–2447.

[22] L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps, Chaos, Solitons & Fractals 24 (2005) 759–765.

[23] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons & Fractals 35 (2008) 408–419.

[24] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Processing 90 (2010) 2714–2722.