Signal Processing 93 (2013) 977–995

Contents lists available at SciVerse ScienceDirect

Signal Processing

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

Improving the visual quality of random grid-based visual secret sharing

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 11 March 2012
Received in revised form
12 November 2012
Accepted 14 November 2012
Available online 23 November 2012

Keywords:
Visual secret sharing
Visual quality
Random grid
Contrast
Void-and-cluster

ABSTRACT

Pixel expansion and visual quality of the revealed secret image are two major concerns in visual secret sharing (VSS). Random grid (RG) is an alternative approach to solve the pixel expansion problem by making the share as big as the original secret image, at the expense of sacrificing the visual quality of the reconstructed secret image. In this paper, two algorithms, including a contrast-enhanced RG-based VSS and a void-and-cluster-based (VAC-based) post-processing, are introduced to improve the reconstructed image quality. Experimental results and theoretical analysis are provided, illustrating that competitive visual quality is obtained by combined use of the two proposed methods.
© 2012 Elsevier B.V. All rights reserved.

1. Introduction

With the rapid development of multimedia technology, digital images are easily obtained and manipulated. The security of digital image becomes a concerned problem to be solved. To protect the images, techniques such as image encryption [1–3], data hiding [4–6] and watermarking [7,8] are proposed.

Secret image sharing is another technique to solve the security problem for digital images. VSS, which is also called visual cryptography (VC), is a significant branch of secret image sharing. It is such an approach to protect a secret image among a group of participants via splitting the secret image into random-looking images (called shares or shadows) and recovering the secret by superimposing sufficient shares.

The basic concept of VSS was proposed by Naor and Shamir in 1995 [9]. Generally speaking, in a (k,n)-threshold VSS, a binary secret image is encrypted into n meaningless shares, which are distributed to n associated participants. When any k or more participants print their shares on transparencies and stack them together, the secret image is visually revealed. However, any $k-1$ or less participants cannot guess any information about the secret by inspecting their shares. Advanced merit 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 by Naor and Shamir [9], many investigations on VSS have been conducted. To provide flexible sharing strategies, general access structure (GAS) for conventional VSS was proposed [10,11]. For the aim of generating meaningful shares, extended VSS [12,13] and halftone VSS [14,15] were introduced. For sharing different types of images, constructions for graylevel/color images were presented [16–19]. Misalignment problem of VSS was discussed in [20]. However, most of the above-mentioned conventional VSS schemes still suffer from the following drawbacks:

- Pixel expansion. The output shares are $m \geq 2$ times as big as the original secret image, where m is referred to the pixel expansion.

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

0165-1684/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2012.11.014

- Code book needed. A code book is required in the encryption phase of VSS. Sometimes, designing a code book for a specific sharing strategy is not trivial.

To construct size invariant shares, probabilistic methods were proposed. Ito et al. [21] introduced a size invariant probabilistic VSS, where each secret pixel is encoded by a column matrix selected from the corresponding basis matrix. Yang [22] proposed a non-expansible probabilistic VSS that adopts column matrices to encrypt the secret pixel. Cimato et al. [23] further extended the model proposed by Yang to form a generalized probabilistic VSS. For $m=1$, their method reduces to the one of Yang's methods [22]. For big enough values of m, for which a deterministic scheme exists, their method reduces to the classical deterministic model.

RG serves as an alternative approach to implement the size invariant VSS. In 1987, three distinct algorithms that employ RG to encrypt a binary image into two shares were proposed by Kafri and Kerenv [24]. Shyu [25] extended the pioneer work by Kafri and Keren to encode a grayscale/color image into two RGs. Later, the same author proposed a RG-based VSS for the (n,n) case [26]. In the same year, RG-based VSS schemes for the $(2,n)$ and (n,n) cases were presented by Chen and Tsao [27]. Recently, Chen and Tsao introduced a more generalized RG-based VSS model for the (k,n) threshold [28]. Other research topics on RG-based VSS such as collusive cheating activities [29] and multi-secret sharing [30] were also proposed. Note that, significant different between probabilistic VSS and RG-based VSS is that code book is not required in RG-based VSS. In addition, designing such a tailor-made code book for specific case is complicated.

Probabilistic VSS and RG-based VSS generate size invariant shares at the expense of sacrificing the visual quality of the reconstructed secret image. In this paper, we (1) extend Chen and Tsao's method [28] to develop a contrast-enhanced RG-based VSS, and (2) propose a VAC-based post-processing to improve the evenness of the reconstructed secret image. Competitive visual quality of the revealed secret image is obtained by combined use of the two proposed methods.

The remaining part of this paper is organized as follows. Section 2 formulates the (k,n) RG-based VSS proposed by Chen and Tsao [28], as well as some definitions on RG. The contrast-enhanced RG-based VSS and VAC-based post-processing are described in Section 3. Experimental results and discussions are illustrated in Section 4. Section 5 concludes our work.

2. RG-based threshold VSS

A RG is defined as a transparency consisting of a two-dimensional array of pixels [24]. Each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. There is no correlation between the values of different pixels in the array.

In a RG-based (k,n)-threshold VSS, a secret image S is encrypted into n RGs $R_1, \ldots, R_n$. To reveal the secret image, any k or more RGs $R_{i_1}, \ldots, R_{i_k}$ are stacked together directly. Let $\otimes$ denote the Boolean OR operation, the stacked result of $R_{i_1}, \ldots, R_{i_k}$ can be represented by $R_{i_1} \otimes \cdots \otimes R_{i_k}$. Prior to describing the RG-based threshold VSS, some definitions on RG are given as follows, which are borrowed from [25,28]. In addition, digit 0 denotes a white pixel and digit 1 denotes a black pixel in this paper.

Definition 1 (*Average light transmission, Shyu [25]*). 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, Shyu [25]*). 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 RG R.

Definition 3 (*Contrast, Shyu [25], Chen and Tsao [28]*). The contrast of the reconstructed secret image $S_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ with respect to the original secret image S is

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

Contrast determines how well human eyes can recognize the reconstructed secret image. It is considered to be as large as possible.

Definition 4 (*Visual recognition, Chen and Tsao [28]*). The revealed secret image $S_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ is visual recognizable as the original secret image S by contrast $\alpha > 0$. Precisely, it is $T(S_{i_1 \otimes \cdots \otimes i_k}[S(0)]) > T(S_{i_1 \otimes \cdots \otimes i_k}[S(1)])$. Whereas, it gives no clue about the secret image when $\alpha = 0$.

The RG-based (k,n)-threshold VSS proposed by Chen and Tsao [28] is formulated as follows.

RG-based VSS for (k,n) **threshold.** [28]
Input: $AM \times N$ binary secret image S.
Output: n RGs $R_1, \ldots, R_n$.
Step 1: For each position $(i,j) \in \{(i,j) | 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2–5.
Step 2: Generate $k-1$ bits b_u $(1 \le u \le k-1)$ by randomly assigning value 0 or 1 to b_u.
Step 3: Compute the k-th bit b_k by

$$b_k = S(i,j) \oplus b_1 \oplus \cdots \oplus b_{k-1}$$

where $\oplus$ denotes the Boolean XOR operation.
Step 4: Generate $n-k$ bits b_v $(k+1 \le v \le n)$ by randomly assigning value 0 or 1 to b_v.
Step 5: Randomly rearrange the order the n bits $b_1, \ldots, b_n$, and assign the rearranged n bits to n RGs $R_1(i,j), \ldots, R_n(i,j)$.
Step 6: Output the n RGs $R_1, \ldots, R_n$.

3. The proposed algorithms

In this section, a contrast-enhanced (k,n) RG-based VSS is introduced, as well as the theoretical analysis on the

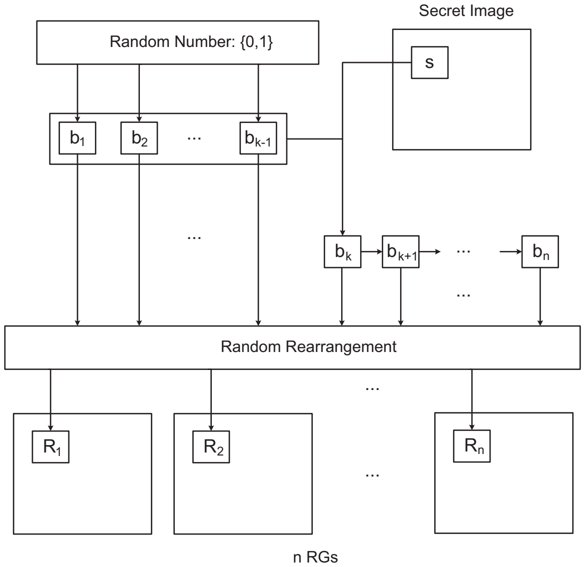

Fig. 1. Diagram of the proposed contrast-enhanced RG-based VSS.

proposed method. Due to fact that some detailed information in the original secret image would be lost by the stacking decryption, small k and n are preferred in practical applications. Specifically, $k \le 5$ and $n \le 5$. Further, a VAC-based post-processing is presented to manipulate the pixel locations in the RGs, so that a more even reconstructed secret image can be obtained.

3.1. Contrast-enhanced method

In Chen and Tsao's method [28], a secret pixel is encoded into n shared bits. Among the n bits, $k-1$ bits b_u $(1 \le u \le k-1)$ are generated randomly. b_k is then constructed by

$$b_k = S(i,j) \oplus b_1 \oplus \cdots \oplus b_{k-1}. \tag{1}$$

And finally, the rest $n-k$ bits b_v $(k+1 \le v \le n)$ are randomly generated as well. Our contribution is to enhance the contrast by determining the values of the rest $n-k$ bits, as represented by

$$b_{k+1} = b_k, b_{k+2} = b_k, \ldots, b_n = b_k. \tag{2}$$

Diagram of the proposed contrast-enhanced algorithm is shown in Fig. 1. Detailed description is formulated as follows.

Algorithm 1. Contrast-enhanced RG-based VSS for (k,n) threshold.

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

$$b_k = S(i,j) \oplus b_1 \oplus \cdots \oplus b_{k-1}$$

where $\oplus$ denotes the Boolean XOR operation.
Step 4: Compute the rest $n-k$ bits b_v $(k+1 \le v \le n)$ by $b_{k+1} = b_k, b_{k+2} = b_k, \cdots, b_n = b_k$.
Step 5: Randomly rearrange the order of the n bits $b_1, \ldots, b_n$, and assign the rearranged n bits to n RGs $R_1(i,j), \ldots, R_n(i,j)$.
Step 6: Output the n RGs $R_1, \ldots, R_n$.

Theoretical analysis on the proposed contrast-enhanced method is provided as follows.

Lemma 1. *Given a secret pixel s, the light transmissions of the n output bits $b_1, \ldots, b_n$ generated by the contrast-enhanced method are*

$$T(b_i[s=0]) = T(b_i[s=1]) = \tfrac{1}{2}, \quad i = 1, \ldots, n.$$

Proof. The first $k-1$ bits are randomly assigned the value 0 or 1, therefore $Prob(b_i = 0) = Prob(b_i = 1) = \frac{1}{2}$ for $1 \le i \le k-1$, where $Prob$ represents the probability. Since the $k-1$ bits are random, no matter the secret pixel s is black or white, the light transmissions are $T(b_i[s=0]) = T(b_i[s=1]) = \frac{1}{2}$ for $1 \le i \le k-1$. For $s=0$, the k-th bit b_k is constructed by $b_k = 0 \oplus b_1 \oplus \cdots \oplus b_{k-1} = b_1 \oplus \cdots \oplus b_{k-1}$. For $s=1$, the k-th bit b_k is $b_k = 1 \oplus b_1 \oplus \cdots \oplus b_{k-1} = \overline{b_1} \oplus \cdots \oplus b_{k-1}$. Since b_1 is random, $\overline{b_1}$ is random as well. b_k is random because it is determined by the $k-1$ random bits. We have $Prob(b_k = 0) = Prob(b_k = 1) = \frac{1}{2}$ no matter s is black or white. That is $T(b_k[s=0]) = T(b_k[s=1]) = \frac{1}{2}$. □

For the rest $n-k$ bits, since they take the same value as b_k, we get $T(b_i[s=0]) = T(b_i[s=1]) = \frac{1}{2}$ for $k+1 \le i \le n$.

Totally, the light transmissions of the n bits generated by the contrast-enhanced method are

$$T(b_i[s=0]) = T(b_i[s=1]) = \tfrac{1}{2}, \quad i = 1, \ldots, n. \qquad \square$$

Lemma 2. *Given a secret pixel s, $b_1, \ldots, b_k$ are the first k bits generated by the contrast-enhanced method. By stacking any p $(p<k)$ bits to form $b_{i_1 \otimes \cdots \otimes i_p} = b_{i_1} \otimes \cdots \otimes b_{i_p}$, the light transmissions of the stacked results are*

$$T(b_{i_1 \otimes \cdots \otimes i_p}[s=0]) = T(b_{i_1 \otimes \cdots \otimes i_p}[s=1]) = (\tfrac{1}{2})^p, \quad p<k.$$

Proof. Without loss of generality, $\{i_1, \ldots, i_p\}$ is a subset of $\{1, \ldots, k\}$. To prove this lemma, two cases are considered: (1) $k \in \{i_1, \ldots, i_p\}$, (2) $k \notin \{i_1, \ldots, i_p\}$.

(1) $k \in \{i_1, \ldots, i_p\}$. The k-th bit b_k is in $\{b_{i_1}, \ldots, b_{i_p}\}$. Let $g, \ldots, h$ be the indices in $\{i_1, \ldots, i_p\}$ besides k. The stacked result of the p bits is rewrote as

$$b_{i_1 \otimes \cdots \otimes i_p} = b_{i_1} \otimes \cdots \otimes b_{i_p} = b_g \otimes \cdots \otimes b_h \otimes b_k.$$

Since $p-1$ bits $b_g, \ldots, b_h$ are randomly generated, they are independent of the corresponding secret pixel s. We have

$$T(b_{g \otimes \cdots \otimes h}[s=0]) = T(b_{g \otimes \cdots \otimes h}[s=1]) = (\tfrac{1}{2})^{(p-1)}.$$

Since $p<k$ and $k \in \{i_1, \ldots, i_p\}$, an independent random bit b_m which meets the following conditions can be found:

$$b_m \in \{b_1, \ldots, b_{k-1}\} \quad \text{and} \quad b_m \notin \{b_{i_1}, \ldots, b_{i_p}\}.$$

Since $b_k = s \oplus b_1 \oplus \cdots \oplus b_m \oplus \cdots \oplus b_{k-1} = s \oplus \ b_{i_1} \oplus \cdots \oplus b_{i_p} \oplus b_m \oplus \cdots$, b_k is independent of $s, b_{i_1}, \ldots, b_{i_p}$. Therefore,

$$T(b_{g \otimes \cdots \otimes h \otimes k}[s=0]) = T(b_{g \otimes \cdots \otimes h}[s=0]) \times T(b_k[s=0]) = (\tfrac{1}{2})^{(p-1)} \times \tfrac{1}{2} = (\tfrac{1}{2})^p,$$

$$T(b_{g \otimes \cdots \otimes h \otimes k}[s=1]) = T(b_{g \otimes \cdots \otimes h}[s=1]) \times T(b_k[s=1]) = (\tfrac{1}{2})^{(p-1)} \times \tfrac{1}{2} = (\tfrac{1}{2})^p.$$

We finally obtain $T(b_{i_1 \otimes \cdots \otimes i_p}[s=0]) = T(b_{i_1 \otimes \cdots \otimes i_p}[s=1]) = (\frac{1}{2})^p$.

(2) $k \notin \{i_1,\ldots,i_p\}$. The p bits $b_{i_1},\ldots,b_{i_p}$ are randomly generated and they are independent of the secret pixel s. Hence, the light transmissions of the stacked results of the p bits are

$T(b_{i_1\otimes\cdots\otimes i_p}[s=0]) = T(b_{i_1\otimes\cdots\otimes i_p}[s=1]) = (\frac{1}{2})^p$. □

Lemma 3. *Given a secret pixel s, $b_1,\ldots,b_n$ are the n bits generated by the contrast-enhanced method. By stacking any p ($p<n$) bits to form $b_{i_1\otimes\cdots\otimes i_p} = b_{i_1}\otimes\cdots\otimes b_{i_p}$, the light transmissions of the stacked results are*

$T(b_{i_1\otimes\cdots\otimes i_p}[s=0]) = T(b_{i_1\otimes\cdots\otimes i_p}[s=1])$.

Proof. Generally speaking, for the p bits, u bits can be selected from the first $k-1$ random bits $b_1,\ldots,b_{k-1}$ and v bits can be selected from the rest $n-k+1$ bits $b_k,\ldots,b_n$. The proof of this lemma is divided into two components: (1) $u=p$, $v=0$, (2) $u<p$, $v=p-u$.

(1) $u=p$, $v=0$. The p bits are selected from $\{b_1,\ldots,b_{k-1}\}$. The p bits are randomly generated and are independent of the corresponding secret pixel s. The light transmissions of the stacked results of the p bits are

$T(b_{i_1\otimes\cdots\otimes i_p}[s=0]) = T(b_{i_1\otimes\cdots\otimes i_p}[s=1]) = (\frac{1}{2})^p$.

(2) $u<p$, $v=p-u$. In this case, v bits are selected from $b_k,\ldots,b_n$. Since $b_n=\cdots=b_k$, the stacked result of the v bits is the same as b_k. The v bits can be considered as one bit b_k. That means, the light transmissions of the stacked results of the p bits are equal to the light transmissions of the stacked results of the u bits and b_k. By Lemma 2, the light transmissions of the stacked results of the u bits and b_k are $(\frac{1}{2})^{(u+1)}$, no matter the corresponding secret pixel s is black or white.

Totally, the light transmissions of the two cases are the same no matter the corresponding secret pixel is black or white. Therefore, we have

$T(b_{i_1\otimes\cdots\otimes i_p}[s=0]) = T(b_{i_1\otimes\cdots\otimes i_p}[s=1])$. □

Lemma 4. *Given a secret pixel s, $b_1,\ldots,b_k$ are the k bits generated by the contrast-enhanced method. That is, $b_1,\ldots,b_{k-1}$ are random and $b_k = s\oplus b_1\oplus\cdots\oplus b_{k-1}$. For $s=0$, the light transmission of the stacked result of the k bits is $T(b_{1\otimes\cdots\otimes k}[s=0]) = (\frac{1}{2})^{k-1}$. Whereas, $T(b_{1\otimes\cdots\otimes k}[s=1]) = 0$ for $s=1$.*

Proof. If the stacked result $b_{1\otimes\cdots\otimes k}$ is white, all the k pixels have to be white. Since the $k-1$ bits $b_1,\ldots,b_{k-1}$ are randomly generated, the probability for the $k-1$ pixels to be white is $Prob(b_1=0\cap\cdots\cap b_{k-1}=0) = (\frac{1}{2})^{k-1}$. For $s=0$, $b_k = 0\oplus b_1\oplus\cdots\oplus b_{k-1}$. If $b_1,\ldots,b_{k-1}$ are all white, b_k is certainly white. Therefore, we have $T(b_{1\otimes\cdots\otimes k}[s=0]) = (\frac{1}{2})^{k-1}$.

For $s=1$, $b_k = 1\oplus b_1\oplus\cdots\oplus b_{k-1}$. If $b_1,\ldots,b_{k-1}$ are all white, b_k is black. The stacked result is black. When $b_1,\ldots,b_{k-1}$ are not all white, at least one bit is black, the stacked result is black. That means, the stacked result of the k bits is certainly black when $s=1$. Hence, we get $T(b_{1\otimes\cdots\otimes k}[s=1]) = 0$. □

Lemma 5. *Given a secret pixel s, $b_1,\ldots,b_n$ are the n bits generated by the contrast-enhanced method. By stacking any q ($q\ge k$) bits to form $b_{i_1\otimes\cdots\otimes i_q} = b_{i_1}\otimes\cdots\otimes b_{i_q}$, for $s=0$, the light transmission of the stacked result is*

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=0]) = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } q=n, \\ \frac{1}{\binom{n}{q}}(A\cdot B\cdot C) & \text{otherwise,} \end{cases}$$

where "·" denotes inner product and

$$A = \begin{cases} \left[\binom{k-1}{q-n+k-1},\ldots,\binom{k-1}{k-1}\right] & \text{for } n-k+1\le q<n, \\ \left[\binom{k-1}{0},\ldots,\binom{k-1}{k-1}k-1\right] & \text{otherwise,} \end{cases}$$

$$B = \begin{cases} \left[\binom{n-k+1}{n-k+1},\ldots,\binom{n-k+1}{q-k+1}\right] & \text{for } n-k+1\le q<n, \\ \left[\binom{n-k+1}{q},\ldots,\binom{n-k+1}{q-k+1}\right] & \text{otherwise,} \end{cases}$$

$$C = \begin{cases} \left[\left(\frac{1}{2}\right)^{q-n+k},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},\left(\frac{1}{2}\right)^{k-1}\right] & \text{for } n-k+1\le q<n, \\ \left[\frac{1}{2},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},\left(\frac{1}{2}\right)^{k-1}\right] & \text{otherwise.} \end{cases}$$

Whereas, for $s=1$, the light transmission of the stacked result is

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=1]) = \begin{cases} 0 & \text{for } q=n, \\ \frac{1}{\binom{n}{q}}(A\cdot B\cdot D) & \text{otherwise,} \end{cases}$$

where

$$D = \begin{cases} \left[\left(\frac{1}{2}\right)^{q-n+k},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},0\right] & \text{for } n-k+1\le q<n, \\ \left[\frac{1}{2},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},0\right] & \text{otherwise.} \end{cases}$$

Proof. For any q bits, u bits can be selected from $b_1,\ldots,b_{k-1}$ and v bits can be selected from $b_k,\ldots,b_n$. Two cases are taken into consideration: (1) $u=k-1$, $v=q-u$, (2) $u<k-1$, $v=q-u$.

(1) $u=k-1$, $v=q-u$. Since $q\ge k$ and $u=k-1$, we have $v=q-u>0$. At least one bit in $b_k,\ldots,b_n$ is selected. For $b_n=\cdots=b_k$, the stacked result of the selected v bits is the same as b_k. In this case, light transmission of the stacked results of the q bits is the same as the light transmission of the stacked result of $b_1,\ldots,b_{k-1},b_k$. By Lemma 4, we have

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=0]) = T(b_{1\otimes\cdots\otimes k}[s=0]) = (\tfrac{1}{2})^{k-1},$$
$$T(b_{i_1\otimes\cdots\otimes i_q}[s=1]) = T(b_{1\otimes\cdots\otimes k}[s=1]) = 0.$$

(2) $u<k-1$, $v=q-u$. Similar to the first case, the stacked result of the q bits is the same as the stacked result of the u bits with b_k. Since $u<k-1$, the u bits and b_k

form a subset of $\{b_1,\ldots,b_k\}$. By Lemma 2, we obtain

$T(b_{i_1\otimes\cdots\otimes i_q}[s=0])=T(b_{i_1\otimes\cdots\otimes i_u\otimes k}[s=0])=(\frac{1}{2})^{u+1}$,
$T(b_{i_1\otimes\cdots\otimes i_q}[s=1])=T(b_{i_1\otimes\cdots\otimes i_u\otimes k}[s=1])=(\frac{1}{2})^{u+1}$.

Generally, the probability for picking up u bits from $b_1,\ldots,b_{k-1}$ and picking up v bits from $b_k,\ldots,b_n$ simultaneously is $\binom{k-1}{u}\binom{n-k+1}{v}/\binom{n}{q}$. For the first case, $u=k-1, v=q-k+1$, the probability is $\binom{k-1}{k-1}\binom{n-k+1}{q-k+1}/\binom{n}{q}$. For the second case, it is divided into three situations for different q. When $q=n$, the probability of the second case is 0. When $n-k+1\le q<n$, at most $n-k+1$ bits are selected from $b_k,\ldots,b_n$. The probability is modified to $\binom{k-1}{q-n+k-1}\binom{n-k+1}{n-k+1}+\binom{k-1}{q-n+k}\binom{n-k+1}{n-k}+\cdots+\binom{k-1}{k-2}\binom{n-k+1}{q-k+2}/\binom{n}{q}$. When $k\le q<n-k+1$, at most q bits are selected from $b_k,\ldots,b_n$. the probability is $\binom{k-1}{0}\binom{n-k+1}{q}+\binom{k-1}{1}\binom{n-k+1}{q-1}+\cdots+\binom{k-1}{k-2}\binom{n-k+1}{q-k+2}/\binom{n}{q}$.

Therefore, for $s=0$, the light transmission of the stacked result of the q bits is

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=0])=\begin{cases}\left(\frac{1}{2}\right)^{k-1} & \text{for } q=n,\\ \frac{1}{\binom{n}{q}}\left(\binom{k-1}{q-n+k-1}\binom{n-k+1}{n-k+1}\left(\frac{1}{2}\right)^{q-n+k}+\binom{k-1}{q-n+k}\binom{n-k+1}{n-k+2}\left(\frac{1}{2}\right)^{q-n+k+1}+\cdots+\right.\\ \left.\binom{k-1}{k-2}\binom{n-k+1}{q-k+2}\left(\frac{1}{2}\right)^{k-1}+\binom{k-1}{k-1}\binom{n-k+1}{q-k+1}\left(\frac{1}{2}\right)^{k-1}\right) & \text{for } n-k+1\le q<n,\\ \frac{1}{\binom{n}{q}}\left(\binom{k-1}{0}\binom{n-k+1}{q}\left(\frac{1}{2}\right)+\binom{k-1}{1}\binom{n-k}{n-k+2}\left(\frac{1}{2}\right)^{2}+\cdots+\right.\\ \left.\binom{k-1}{k-2}\binom{n-k+1}{q-k+2}\left(\frac{1}{2}\right)^{k-1}+\binom{k-1}{k-1}\binom{n-k+1}{q-k+1}\left(\frac{1}{2}\right)^{k-1}\right) & \text{otherwise.}\end{cases}$$

Let

$$A=\begin{cases}\left[\binom{k-1}{q-n+k-1},\ldots,\binom{k-1}{k-1}\right] & \text{for } n-k+1\le q<n,\\ \left[\binom{k-1}{0},\ldots,\binom{k-1}{k-1}\right] & \text{otherwise,}\end{cases}$$

$$B=\begin{cases}\left[\binom{n-k+1}{n-k+1},\ldots,\binom{n-k+1}{q-k+1}\right] & \text{for } n-k+1\le q<n,\\ \left[\binom{n-k+1}{q},\ldots,\binom{n-k+1}{q-k+1}\right] & \text{otherwise,}\end{cases}$$

$$C=\begin{cases}\left[\left(\frac{1}{2}\right)^{q-n+k},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},\left(\frac{1}{2}\right)^{k-1}\right] & \text{for } n-k+1\le q<n,\\ \left[\frac{1}{2},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},\left(\frac{1}{2}\right)^{k-1}\right] & \text{otherwise.}\end{cases}$$

We have

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=0])=\begin{cases}\left(\frac{1}{2}\right)^{k-1} & \text{for } q=n,\\ \frac{1}{\binom{n}{q}}(A\cdot B\cdot C) & \text{otherwise.}\end{cases}$$

Similarly, the light transmission of the stacked result of the q bits when $s=1$ is

$$T(b_{i_1\otimes\cdots\otimes i_q}[s=1])=\begin{cases}0 & \text{for } q=n,\\ \frac{1}{\binom{n}{q}}(A\cdot B\cdot D) & \text{otherwise,}\end{cases}$$

where

$$D=\begin{cases}\left[\left(\frac{1}{2}\right)^{q-n+k},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},0\right] & \text{for } n-k+1\le q<n,\\ \left[\frac{1}{2},\ldots,\left(\frac{1}{2}\right)^{k-2},\left(\frac{1}{2}\right)^{k-1},0\right] & \text{otherwise.}\end{cases}$$

□

Theorem 1. *Given a secret image S, $R_1,\ldots,R_n$ are the n shares generated by the contrast-enhanced method. Let $S_{i_1\otimes\cdots\otimes i_t}=R_{i_1}\otimes\cdots\otimes R_{i_t}$ be the stacked result of any t shares. The contrast-enhanced method is a valid construction of a (k,n)-threshold VSS scheme by RGs. It meets the following three conditions*:

(i) *For $1\le i\le n$, R_i is a RG with $T(R_i[S(0)])=T(R_i[S(1)])=\frac{1}{2}$.*
(ii) *If $t<k$, $T(S_{i_1\otimes\cdots\otimes i_t}[S(0)])=T(S_{i_1\otimes\cdots\otimes i_t}[S(1)])$.*
(iii) *If $t\ge k$, $T(S_{i_1\otimes\cdots\otimes i_t}[S(0)])>T(S_{i_1\otimes\cdots\otimes i_t}[S(1)])$.*

Proof. By Lemma 1, we have $T(b_i[s=0])=T(b_i[s=1])=\frac{1}{2}, 1\le i\le n$. By Definition 1, we get $T(R_i[S(0)])=T(R_i[S(1)])=\frac{1}{2}, 1\le i\le n$.

If $t<k$, by Lemma 3, we obtain $T(b_{i_1\otimes\cdots\otimes i_t}[s=0])=T(b_{i_1\otimes\cdots\otimes i_t}[s=1])$. By Definition 1, we get $T(S_{i_1\otimes\cdots\otimes i_t}[S(0)])=T(S_{i_1\otimes\cdots\otimes i_t}[S(1)])$. By Definition 4, any $k-1$ or less shares give no clue about the secret image.

If $t \geq k$, by Lemma 5, we obtain

$$T(b_{i_1 \otimes \cdots \otimes i_t}[s=0]) - T(b_{i_1 \otimes \cdots \otimes i_t}[s=1]) = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } t=n, \\ \dfrac{\binom{k-1}{k-1}\binom{n-k+1}{t-k+1}\left(\frac{1}{2}\right)^{k-1}}{\binom{n}{t}} & \text{otherwise.} \end{cases}$$

Since $(\frac{1}{2})^{k-1} > 0$ and $\binom{k-1}{k-1}\binom{n-k+1}{t-k+1}(\frac{1}{2})^{k-1}/\binom{n}{t} > 0$, $T(b_{i_1 \otimes \cdots \otimes i_t}[s=0]) > T(b_{i_1 \otimes \cdots \otimes i_t}[s=1])$. By Definition 1, we get $T(S_{i_1 \otimes \cdots \otimes i_t}[S(0)]) > T(S_{i_1 \otimes \cdots \otimes i_t}[S(1)])$. By Definition 4, the secret image is visual recognized by stacking any k or more shares. □

Theorem 2. *The contrast α of the stacked result of t $(k \leq t \leq n)$ shares generated by the contrast-enhanced (k,n)-threshold VSS is*

$$\alpha = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } t=n, \\ \dfrac{\binom{n-k+1}{t-k+1}\left(\frac{1}{2}\right)^{k-1}}{\binom{n}{t} + A \cdot B \cdot D} & \text{otherwise,} \end{cases}$$

where

$$A = \begin{cases} \left[\binom{k-1}{q-n+k-1}, \ldots, \binom{k-1}{k-1}\right] & \text{for } n-k+1 \leq q < n, \\ \left[\binom{k-1}{0}, \ldots, \binom{k-1}{k-1}\right] & \text{otherwise,} \end{cases}$$

$$B = \begin{cases} \left[\binom{n-k+1}{n-k+1}, \ldots, \binom{n-k+1}{q-k+1}\right] & \text{for } n-k+1 \leq q < n, \\ \left[\binom{n-k+1}{q}, \ldots, \binom{n-k+1}{q-k+1}\right] & \text{otherwise,} \end{cases}$$

$$D = \begin{cases} \left[\left(\frac{1}{2}\right)^{q-n+k}, \ldots, \left(\frac{1}{2}\right)^{k-2}, \left(\frac{1}{2}\right)^{k-1}, 0\right] & \text{for } n-k+1 \leq q < n, \\ \left[\frac{1}{2}, \ldots, \left(\frac{1}{2}\right)^{k-2}, \left(\frac{1}{2}\right)^{k-1}, 0\right] & \text{otherwise.} \end{cases}$$

Proof. By Lemma 5, we have

$$T(b_{i_1 \otimes \cdots \otimes i_t}[s=0]) - T(b_{i_1 \otimes \cdots \otimes i_t}[s=1]) = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } t=n, \\ \dfrac{\binom{k-1}{k-1}\binom{n-k+1}{t-k+1}\left(\frac{1}{2}\right)^{k-1}}{\binom{n}{t}} & \text{otherwise.} \end{cases}$$

Furthermore,

$$\frac{T(b_{i_1 \otimes \cdots \otimes i_t}[s=0]) - T(b_{i_1 \otimes \cdots \otimes i_t}[s=1])}{1 + T(b_{i_1 \otimes \cdots \otimes i_t}[s=1])} = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } t=n, \\ \dfrac{\binom{n-k+1}{t-k+1}\left(\frac{1}{2}\right)^{k-1}}{\binom{n}{t} + A \cdot B \cdot D} & \text{otherwise,} \end{cases}$$

where

$$A = \begin{cases} \left[\binom{k-1}{q-n+k-1}, \ldots, \binom{k-1}{k-1}\right] & \text{for } n-k+1 \leq q < n, \\ \left[\binom{k-1}{0}, \ldots, \binom{k-1}{k-1}\right] & \text{otherwise,} \end{cases}$$

$$B = \begin{cases} \left[\binom{n-k+1}{n-k+1}, \ldots, \binom{n-k+1}{q-k+1}\right] & \text{for } n-k+1 \leq q < n, \\ \left[\binom{n-k+1}{q}, \ldots, \binom{n-k+1}{q-k+1}\right] & \text{otherwise,} \end{cases}$$

$$D = \begin{cases} \left[\left(\frac{1}{2}\right)^{q-n+k}, \ldots, \ldots, \left(\frac{1}{2}\right)^{k-2}, \left(\frac{1}{2}\right)^{k-1}, 0\right] & \text{for } n-k+1 \leq q < n, \\ \left[\frac{1}{2}, \ldots, \ldots, \left(\frac{1}{2}\right)^{k-2}, \left(\frac{1}{2}\right)^{k-1}, 0\right] & \text{otherwise.} \end{cases}$$

By Definition 1, the contrast is

$$\alpha = \frac{T(S_{i_1 \otimes \cdots \otimes i_t}[S(0)]) - T(S_{i_1 \otimes \cdots \otimes i_t}[S(1)])}{1 + T(S_{i_1 \otimes \cdots \otimes i_t}[S(1)])} = \begin{cases} \left(\frac{1}{2}\right)^{k-1} & \text{for } t=n, \\ \dfrac{\binom{n-k+1}{t-k+1}\left(\frac{1}{2}\right)^{k-1}}{\binom{n}{t} + A \cdot B \cdot D} & \text{otherwise.} \end{cases}$$ □

3.2. VAC-based post-processing

RG-based VSS generates size invariant shares at the expense of sacrificing the visual quality of reconstructed secret image. In the recovered secret image, black or white pixels may cluster together since they are generated randomly. Those clustered pixels would reduce the recovered image quality in certain degree. On the other hand, more detailed information in the reconstructed secret image can be identified by human eyes when a more even recovered image is obtained. To achieve a more even reconstructed secret image, the black and white pixels on the revealed secret image should be distributed homogeneously and be maximally separated from each other. Herein, a VAC-based algorithm is proposed to achieved this aim.

The VAC algorithm was initially introduced by Ulichney [31] for constructing dither arrays for order dithering. In his work, the terms minority pixel and majority pixel are utilized. When less than half of the pixel are black, they are minority pixels and the majority pixels are white. The reverse is true when more than half of the pixels are white. Moreover, the terms cluster and void refer to the arrangement of minority pixels on the background of majority pixels. A cluster is a tight group of minority pixels and a void is a large space between minority pixels. In this paper, the black pixels are considered as minority pixels and the white pixels are referred to majority pixels. To produce homogeneous distribution of the minority pixels, minority pixels are added in the center of the largest voids, and majority pixels are added in the center of the tightest clusters.

To find the largest void and the tightest cluster in a binary image I, a void-and-cluster-finding filter is adopted, as given by

$$M(i,j) = \sum_{p=-W/2}^{W/2} \sum_{q=-W/2}^{W/2} G(p,q) D(i+p,j+q), \tag{3}$$

where $M(i,j)$ is the minority pixel density (m.p.d.) at position (i,j), $G(p,q)$ is a two-dimensional Gaussian filter, W is the window width of the filter, and $D(i+p,j+q)$ is defined by

$$D(i+p,j+q) = \begin{cases} 1 & \text{if } I(i+p,j+q) \text{ is black,} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

The two-dimensional Gaussian filter is given by

$$G(p,q) = e^{-(p^2+q^2)/2\sigma^2}, \tag{5}$$

where σ is a scalar constant which provides best results at $\sigma = 1.5$ in [31]. The VAC algorithm, in essence, identifies the minority pixel with the highest m.p.d. and the majority pixel with the lowest m.p.d., and switches their positions. In general, this operation spreads the minority pixels as homogeneously as possible. The VAC algorithm executes iteratively until switching the minority pixel with the highest m.p.d. and the majority pixel with the lowest m.p.d. would create larger void. Then the minority pixels in the image I are distributed homogeneously. An example of applying the VAC algorithm to the binary random pattern to form homogeneous distribution of minority pixels is shown in Fig. 2.

To generate an even reconstructed secret image, a VAC-based post-processing is proposed, as described as follows.

Algorithm 2. VAC-based post-processing.

Input: The binary secret image S and n RGs $R_1, \ldots, R_n$.
Output: n RGs $R_1, \ldots, R_n$.
Step 1: Randomly select a RG R_i from the n RGs.
Step 2: Identify the black pixel location with the highest m.p.d. by using the VAC algorithm and determine the region it belongs to ($R_i[S(0)]$ or $R_i[S(1)]$).
Step 3: Identify the white pixel location with the lowest m.p.d. by using the VAC algorithm in the same region.
Step 4: Switch the two identified black and white pixels on the chosen RG.
Step 5: Conduct the same switching procedure on the rest $n-1$ RGs at the same location as the chosen RG.
Step 6: Steps 1–5 execute iteratively until the switching procedure on the chosen RG creates larger white area.
Step 7: Output the n RGs $R_1, \ldots, R_n$.

The proposed post-processing manipulates the locations of black and white pixels in the RGs, so that black pixels in the RGs are distributed homogeneously. Further, homogeneous distribution of black pixels in the RGs can lead to homogeneous distribution of reconstructed black pixels in the revealed secret image. As a result, the evenness of the reconstructed secret image can be improved. Note that, in order to guarantee that the information in the decoded secret image is not changed by the post-processing, the switching procedure must be conducted within the same region ($R_i[S(0)]$ or $R_i[S(1)]$).

In each RG, the probability for a pixel to be black is about $\frac{1}{2}$. Hence, the number of black pixels is approximately the same as the number of white pixels in each RG. It is possible to consider the white pixels as the minority pixels and black pixels as the majority pixels. However, no matter which type of pixels is considered as minority, the purpose of utilizing the VAC-based post-processing is to distribute the black (white) pixels homogeneously and let them be maximally separated form each other. Since the number of black pixels is approximately the same as the number of white pixels in each RG, the homogeneous distribution of black (resp. white) pixels would certainly result in the homogeneous

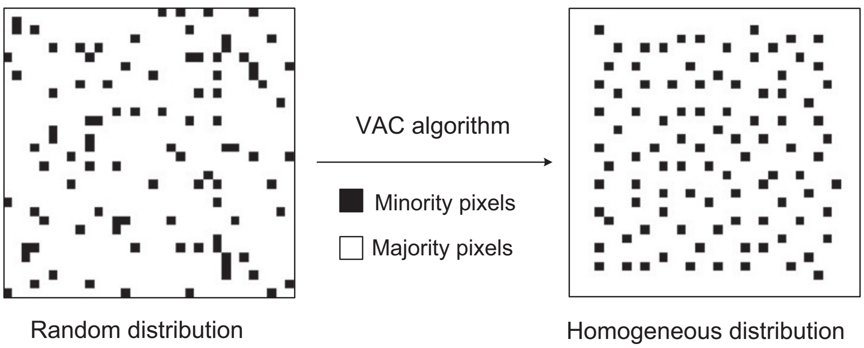

Fig. 2. Example of generating homogeneous distribution of minority pixels from the random pattern by using the VAC algorithm.

distribution of white (resp. black) pixels. The visual quality of reconstructed secret image will not be affected, in spite of which type of pixels is considered as minority. For convenient, we define the black pixels as minority pixels so that the calculation of exact number of black pixels in each RG can be avoided.

3.3. Extension for grayscale/color images

The two proposed methods can be further extended to share grayscale/color images. For sharing the graylevel images, halftoning techniques such as order dithering, error diffusion and dot diffusion are applied to the grayscale image to convert it into binary. Then, the two proposed methods are applied to the halftone image, and the output RGs are obtained.

To share the color images, color decomposition, halftone technique and color composition are utilized. The constitution of colors is described by color model. There are totally two types of color models: (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

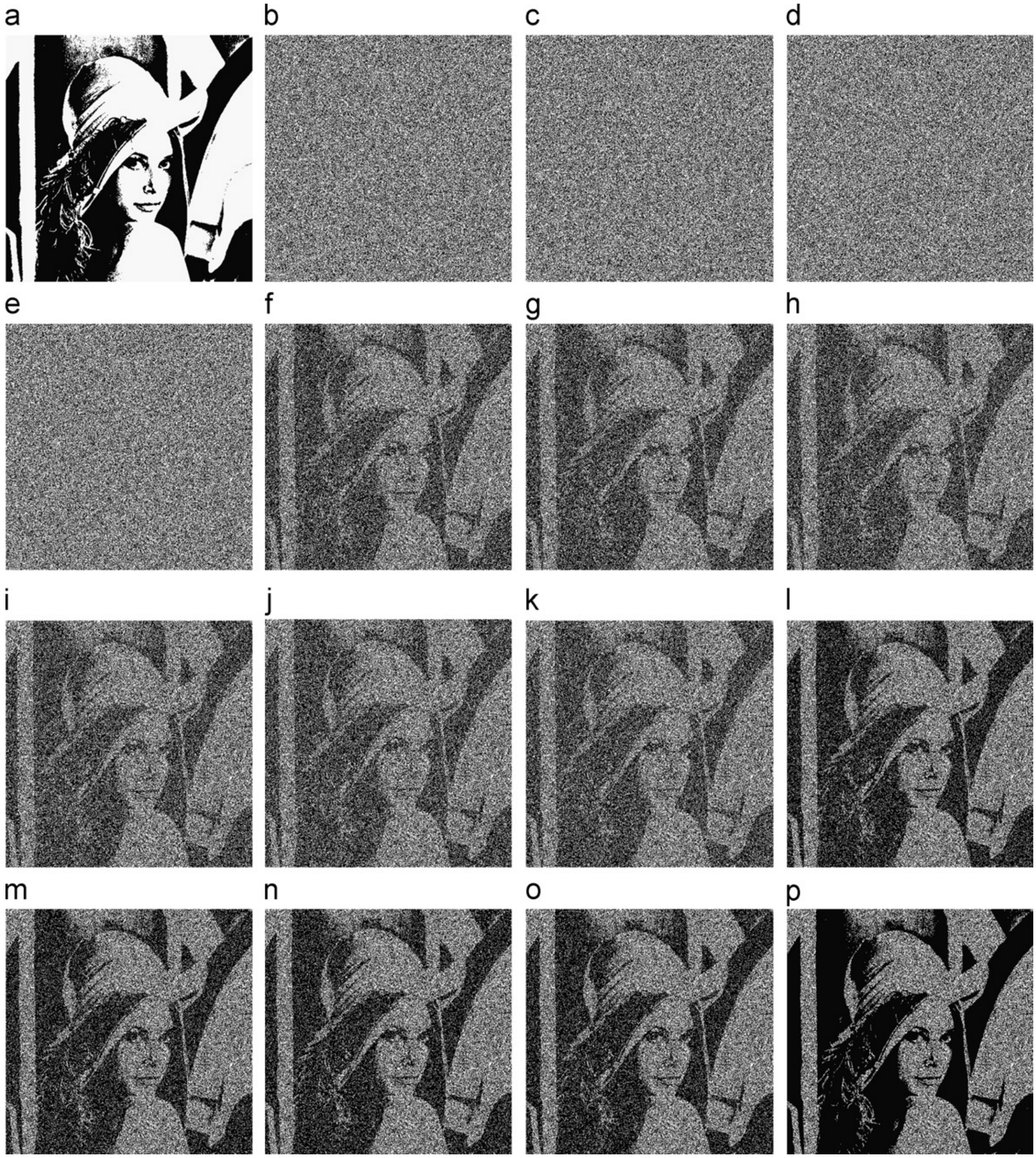

Fig. 3. Experiment of a (2,4) case by the proposed contrast-enhanced VSS. (a) The binary secret image, (b)–(e) four RGs: R_1, R_2, R_3 and R_4, (f) $R_1 \otimes R_2$, (g) $R_1 \otimes R_3$, (h) $R_1 \otimes R_4$, (i) $R_2 \otimes R_3$, (j) $R_2 \otimes R_4$, (k) $R_3 \otimes R_4$, (l) $R_1 \otimes R_2 \otimes R_3$, (m) $R_1 \otimes R_2 \otimes R_4$, (n) $R_1 \otimes R_3 \otimes R_4$, (o) $R_2 \otimes R_3 \otimes R_4$, (p) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

(cyan–magenta–yellow) model. Since the secret image is visually reconstructed by stacking, the CMY model is adopted in this paper. In all, 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 two proposed methods, and some RGs are constructed. Finally, those corresponding RGs are composed by the CMY color model to form color RGs.

4. Experimental results and discussions

4.1. Visual quality evaluation

In reported RG-based VSS, the visual quality of recovered secret image is only evaluated by average contrast, as defined in Definition 3. However, the average contrast alone is not enough to reflect the visual quality, and Liu et al. [32] pointed out that the visual quality of reconstructed secret image can be measured by both contrast and evenness. Contrast refers to the difference between the average light transmission of the reconstructed white secret pixels and the average light transmission of the reconstructed black secret pixels. It determines how well human eyes can recognize the sketch of the reconstructed secret image. But in some VSS schemes, the same contrast is obtained but those recovered secret images are with different visual quality. Some recovered secret images are quite noisy and some are more even. However, more detailed information can be identified by human eyes in an even recovered secret image. The evenness of the recovered image affects the image quality as well. In this paper, the variance of the darkness levels of a block is introduced to evaluate the evenness of the recovered secret image, where Hou and Tu [33] and Liu et al. [32] also mentioned the same criterion. The definition on variance of the darkness levels of a block is given below.

Definition 5 (*Variance*). 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 non-overlapping 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 VSS, and M blocks in the same locations of the recovered image are obtained. Denote the corresponding M blocks in the recovered image as $RS_1,\ldots,RS_M$. Variance $\sigma_{t,b}$ of the darkness levels of $B_{t,b}$ is calculated by

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

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

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

With a small variance, a more even recovered secret image is obtained. For achieving competitive visual quality, increasing the contrast and reducing the variance are required.

In this paper, t is set to be 4, and the size of the block is set to be 2×2. The reasons for selecting such a block size are: (1) images are two-dimensional signals, vertical, horizontal and diagonal directions of the signals should be considered for calculating the variance, and (2) 2×2 is the smallest size for a block to contain the three directions simultaneously. Since t=4, five types of blocks are used totally. Five variances $\sigma_{4,4},\ldots,\sigma_{4,0}$ are employed for evaluating the evenness of the recovered secret image in this work.

4.2. Example of contrast-enhanced scheme

Experiment of a (2,4) case by using the proposed contrast-enhanced algorithm is illustrated in Fig. 3. The binary secret image is shown in Fig. 3(a), which consists of 512×512 pixels. The four generated RGs are demonstrated in Fig. 3(b)–(e). The stacked results by any two of the four RGs are shown in Fig. 3(f)–(k). The stacked results by any three of the four RGs are demonstrated in Fig. 3(l)–(o). The superimposed result of the four RGs is shown in Fig. 3(p). To evaluate the visual quality of the constructed secret images, the contrast and variance are adopted. Table 1 illustrates the experimental contrasts

Table 1
Contrasts and variances of the reconstructed secret images by the proposed contrast-enhanced method for the (2,4) case.

Recovered image	Contrast	Variance				
		$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
$R_1 \otimes R_2$	0.1967	0.7677	0.7957	0.8606	0.9291	0.9962
$R_1 \otimes R_3$	0.1980	0.7514	0.7906	0.8806	0.9256	0.9962
$R_1 \otimes R_4$	0.1979	0.7472	0.7786	0.8910	0.9372	0.9962
$R_2 \otimes R_3$	0.2000	0.7370	0.8153	0.8874	0.9135	0.9962
$R_2 \otimes R_4$	0.1999	0.7490	0.8075	0.8864	0.9251	0.9962
$R_3 \otimes R_4$	0.2012	0.7472	0.7910	0.8995	0.9216	0.9962
$R_1 \otimes R_2 \otimes R_3$	0.3306	0.4408	0.5728	0.7175	0.8380	0.9962
$R_1 \otimes R_2 \otimes R_4$	0.3305	0.4377	0.5674	0.7189	0.8511	0.9962
$R_1 \otimes R_3 \otimes R_4$	0.3321	0.4417	0.5540	0.7290	0.8464	0.9962
$R_2 \otimes R_3 \otimes R_4$	0.3346	0.4281	0.5742	0.7347	0.8326	0.9962
$R_1 \otimes R_2 \otimes R_3 \otimes R_4$	0.4991	0	0.2498	0.5033	0.7291	0.9962

and variances of the recovered secret images which are shown in Fig. 3. The experimental contrasts of the reconstructed secret image are approximately the same as the theoretical results, where the theoretical contrasts of stacked results by two, three, four RGs are $\frac{1}{5}, \frac{1}{3}$ and $\frac{1}{2}$, respectively, for the (2,4) case.

4.3. Example of the post-processing

The proposed post-processing is applied to the four RGs, which are obtained from the above (2,4) case. The four RGs after post-processing are illustrated in Fig. 4(a)–(d). The stacked results by different combinations of the four RGs are shown in Fig. 4(e)–(o). Moreover, contrasts and variances calculated from the reconstructed secret images are demonstrated in Table 2. Obviously, smaller variances are achieved, and the same contrasts of the recovered images are maintained. In all, a more even reconstructed secret image is obtained by the post-processing.

4.4. Examples for the grayscale/color images

Experiment of a (2,3) case for grayscale images by combined use of the two proposed methods (the combined

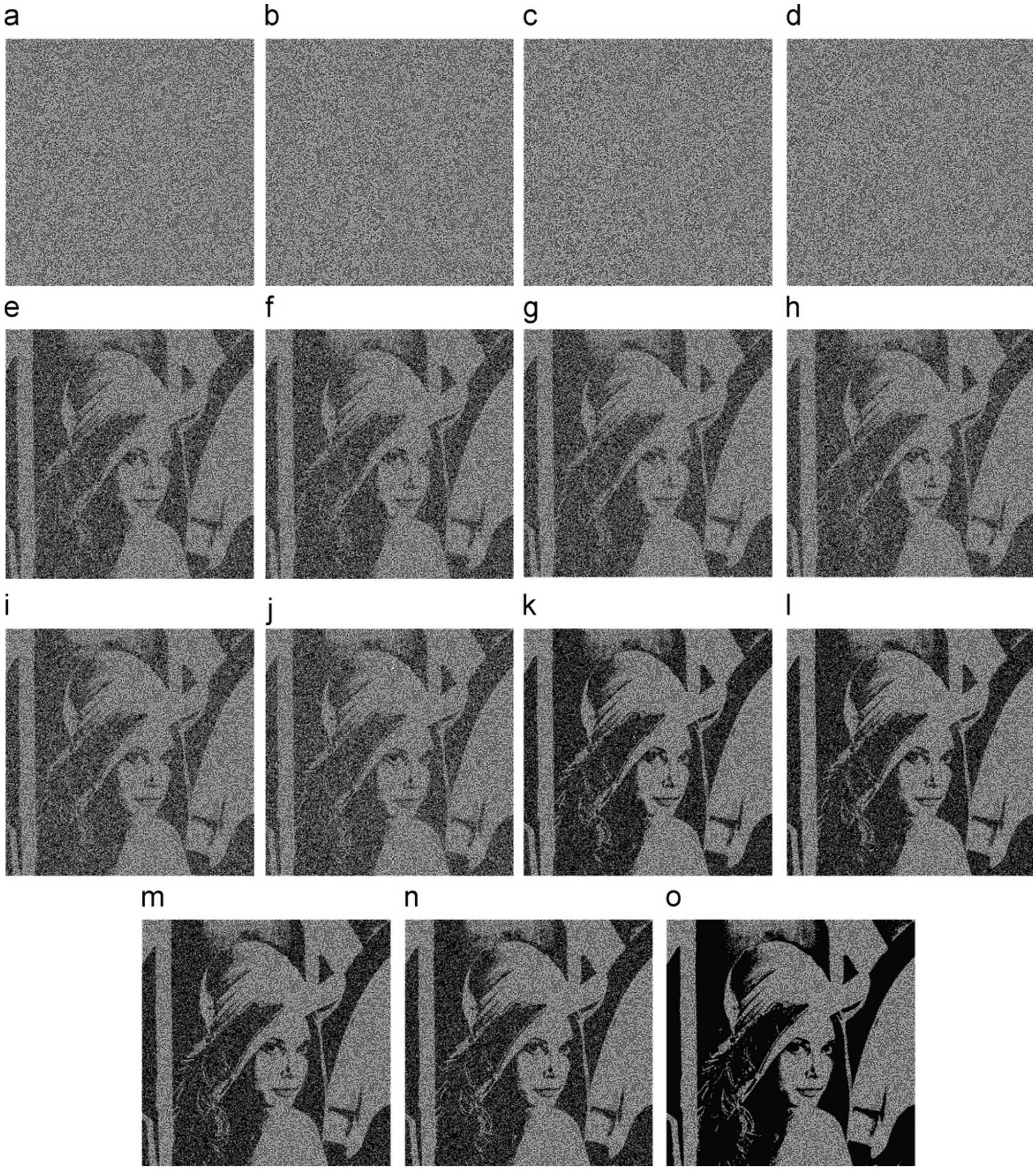

Fig. 4. Experiment of a (2,4) case by the combined method. (a)–(d) Four RGs: R_1, R_2, R_3 and R_4, (e) $R_1 \otimes R_2$, (f) $R_1 \otimes R_3$, (g) $R_1 \otimes R_4$, (h) $R_2 \otimes R_3$, (i) $R_2 \otimes R_4$, (j) $R_3 \otimes R_4$, (k) $R_1 \otimes R_2 \otimes R_3$, (l) $R_1 \otimes R_2 \otimes R_4$, (m) $R_1 \otimes R_3 \otimes R_4$, (n) $R_2 \otimes R_3 \otimes R_4$, (o) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

Table 2
Contrasts and variances of the reconstructed secret images by the combined method for the (2,4) case.

Recovered image	Contrast	Variance				
		$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
$R_1 \otimes R_2$	0.1967	0.6929	0.7021	0.7087	0.6833	0.8024
$R_1 \otimes R_3$	0.1980	0.6964	0.7397	0.7250	0.7107	0.8024
$R_1 \otimes R_4$	0.1979	0.6907	0.7103	0.7016	0.7265	0.8024
$R_2 \otimes R_3$	0.2000	0.6988	0.7328	0.7081	0.6763	0.8024
$R_2 \otimes R_4$	0.1999	0.6946	0.7330	0.6936	0.6896	0.8024
$R_3 \otimes R_4$	0.2012	0.6913	0.7284	0.7119	0.7168	0.8024
$R_1 \otimes R_2 \otimes R_3$	0.3306	0.4074	0.5443	0.6073	0.6107	0.8024
$R_1 \otimes R_2 \otimes R_4$	0.3305	0.4064	0.5306	0.5814	0.6237	0.8024
$R_1 \otimes R_3 \otimes R_4$	0.3321	0.4053	0.5303	0.5980	0.6543	0.8024
$R_2 \otimes R_3 \otimes R_4$	0.3346	0.4046	0.5289	0.5794	0.6186	0.8024
$R_1 \otimes R_2 \otimes R_3 \otimes R_4$	0.4991	0	0.2500	0.4156	0.5218	0.8024

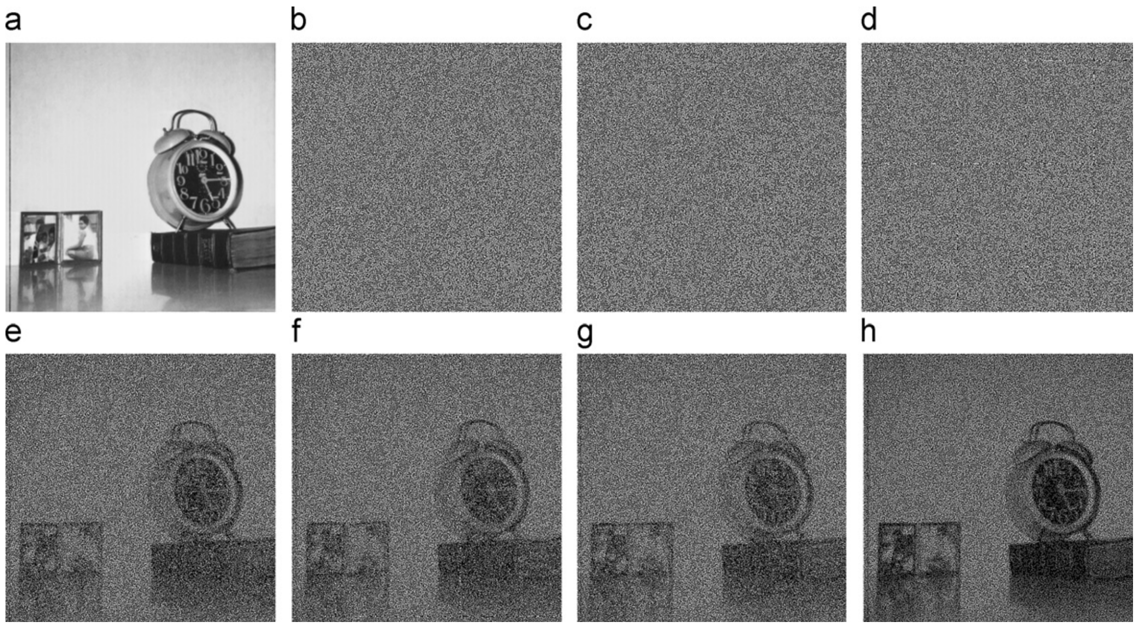

Fig. 5. Experiment of a (2,3) case for grayscale images by the combined method. (a) The grayscale secret image, (b)–(d) three RGs: R_1,R_2 and R_3, (e) $R_1 \otimes R_2$, (f) $R_1 \otimes R_3$, (g) $R_2 \otimes R_3$, (h) $R_1 \otimes R_2 \otimes R_3$.

method) is shown in Fig. 5, where Fig. 5(a) illustrates the grayscale secret image. Three generated RGs are shown in Fig. 5(b)–(d). The stacked results by any two of the three RGs are demonstrated in Fig. 5(e)–(g). And Fig. 5(h) shows the superimposed result of the three RGs.

Another (2,3) case for color images by the combined method is illustrated in Fig. 6. The color secret image and three generated RGs are demonstrated in Fig. 6(a) and (b)–(d), respectively. The stacked results by different combinations of the three RGs are shown in Fig. 6(e)–(h). Any two or more RGs can visually reveal the secret image.

4.5. Comparisons and discussions

4.5.1. Comparisons of theoretical contrast

Theoretical contrast of the recovered secret image by using the contrast-enhanced method can be calculated by Theorem 2. Note that, the VAC-based post-processing do not affect the contrast since the total number of white pixels in area of the reconstructed secret image corresponding to the black (white) area of the original secret image keeps the same. The switching operation in the post-processing just exchanges the positions of pixels within the same area (corresponding to the black or white area of the original secret image) of the RGs. Hence, the contrast by the combined method is the same as that by the contrast-enhanced method.

Comparisons of theoretical contrast for different cases among the proposed contrast-enhanced method, the combined method and related RG-based VSS are demonstrated. For (n,n) case, the contrast-enhanced method and the combined method are reduced to Chen and Tsao's method [28]. Table 3 shows the comparisons of theoretical contrast for the (n,n) case. Note that, there are three contrasts in [26,27] since three different algorithms are

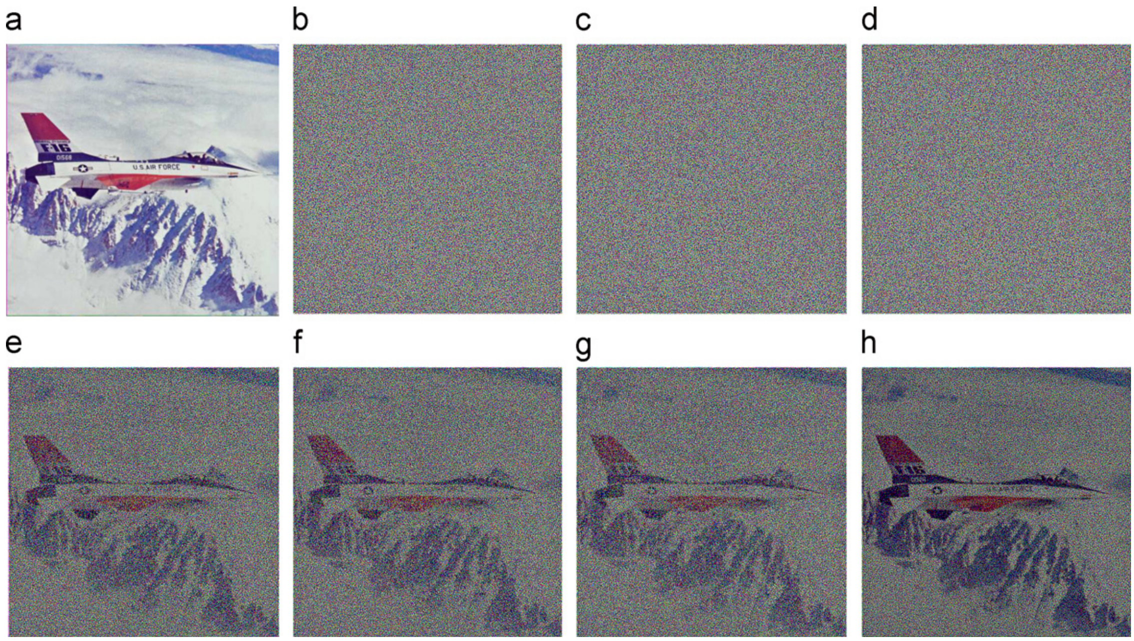

Fig. 6. Experiment of a (2,3) case for color images by the combined method. (a) The color secret image, (b)–(d) three RGs: R_1,R_2 and R_3, (e) $R_1 \otimes R_2$, (f) $R_1 \otimes R_3$, (g) $R_2 \otimes R_3$, (h) $R_1 \otimes R_2 \otimes R_3$. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this article.)

Table 3
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and related methods for the (n,n) case.

Threshold case	Schemes				
	Shyu [26]	Chen and Tsao [27]	Chen and Tsao [28]	Contrast-enhanced method	The combined method
(n,n)	$\frac{1}{2^{(n-1)}}$, $\frac{1}{2^n+1}$, $\frac{1}{2^n}$	$\frac{1}{2^{(n-1)}}$, $\frac{1}{2^n+1}$, $\frac{1}{2^n}$	$\frac{1}{2^{(n-1)}}$	$\frac{1}{2^{(n-1)}}$	$\frac{1}{2^{(n-1)}}$

Table 4
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and related methods for the (2,3) case, where t is the number of stacked RGs.

Scheme	$t=2$	$t=3$
Chen and Tsao [27]	$\frac{1}{5}$	$\frac{1}{3}$
Chen and Tsao [28]	$\frac{1}{7}$	$\frac{1}{4}$
Contrast-enhanced method	$\frac{2}{7}$	$\frac{1}{2}$
The combined method	$\frac{2}{7}$	$\frac{1}{2}$

proposed in their work. Tables 4–6 illustrate the comparisons of theoretical contrast for the cases of (2,3), (2,4) and (2,5), respectively. Similarly, comparisons of contrast for cases of (3,4), (3,5) and (4,5) are provided in Tables 7–9, as well. In general, competitive contrast is achieved by the proposed methods.

Table 5
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and related methods for the (2,4) case, where t is the number of stacked RGs.

Scheme	$t=2$	$t=3$	$t=4$
Chen and Tsao [27]	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{7}{17}$
Chen and Tsao [28]	$\frac{2}{29}$	$\frac{6}{51}$	$\frac{1}{8}$
Contrast-enhanced method	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{2}$
The combined method	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{2}$

Table 6
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and related methods for the (2,5) case, where t is the number of stacked RGs.

Scheme	$t=2$	$t=3$	$t=4$	$t=5$
Chen and Tsao [27]	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{7}{17}$	$\frac{5}{11}$
Chen and Tsao [28]	$\frac{2}{49}$	$\frac{2}{29}$	$\frac{3}{41}$	$\frac{1}{16}$
Contrast-enhanced method	$\frac{2}{13}$	$\frac{6}{23}$	$\frac{4}{11}$	$\frac{1}{2}$
The combined method	$\frac{2}{13}$	$\frac{6}{23}$	$\frac{4}{11}$	$\frac{1}{2}$

Table 7
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and Chen and Tsao's method [28] for the (3,4) case, where t is the number of stacked RGs.

Scheme	$t=3$	$t=4$
Chen and Tsao [28]	$\frac{2}{35}$	$\frac{1}{8}$
Contrast-enhanced method	$\frac{1}{9}$	$\frac{1}{4}$
The combined method	$\frac{1}{9}$	$\frac{1}{4}$

Table 8
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and Chen and Tsao's method [28] for the (3,5) case, where t is the number of stacked RGs.

Scheme	$t=3$	$t=4$	$t=5$
Chen and Tsao [28]	$\frac{1}{44}$	$\frac{4}{83}$	$\frac{1}{16}$
Contrast-enhanced method	$\frac{1}{16}$	$\frac{3}{22}$	$\frac{1}{4}$
The combined method	$\frac{1}{16}$	$\frac{3}{22}$	$\frac{1}{4}$

Table 9
Comparisons of theoretical contrast among the proposed contrast-enhanced method, the combined method and Chen and Tsao's method [28] for the (4,5) case, where t is the number of stacked RGs.

Scheme	$t=4$	$t=5$
Chen and Tsao [28]	$\frac{2}{43}$	$\frac{1}{16}$
Contrast-enhanced method	$\frac{1}{9}$	$\frac{1}{8}$
The combined method	$\frac{1}{9}$	$\frac{1}{8}$

4.5.2. *Comparisons of visual quality via experiments*

Further, illustrations for comparisons of visual quality of the recovered secret image are provided to demonstrate the advantage of the proposed methods. Fig. 7 shows the comparisons of visual quality for the (2,4) case among Chen and Tsao's method [28], contrast-enhanced method and the combined method. The left column (Fig. 7(a), (d) and (g)), middle column (Fig. 7(b), (e) and (h)) and right column (Fig. 7(c), (f) and (i)) are the recovered secret images by using Chen and Tsao's method, the contrast-enhanced method and the combined method, respectively. The associated contrasts and variances calculated from the reconstructed secret images shown in Fig. 7 are demonstrated in Table 10. As shown in Table 10, better contrasts are provided by the proposed methods. Smaller variances are obtained by using the post-processing while comparing to those of the contrast-enhanced method. In other words, more even reconstructed secret images are obtained. To be noticed, the variance by Chen and Tsao's method [28] is relatively

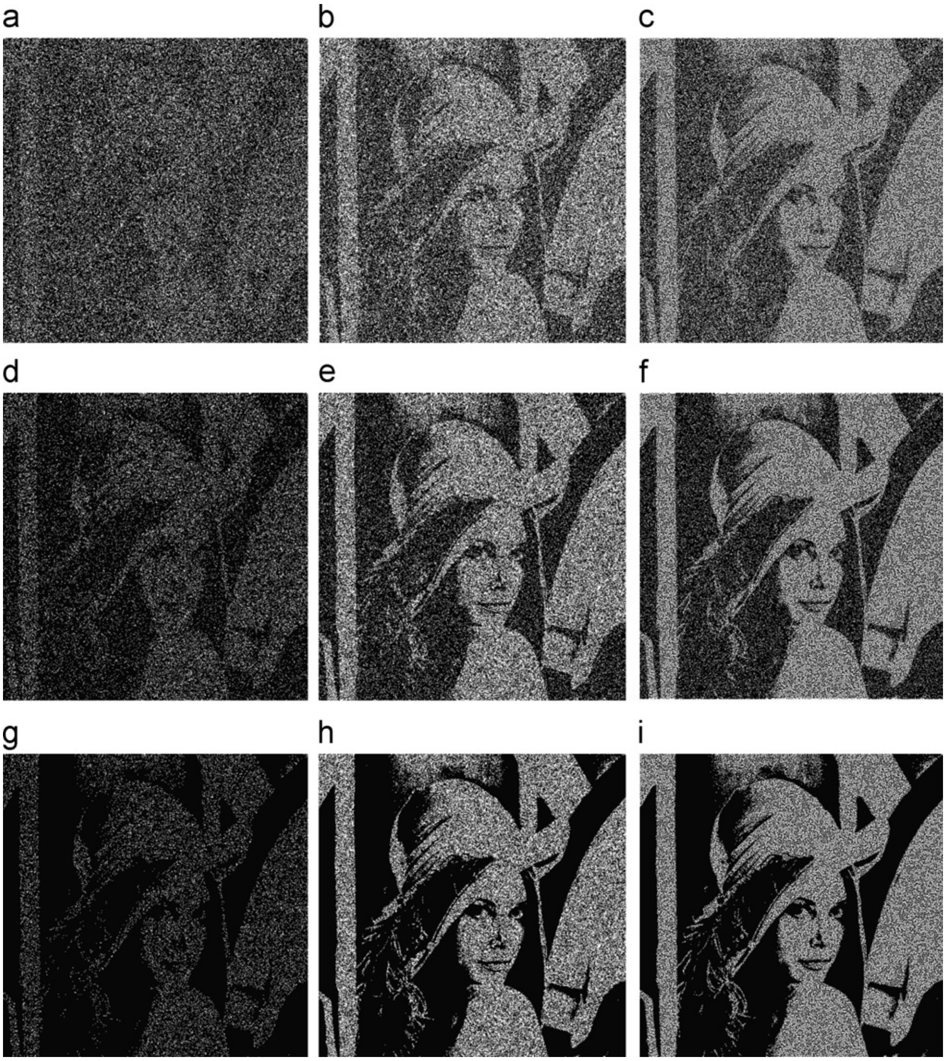

Fig. 7. Comparisons of visual quality of the recovered secret image for a (2,4) case among Chen and Tsao's method [28], the contrast-enhanced method and the combined method. (a), (d), (g) Stacked results of two, three and four RGs by Chen and Tsao's method, respectively, (b), (e), (h) stacked results of two, three and four RGs by contrast-enhanced method, (c), (f), (i) stacked results of two, three and four RGs by the combined method, respectively.

Table 10
Comparisons of contrasts and variances among Chen and Tsao's method [28], the contrast-enhanced method and the combined method for the (2,4) case, where t is the number of stacked RGs.

Methods	t	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [28]	2	0.0655	0.6676	0.6758	0.7761	0.7653	0.8171
	3	0.1156	0.2367	0.3251	0.4465	0.4990	0.5973
	4	0.1231	0	0.1130	0.2163	0.3116	0.4291
Contrast-enhanced method	2	0.1967	0.7677	0.7957	0.8606	0.9291	0.9962
	3	0.3306	0.4408	0.5728	0.7175	0.8380	0.9962
	4	0.4991	0	0.2498	0.5033	0.7291	0.9962
Two proposed methods	2	0.1967	0.6929	0.7021	0.7087	0.6833	0.8024
	3	0.3306	0.4074	0.5443	0.6073	0.6107	0.8024
	4	0.4991	0	0.2500	0.4156	0.5218	0.8024

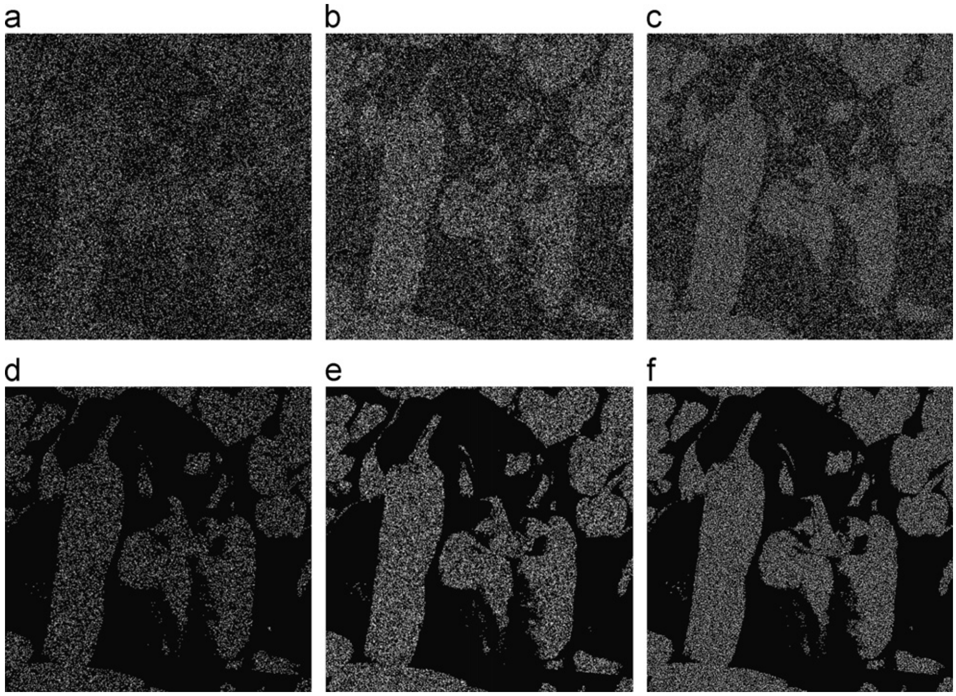

Fig. 8. Comparisons of visual quality of the recovered secret image for a (3,4) case among Chen and Tsao's method [28], the contrast-enhanced method and the combined method. (a), (d) Stacked results of three and four RGs by Chen and Tsao's method, respectively, (b), (e) stacked results of three and four RGs by contrast-enhanced method, (c), (f) stacked results of three and four RGs by the combined method, respectively.

small, since too many black pixels are contained in the reconstructed secret image.

In Table 10, the variance $\sigma_{4,3}$ (0.2498) by the contrast-enhanced method is approximately the same as that (0.2500) by the combined method when four RGs are stacked. Some possible reasons for this special point are described as below.

- The numbers of blocks which contain three, two or one black pixels are small. For the (2,4) case, the number of blocks which contain three black pixels accounts for 2.96% of the total. It is possible that most of these blocks may have been distributed homogeneously before the post-processing is applied since the number is relatively small. As a result, the variance for this type of blocks is not reduced significantly when the post-processing is used.
- The variance does not decrease substantially when more RGs are stacked due to the increasing number of black pixels in the associated reconstructed secret image blocks. When more RGs are superimposed, smaller difference between the contrast-enhanced method and the combined method is obtained. For example, the difference of $\sigma_{4,4}$ between the contrast-enhanced method and the combined method is 0.7677–0.6929 = 0.0748 when two RGs are stacked. But the difference decreases to 0 when four RGs

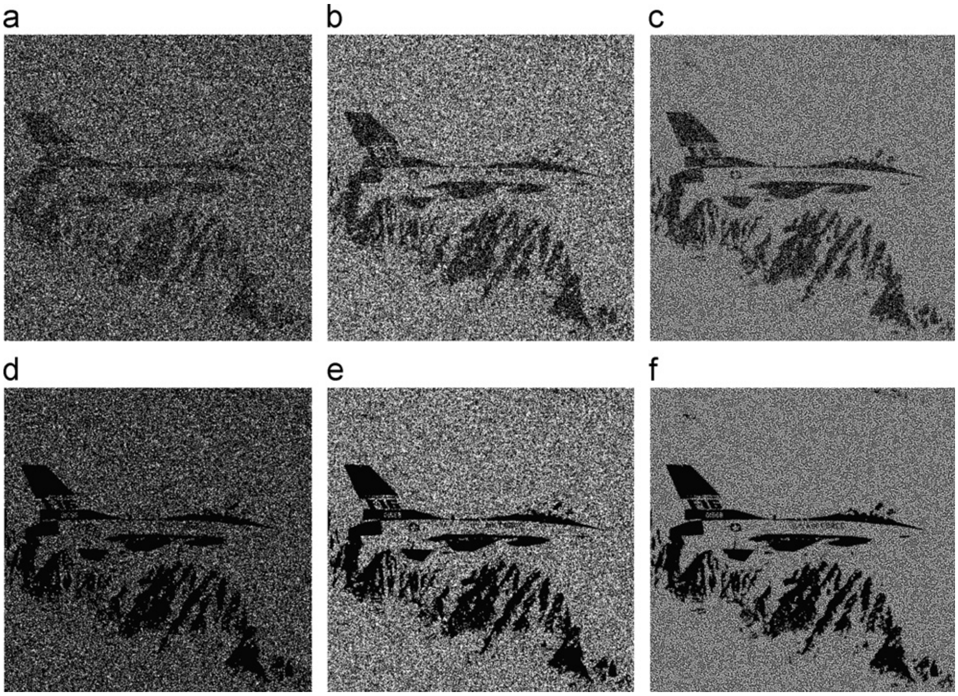

Fig. 9. Comparisons of visual quality of the recovered secret image for a (2,3) case among Chen and Tsao's method [28], the contrast-enhanced method and the combined method. (a), (d) Stacked results of two and three RGs by Chen and Tsao's method, respectively, (b), (e) stacked results of two and three RGs by contrast-enhanced method, (c), (f) stacked results of two and three RGs by the combined method, respectively.

Table 11
Comparisons of contrasts and variances among Chen and Tsao's method [28], the contrast-enhanced method and the combined method for the (3,4) case, where t is the number of stacked RGs.

Methods	t	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [28]	3	0.0591	0.3411	0.3977	0.4328	0.4743	0.5319
	4	0.1261	0	0.1098	0.2078	0.3329	0.4366
Contrast-enhanced method	3	0.1099	0.4407	0.5279	0.6069	0.6664	0.7499
	4	0.2494	0	0.1887	0.3796	0.5465	0.7499
Two proposed methods	3	0.10991	0.4128	0.5151	0.5508	0.5646	0.6071
	4	0.2494	0	0.1855	0.3487	0.4829	0.6071

Table 12
Comparisons of contrasts and variances among Chen and Tsao's method [28], the contrast-enhanced method and the combined method for the (2,3) case, where t is the number of stacked RGs.

Methods	t	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [28]	2	0.1457	0.5511	0.6428	0.7244	0.8366	0.8898
	3	0.2514	0	0.1928	0.3963	0.5590	0.7549
Contrast-enhanced method	2	0.2864	0.5533	0.6509	0.7777	0.8850	0.9950
	3	0.5012	0	0.2500	0.4962	0.7272	0.9950
The combined method	2	0.2864	0.4757	0.5621	0.5807	0.5795	0.7124
	3	0.5012	0	0.2498	0.3737	0.4669	0.7124

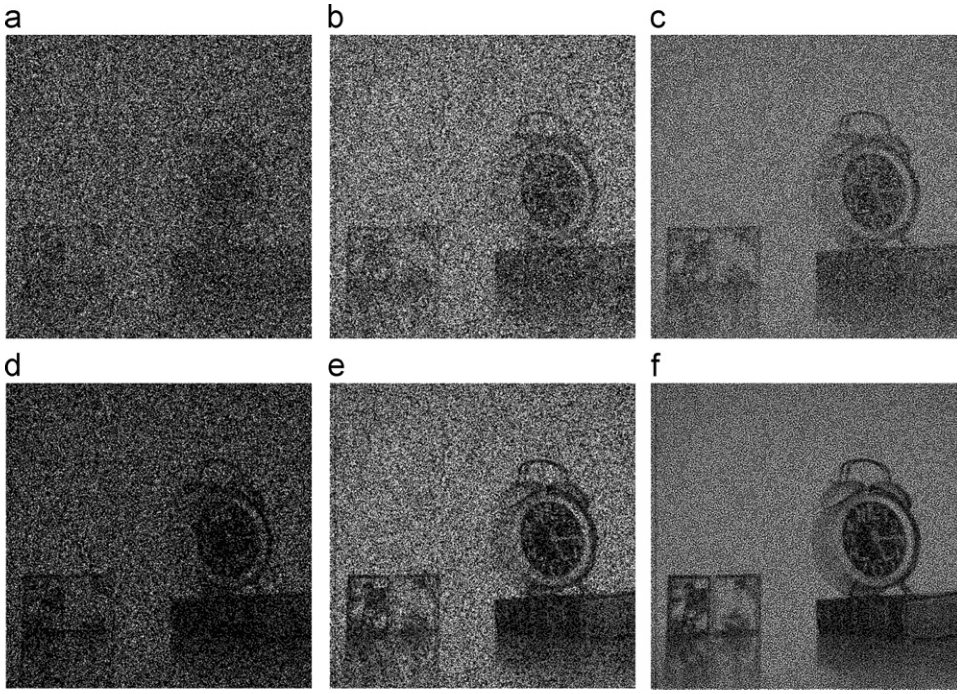

Fig. 10. Comparisons of visual quality of a (2,3) case for grayscale images among Chen and Tsao's method [28], the contrast-enhanced method and the combined method. (a), (d) Stacked results of two and three RGs by Chen and Tsao's method, respectively, (b), (e) stacked results of two and three RGs by contrast-enhanced method, (c), (f) stacked results of two and three RGs by the combined method, respectively.

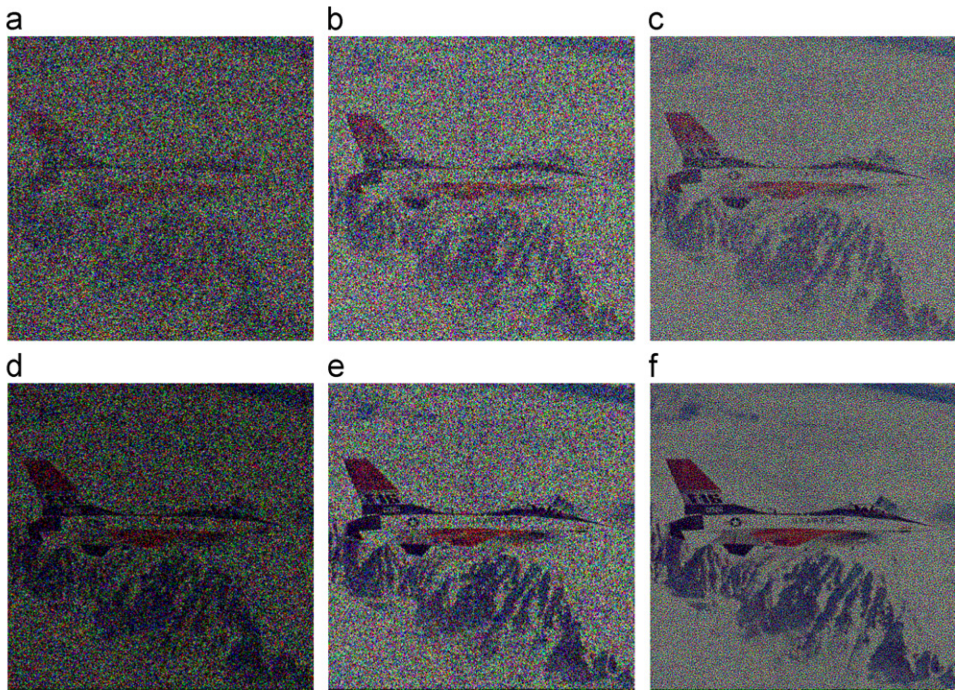

Fig. 11. Comparisons of visual quality of a (2,3) case for color images among Chen and Tsao's method [28], the contrast-enhanced method and the combined method. (a), (d) Stacked results of two and three RGs by Chen and Tsao's method, respectively, (b), (e) stacked results of two and three RGs by contrast-enhanced method, (c), (f) stacked results of two and three RGs by the combined method, respectively. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this article.)

are superimposed. Similar results would possibly appear in the variance $\sigma_{4,3}$. But for variance $\sigma_{4,0}$, the differences maintain the same when more RGs are stacked, since the number of black pixels in the associated reconstructed secret image blocks does not increase.

More visual quality comparisons are provided in Figs. 8 and 9, where Figs. 8 and 9 illustrate the comparisons of visual quality for the (3,4) and (2,3) cases, respectively. Further, the associated contrasts and variances calculated from the recovered secret images of Figs. 8 and 9 are demonstrated in Tables 11 and 12, respectively. The same conclusion still holds for these comparisons.

Extensive comparisons of visual quality for the grayscale and color images are shown in Figs. 10 and 11, respectively. Obviously, better contrast is obtained by the contrast-enhanced method and a more even recovered secret image is achieved by the post-processing. In all, the proposed methods can provide better visual quality of the reconstructed secret image for RG-based VSS.

Finally, it is significant to point out that the variances in the proposed methods are larger than those in Chen and Tsao's method [28], since the contrast is improved by the contrast-enhanced method and brighter reconstructed secret image is achieved by the proposed methods. On the other hand, smaller variances are obtained by darker reconstructed secret image, because more black pixels are contained in the associated reconstructed secret image blocks.

In essence, the visual quality of the reconstructed secret image is evaluated by two parameters: contrast and variance. The contrast is expected to be as large as possible, and the variance is expected to be as small as possible when the same contrast is obtained. Variance comparisons should be conducted when the same contrast is utilized. Obviously, larger contrast is achieved by the contrast-enhanced method. Therefore, better visual quality is provided by the contrast-enhanced approach. Further, smaller variance and the same contrast are achieved by the combined method. Competitive visual quality is obtained by the combined method while comparing to the contrast-enhanced method. In total, the combined method provides the best visual quality.

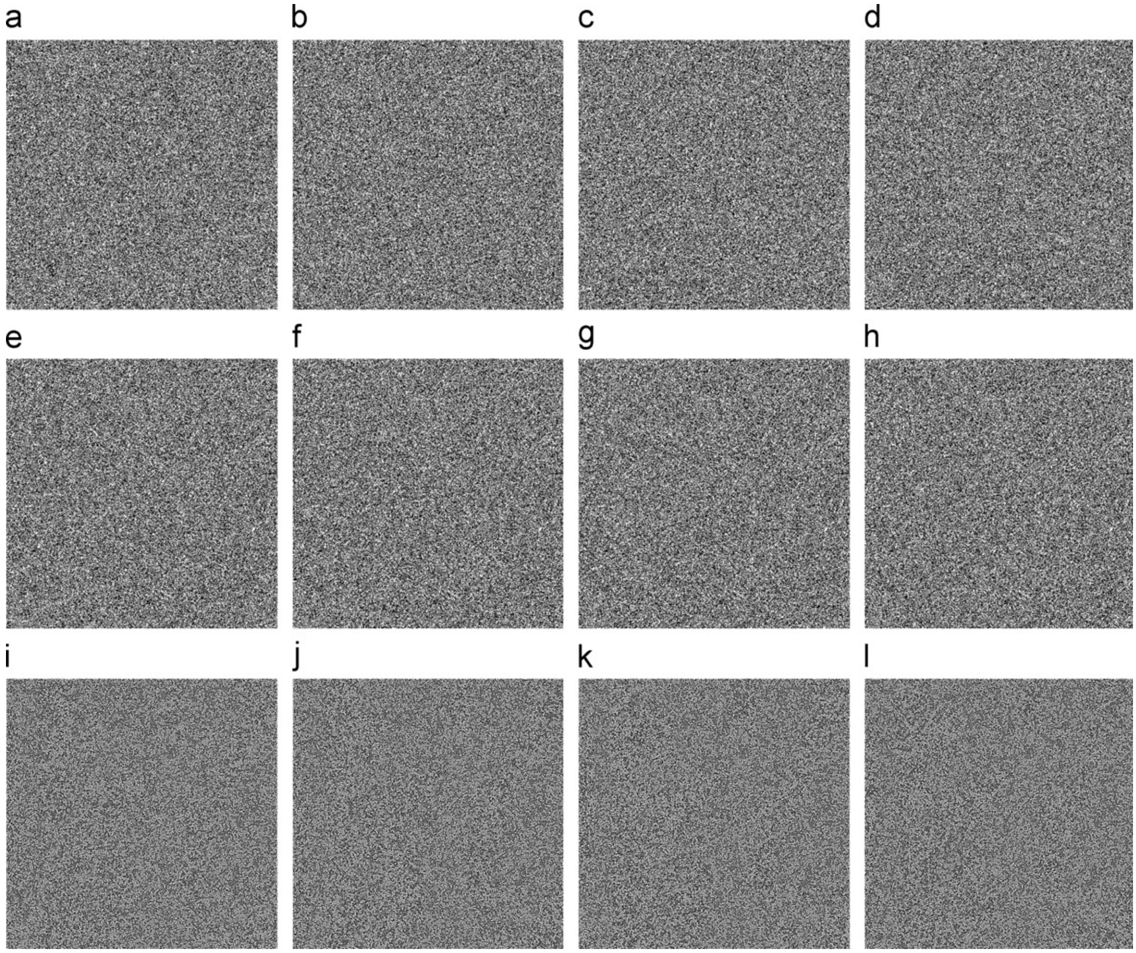

Fig. 12. Comparisons of shares generated by Chen and Tsao's method [28], the contrast-enhanced method and the combined method for the (2,4) case. (a)–(d) Four RGs generated by Chen and Tsao's method, (e)–(h) four RGs generated by the contrast-enhanced method, (i)–(l) four RGs generated by the combined method.

Table 13
Comparisons of contrasts and variances of shares among Chen and Tsao's method [28], the contrast-enhanced method and the combined method for the (2,4) case.

Methods	Shares	Contrast	Variance				
			$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
Chen and Tsao's method [28]	R1	0.0006	64 562	62 450	65 368	64 431	65 451
	R_2	0.0013	64 674	67 239	66 677	63 109	64 090
	R_3	0.0018	65 107	67 155	68 703	66 208	65 014
	R_4	0.0001	64 754	65 427	68 002	63 053	65 008
Contrast-enhanced method	R1	0.0013	64 942	61 640	65 100	63 642	64 780
	R_2	0.0008	64 946	64 454	65 523	65 154	64 780
	R_3	0.0008	64 150	65 441	65 667	64 164	64 780
	R_4	0.0007	64 561	64 889	66 811	64 802	64 780
The combined method	R1	0.0013	57 289	56 850	53 613	49 050	52 179
	R_2	0.0008	57 397	56 782	53 581	48 077	52 179
	R_3	0.0008	59 113	57 653	53 472	50 440	52 179
	R_4	0.0007	57 183	58 010	52 070	50 541	52 179

4.5.3. Comparisons of the RGs

It is also desired to compare the shares generated by Chen and Tsao's method [28] and by the proposed methods. Fig. 12 illustrates the comparisons of shares for the (2,4) case. The first, second and third rows of Fig. 12 are the four RGs generated by Chen and Tsao's method [28], the contrast-enhanced method and the combined method. The corresponding contrasts and variances of these shares are demonstrated in Table 13. As shown in Fig. 12 and Table 13, the shares generated by Chen and Tsao's method are similar to those by the contrast-enhanced method. However, more even shares are constructed after the post-processing since smaller variances are obtained.

5. Conclusions

This paper introduces two methods, a contrast-enhanced RG-based VSS and a VAC-based post-processing, to further improve the visual quality of reconstructed secret image in VSS. More specifically, optimal contrast is achieved by the contrast-enhanced RG-based VSS and a more even reconstructed secret image can be obtained by applying the VAC-based post-processing. Moreover, the post-processing algorithm can be used not only in RG-based VSS but also in size invariant probabilistic VSS for constructing a more even revealed secret image.

Acknowledgment

This work was partially supported by the 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] X. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator, Signal Processing 89 (4) (2009) 480–491.
[2] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Processing 90 (9) (2010) 2714–2722.
[3] W. Xingyuan, T. Lin, Q. Xue, A novel colour image encryption algorithm based on chaos, Signal Processing 92 (4) (2012) 1101–1108.
[4] P. Tsai, Y. Hu, H. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89 (6) (2009) 1129–1143.
[5] X. Gao, L. An, X. Li, D. Tao, Reversibility improved lossless data hiding, Signal Processing 89 (10) (2009) 2053–2065.
[6] W. Hong, T. Chen, Y. Chang, C. Shiu, A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification, Signal Processing 90 (11) (2010) 2911–2922.
[7] P. Tsai, Y. Hu, C. Chang, A color image watermarking scheme based on color quantization, Signal Processing 84 (1) (2004) 95–106.
[8] A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Processing 88 (9) (2008) 2158–2180.
[9] M. Naor, A. Shamir, Visual cryptography, in: Lecture Notes in Computer Science, vol. 950(1), 1995, pp. 1–12.
[10] G. Ateniese, C. Blundo, A. De Santis, D. Stinson, Visual cryptography for general access structures, Information and Computation 129 (2) (1996) 86–106.
[11] F. Liu, C. Wu, X. Lin, Step construction of visual cryptography schemes, IEEE Transactions on Information Forensics and Security 5 (1) (2010) 27–38.
[12] G. Ateniese, C. Blundo, A. Santis, D. Stinson, Extended capabilities for visual cryptography, Theoretical Computer Science 250 (1–2) (2001) 143–161.
[13] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Transactions on Information Forensics and Security 6 (2) (2011) 307–322.
[14] Z. Zhou, G. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Transactions on Image Processing 15 (8) (2006) 2441–2453.
[15] Z. Wang, G. Arce, G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Transactions on Information Forensics and Security 4 (3) (2009) 383–396.
[16] C. Lin, W. Tsai, Visual cryptography for gray-level images by dithering techniques, Pattern Recognition Letters 24 (1–3) (2003) 349–358.
[17] Y. Hou, Visual cryptography for color images, Pattern Recognition 36 (7) (2003) 1619–1629.
[18] S. Cimato, R. De Prisco, A. De Santis, Colored visual cryptography without color darkening, Theoretical Computer Science 374 (1–3) (2007) 261–276.
[19] I. Kang, G. Arce, H. Lee, Color extended visual cryptography using error diffusion, IEEE Transactions on Image Processing 20 (1) (2011) 132–145.

[20] C. Yang, A. Peng, T. Chen, MTVSS: (M)isalignment (T)olerant (V)isual (S)ecret (S)haring on resolving alignment difficulty, Signal Processing 89 (8) (2009) 1602–1624.
[21] R. Ito, H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 82 (10) (1999) 2172–2177.
[22] C. Yang, New visual secret sharing using probabilistic method, Pattern Recognition Letters 25 (4) (2004) 481–494.
[23] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, The Computer Journal 49 (1) (2006) 97–107.
[24] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Optics Letters 12 (6) (1987) 377–379.
[25] S. Shyu, Image encryption by random grids, Pattern Recognition 40 (3) (2007) 1014–1031.
[26] S. Shyu, Image encryption by multiple random grids, Pattern Recognition 42 (7) (2009) 1582–1596.
[27] T. Chen, K. Tsao, Visual secret sharing by random grids revisited, Pattern Recognition 42 (9) (2009) 2203–2217.
[28] T. Chen, K. Tsao, Threshold visual secret sharing by random grids, Journal of Systems and Software 84 (2011) 1197–1208.
[29] Y. Lee, T. Chen, Insight into collusion attacks in random-grid-based visual secret sharing, Signal Processing 92 (3) (2012) 727–736.
[30] T. Chen, K. Tsao, Y. Lee, Yet another multiple-image encryption by rotating random grids, Signal Processing 92 (9) (2012) 2229–2237.
[31] R. Ulichney, Void-and-cluster method for dither array generation, in: Proceedings of SPIE, vol. 1913, 1993, pp. 332–343.
[32] F. Liu, T. Tuo, C. Wu, L. Qian, Improving the visual quality of size invariant visual cryptography scheme, Journal of Visual Communication and Image Representation 23 (2012) 331–342.
[33] Y. Hou, S. Tu, A visual cryptographic technique for chromatic images using multi-pixel encoding method, Journal of Research and Practice in Information Technology 37 (2) (2005) 179–192.