J. Vis. Commun. Image R. 24 (2013) 552–566

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

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

Improving the visual quality of random grid-based visual secret sharing via error diffusion

Xiaotian Wu [a], Tong Liu [b], Wei Sun [c,*]

[a] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
[b] Department of Audio-Visual and Image Technology, China Criminal Police University, Shenyang 110854, China
[c] School of Software, Sun Yat-sen University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 1 April 2012
Accepted 4 March 2013
Available online 15 March 2013

Keywords:
Visual secret sharing
Visual cryptography
Visual quality
Random grid
Error diffusion
Noise balanced
Homogeneous distribution
Pixel expansion

ABSTRACT

Random grid (RG) is an approach to implement visual secret sharing (VSS) without pixel expansion. However, visual quality of the recovered secret image in RG-based VSS is not satisfactory. In this paper, two methodologies are introduced for improving image quality. Firstly, a random noise balanced error diffusion (RNBED) algorithm is proposed for generating RGs whose black pixels are distributed homogeneously. By combining the proposed RNBED algorithm and existing RG-based VSS schemes, two approaches for enhancing the recovered image quality are presented. Experimental results are provided, illustrating that competitive visual quality is achieved.

1. Introduction

Visual secret sharing (VSS) is a cryptographic paradigm that encrypts a secret image into random-looking images (called shares or shadows) and decrypts the secret by stacking sufficient shares together. The aim of VSS is to protect a secret among a group of participants with threshold mechanism.

The initial concept of VSS was introduced by Naor and Shamir [1], where a binary secret image is encrypted into n random-looking shares in a (k, n) scheme, and the shares are delivered to n associated participants. The secret image can be recovered visually by stacking any k or more shares together, whereas any $k-1$ or less shares give no clue about the secret. Note that, VSS is an excellent solution for sharing secret images when computational devices are not available. Based on Naor and Shamir's pioneer work [1], different studies on VSS were widely investigated. To provide more flexible sharing strategy, VSS schemes for general access structures were introduced [2,3]. For the aim of increasing the hiding capacity, multi-secret VSS methods were presented [4,5]. To obtain meaningful shares for solving the management problem and removing the suspicion of secret image encryption, extended VSS [3,6] and halftone VSS [7,8] were proposed. However, pixel expansion problem still remains in the above-mentioned VSS schemes, where pixel expansion indicates that each generated share is $m \geqslant 2$ times as big as the original secret image. When the number of shares increases, pixel expansion problem becomes more serious. In this case, it further burdens the share transmission and storage.

Probabilistic VSS, a significant branch of VSS, was proposed to deal with the pixel expansion problem. Ito et al. [9] introduced an image size invariant VSS method, where a black (resp. white) secret pixel is encoded by a column selected from the corresponding black (resp. white) basis matrix. Yang [10] also proposed a probabilistic model for constructing VSS without pixel expansion. Different threshold VSS schemes are investigated. Further, a generalization of Yang's model [10] was introduced by Cimato et al. [11]. For big enough value of pixel expansion m, their model reduces to the classical deterministic model. For $m = 1$, their model reduces to one of Yang's methods. But in probabilistic VSS, code book is still required to construct the shares in the encryption phase. Sometimes, designing such a code book is not trivial.

Random grid (RG) is an alternative approach that can generate size invariant shares. Advanced merit of RG-based VSS, while comparing to probabilistic VSS, is that code book is not required in the encryption phase. The basic concept of RG was first proposed by Kafri and Keren [12]. Also, three algorithms for encoding a binary secret image into two RGs were presented. Inspired by Kafri and Keren, Shyu [13] introduced enhanced methods to encrypt

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

1047-3203/$ - see front matter © 2013 Published by Elsevier Inc.
http://dx.doi.org/10.1016/j.jvcir.2013.03.002

grayscale and color images in 2007. The same author [14] also proposed a methodology to implement (n,n) RG-based VSS. Chen and Tsao [15] introduced algorithms to construct VSS for $(2,n)$ and (n,n) cases by RGs. Recently, the same authors proposed a (k,n) threshold VSS by RGs [16]. However, both the reported probabilistic VSS and RG-based VSS solve the pixel expansion problem at the expense of sacrificing the visual quality of the reconstructed secret image.

In this paper, two approaches for improving the recovered image quality of RG-based VSS are proposed. The concept of random noise balanced error diffusion (RNBED) is introduced to generate homogeneous distribution of black pixels on the RGs. By combining the RNBED algorithm and reported RG-based VSS [15,16], two methods with improved image quality for $(2,n)$ and (k,n) RG-based VSS are presented.

The remaining part of this paper is organized as follows. Section 2 describes RG-based VSS schemes for $(2,n)$ and (k,n) cases, as well as the error diffusion algorithm. Two proposed methods for improving the visual quality are formulated in Section 3. Experimental results and discussions are illustrated in Section 4. Section 5 concludes our work.

2. Preliminaries

2.1. RG-based VSS

A RG is defined as a transparency consisting of a two-dimensional array of pixels [12]. 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.

Three different RG-based VSS algorithms for (2,2) case were first introduced by Kafri and Keren [12]. Based on Kafri and Keren's work, VSS schemes [14–16] for different thresholds were presented. Herein, the $(2,n)$ and (k,n) RG-based VSS schemes are briefly described. In the $(2,n)$ (resp. (k,n)) case, a secret image S is encrypted into n RGs $R_1,\ldots,R_n$, where any two (resp. k) or more RGs can visually reveal the secret. Let $\otimes$ denote the Boolean OR operation, the stacked result of k RGs $R_{i_1},\ldots,R_{i_k}$ is represented by $R_{i_1}\otimes\cdots\otimes R_{i_k}$. In addition, digit 0 denotes a white pixel and digit 1 denotes a black pixel in this paper. Algorithms of the $(2,n)$ [15] and (k,n) [16] RG-based VSS are formulated as follows.

RG-based (2,n) threshold VSS
Input: A $M\times N$ binary secret image S.
Output: n RGs $R_1,\ldots,R_n$.
Step 1: For each position $(i,j)\in\{(i,j)|1\leqslant i\leqslant M,1\leqslant j\leqslant N\}$, Step 2 or Step 3 is performed based on the color of $S(i,j)$.
Step 2: If $S(i,j)=1$, n numbers $d_1,\ldots,d_n$ are randomly selected from $\{0,1\}$. The n shared pixels $R_1(i,j),\ldots,R_n(i,j)$ are constructed by

$$R_1(i,j)=d_1,\ldots,R_n(i,j)=d_n.$$

Step 3: If $S(i,j)=0$, a number d is randomly selected from $\{0,1\}$. The n shared pixels $R_1(i,j),\ldots,R_n(i,j)$ are constructed by

$$R_1(i,j)=\cdots=R_n(i,j)=d.$$

Step 4: Output the n RGs $R_1,\ldots,R_n$.

RG-based (k,n) threshold VSS
Input: A $M\times N$ binary secret image S.
Output: n RGs $R_1,\ldots,R_n$.
Step 1: For each position $(i,j)\in\{(i,j)|1\leqslant i\leqslant M,1\leqslant j\leqslant N\}$, 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 kth 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 $(k+1\leqslant v\leqslant n)$ by randomly assigning value 0 or 1 to b_v.
Step 5: Randomly assign the n bits $b_1,\ldots,b_n$ to n shared pixels $R_1(i,j),\ldots,R_n(i,j)$.
Step 6: Output the n RGs $R_1,\ldots,R_n$.

In order to formally analyze the properties, the following notations and definitions on RG are given, partially borrowed from [13,15].

Definition 1 (*Average light transmission [13,15]*). 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 [13]*). 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 [13]*). 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

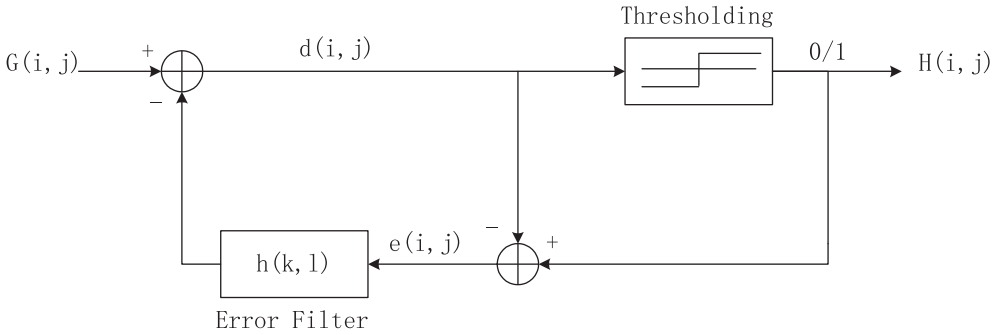

Fig. 1. Diagram of the typical error diffusion algorithm.

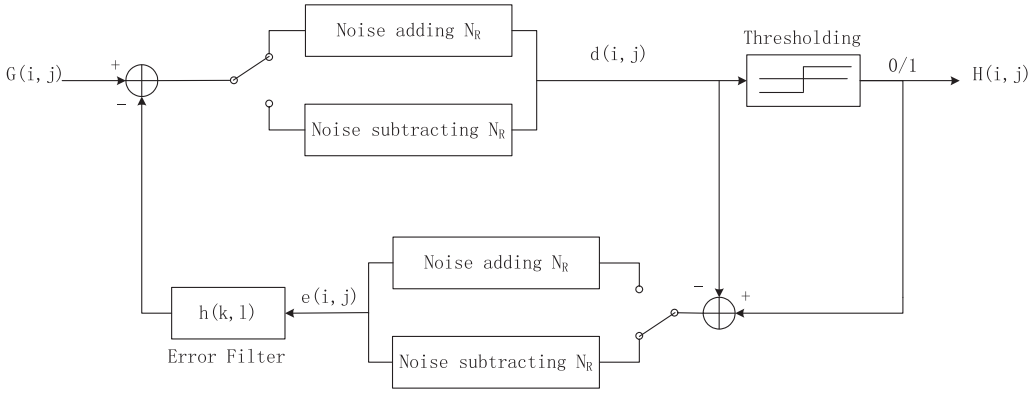

Fig. 2. Diagram of the proposed random noise balanced error diffusion algorithm.

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

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

Definition 4 (*Visual recognition [15]*). 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 $\alpha = 0$.

2.2. Error diffusion

Error diffusion [17] is a commonly used halftoning technique that transforms a continuous-tone image into binary. The conceptual diagram of error diffusion is shown in Fig. 1.

$G(i,j)$ represents the pixel value in position (i,j) of the input multi-tone image. $d(i,j)$ denotes the sum of the input pixel value and the diffused errors from the neighboring processed pixels. $H(i,j)$ is the quantized output pixel whose value is 0 or 1 [18,19]. In general, error diffusion algorithm can be divided into two components: (1) the thresholding block and (2) the error filtering block. In the thresholding block, the output $H(i,j)$ is calculated by

$$H(i,j) = \begin{cases} 1, & \text{if} \quad d(i,j) \geqslant 0.5, \\ 0, & \text{otherwise}. \end{cases} \tag{1}$$

In the error filtering block, the input $e(i,j)$ indicates the difference between $d(i,j)$ and $H(i,j)$, as calculated by

$$e(i,j) = d(i,j) - H(i,j). \tag{2}$$

$d(i,j)$ is computed by

$$d(i,j) = G(i,j) - \sum_{k,l} f(k,l)e(i-k,j-l) \tag{3}$$

where $f(k,l) \in F$ and F denotes a two dimensional error filter. A widely used filter proposed by Floyd and Steinberg [17] is

$$f(k,l) = \frac{1}{16} \times \begin{bmatrix} & C & 7 \\ 3 & 5 & 1 \end{bmatrix} \tag{4}$$

where C denotes the current processing pixel. The weights of the error filter are $f(0,1) = \frac{7}{16}, f(1,-1) = \frac{3}{16}, f(1,0) = \frac{5}{16}$ and $f(1,1) = \frac{1}{16}$.

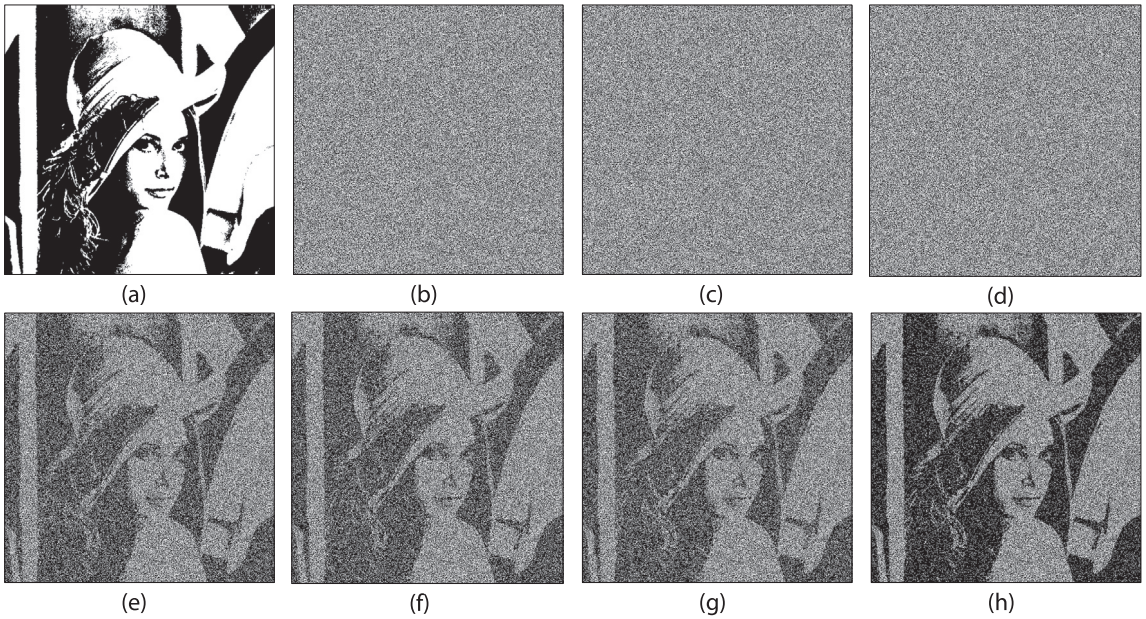

Fig. 3. A $(2,3)$ case by the proposed $(2,n)$ VSS scheme. (a) The secret image, (b)–(d) three RGs R_1, R_2 and R_3, (e) $R_1 \otimes R_2$, (f) $R_1 \otimes R_3$, (g) $R_2 \otimes R_3$, and (h) $R_1 \otimes R_2 \otimes R_3$.

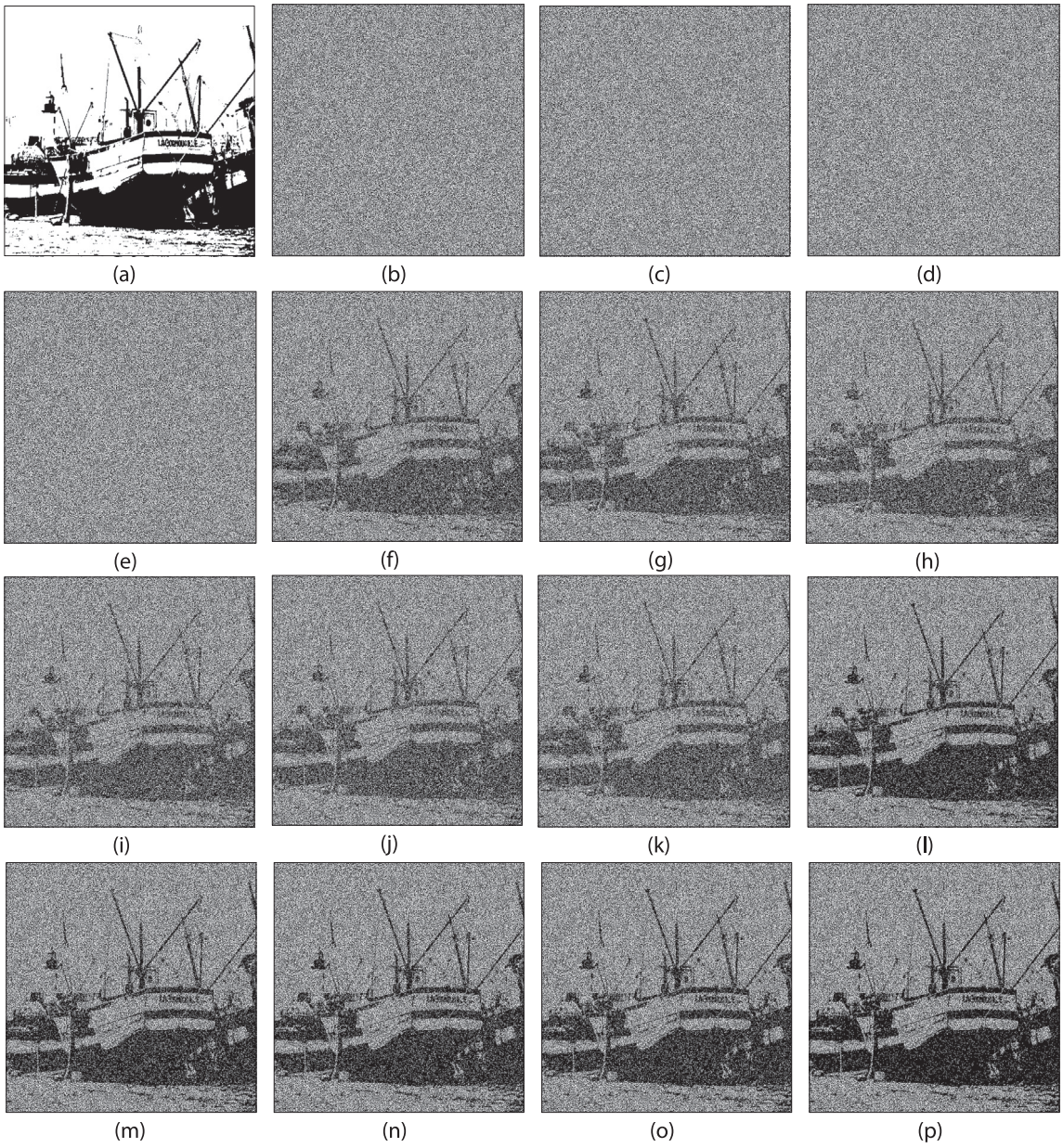

Fig. 4. A $(2,4)$ case by the proposed $(2n)$ VSS scheme. (a) The secret image, (b)–(e) four RGs R_1, R_2, R_3 and R_4, (f) $R_1 \otimes R_2$, (g) $R_1 \otimes R_3$, (h) $R_1 \otimes R_4$, (i) $R_2 \otimes R_3$, (j) $R_2 \otimes R_4$, (k) $R_3 \otimes R_4$, (l) $R1 \otimes R_2 \otimes R_3$, (m) $R1 \otimes R_2 \otimes R_4$, (n) $R1 \otimes R_3 \otimes R_4$, (o) $R2 \otimes R_3 \otimes R_4$, and (p) $R1 \otimes R_2 \otimes R_3 \otimes R_4$.

3. The proposed methods

In this section, RG-based VSS schemes for $(2,n)$ and (k,n) cases with competitive recovered image quality are presented.

3.1. Variance

In reported RG-based VSS, the recovered image quality is only evaluated by the average contrast. However, the evenness of the recovered image affects the image quality as well. Method for evaluating the evenness of the recovered image is ignored in existing RG-based VSS. Herein, variance of the darkness levels of a block is introduced to evaluate the evenness of recovered secret image, where Hou and Tu [20] and Liu et al. [21] 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

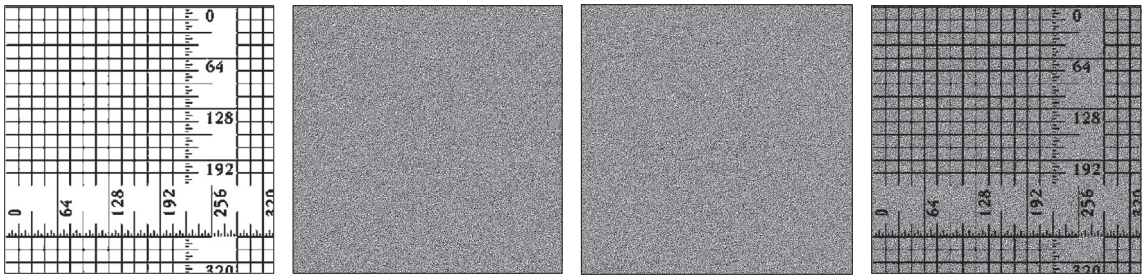

Fig. 5. A (2,2) case by the proposed (k,n) VSS scheme. (a) The secret image, (b) and (c) two RGs R_1 and R_2, and (d) $R_1 \otimes R_2$.

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

With a small variance, a more even recovered secret image is obtained. For achieving competitive visual quality, variance is expected to be as small as possible.

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.

3.2. RNBED algorithm

The visual quality of the recovered image in existing RG-based VSS is not satisfactory due to the random distribution of black pixels in the reconstructed secret image. The random distribution may lead to a consequence that the black pixels cluster together. These clustered black pixels further reduce the evenness of the reconstructed secret image and deteriorate the image quality. To achieve pleasing visual quality, those reconstructed black pixels are suggested to be distributed homogeneously and separated maximally from each other.

Our strategy to obtain homogeneous distribution of recovered black pixels is to generate RGs whose black pixels are homogeneously distributed. A random noise balanced error diffusion (RNBED) is proposed to achieve this goal. Diagram of the proposed RNBED algorithm is illustrated in Fig. 2. The proposed RNBED algorithm is similar to typical error diffusion. Usually, a grayscale image G is considered as the input and a halftone image H is constructed via RNBED algorithm. To guarantee that the generated halftone image H is a RG (the number of black pixels is approximately the same as the number of white pixels), the average gray-level of the image G should be 0.5. The noise N_R is fixed in advance. Further, whether the noise N_R is added or subtracted is randomly determined in every position. If N_R is added, $d(i,j)$ is calculated by

$$d(i,j) = G(i,j) - \sum_{k,l} f(k,l)e(i-k,j-l) + N_R, \tag{5}$$

and $e(i,j)$ is computed by

$$e(i,j) = d(i,j) - H(i,j) - N_R. \tag{6}$$

If N_R is subtracted, then $d(i,j)$ and $e(i,j)$ are calculated by

$$d(i,j) = G(i,j) - \sum_{k,l} f(k,l)e(i-k,j-l) - N_R, \tag{7}$$

and

$$e(i,j) = d(i,j) - H(i,j) + N_R, \tag{8}$$

respectively. The generated halftone pixel $H(i,j)$ is generated by

$$H(i,j) = \begin{cases} 1, & \text{if} \quad d(i,j) \geqslant 0.5, \\ 0, & \text{otherwise}. \end{cases} \tag{9}$$

The proposed RNBED algorithm adopts the error diffusion mechanism for making sure that the generated black halftone pixels are distributed homogeneously and separated maximally from each other. Quantization error in error diffusion algorithm depends not only on the current input and output but also on the entire past history. The error filter is designed in such a way that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or blue noise in nature, leading to visually pleasing halftone images for human vision [18,19].

In addition, according to typical error diffusion, the same halftone image is constructed when the same grayscale image is considered as the input. The halftone pixels are determined. But in RG-based VSS, the shared pixels should be unpredictable to guarantee the security condition. The purpose of adding/subtracting the noise N_R randomly is to ensure that the value of each halftone pixel remains unpredictable even if the same grayscale image is used.

3.3. The proposed RG-based VSS algorithms

By adopting the proposed RNBED algorithm, RG-based VSS schemes for improving the visual quality are presented, as described as follows.

RG-based (2,n) VSS with competitive visual quality
Input: A $M \times N$ binary secret image S and six parameters $u, N_0, N_1, \ldots, N_4$.
Output: n RGs $R_1, \ldots, R_n$.
Step 1: The secret image is divided into non-overlapping blocks whose size is 2×2. All the blocks are classified into five types $B_{4,0}, \ldots, B_{4,4}$.
Step 2: Construct n images $G_1, \ldots, G_n$, where each element in the images is randomly selected from the interval $[0.5 - u, 0.5 + u]$.
Step 3: Each pixel in the secret image is processed by Steps 4–8 in roast-scan order. Denote the current processing pixel as $S(i,j)$, where $1 \leqslant i \leqslant M$ and $1 \leqslant j \leqslant N$.
Step 4: Let B be the non-overlapping block that contains the current processing pixel. The noise N_R is determined by

$$N_R = N_b, \quad \text{if} \quad B \in B_{4,b}$$

where $0 \leqslant b \leqslant 4$.
Step 5: Generate n halftone pixels $R_1(i,j), \ldots, R_n(i,j)$ according to the color of $S(i,j)$ by Step 6 or Step 7.

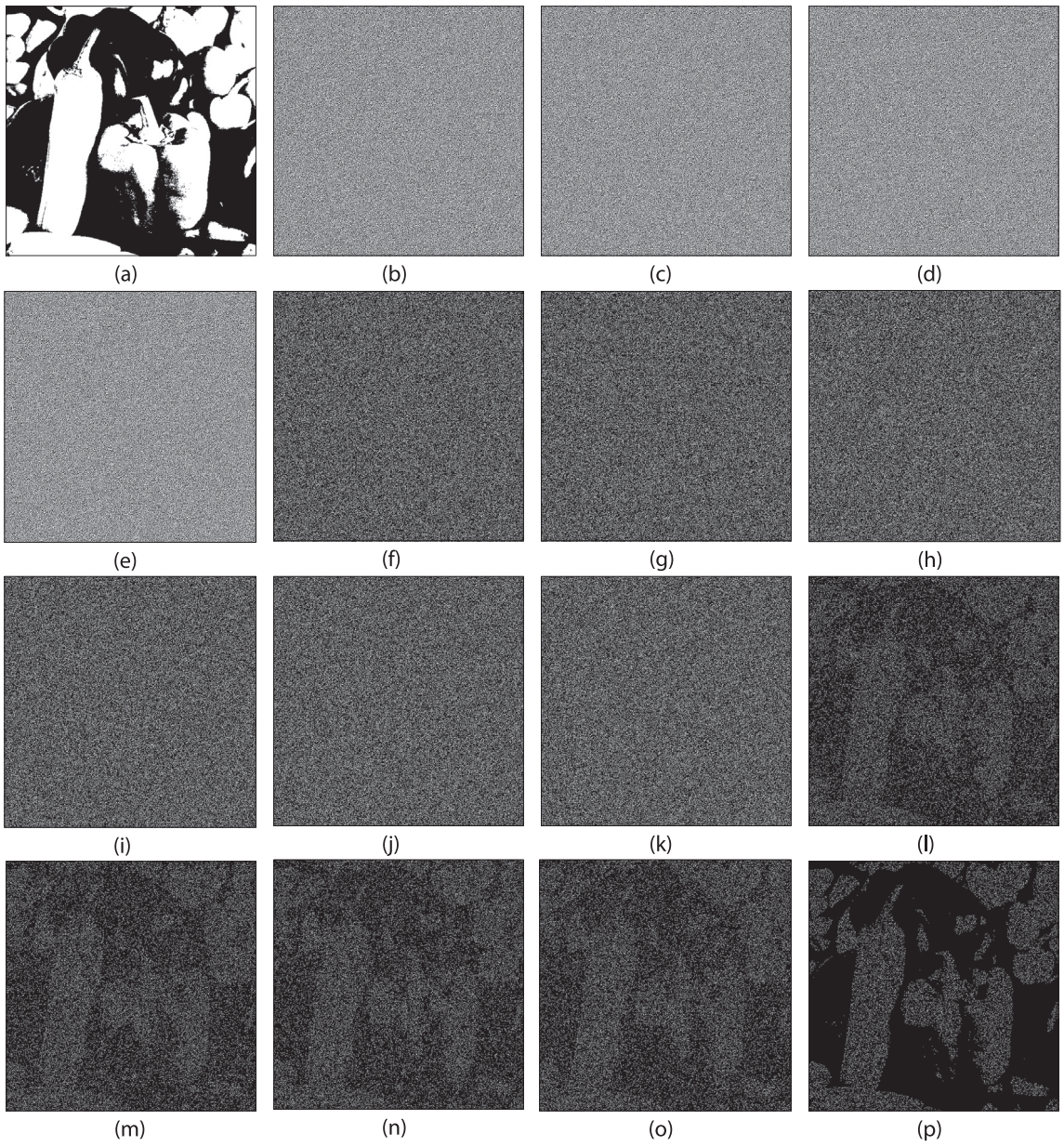

Fig. 6. A (3,4) case by the proposed (k,n) VSS scheme. (a) The secret image, (b)–(e) four RGs R_1, R_2, R_3 and R_4, (f) $R_1 \otimes R_2$, (g) $R_1 \otimes R_3$, (h) $R_1 \otimes R_4$, (i) $R_2 \otimes R_3$, (j) $R_2 \otimes R_4$, (k) $R_3 \otimes R_4$, (l) $R1 \otimes R_2 \otimes R_3$, (m) $R1 \otimes R_2 \otimes R_4$, (n) $R1 \otimes R_3 \otimes R_4$, (o) $R2 \otimes R_3 \otimes R_4$, and (p) $R1 \otimes R_2 \otimes R_3 \otimes R_4$.

Step 6: If $S(i,j) = 1$, the n pixels $G_1(i,j), \ldots, G_n(i,j)$ are processed by the proposed RNBED algorithm with noise N_R, and n halftone pixels $R_1(i,j), \ldots, R_n(i,j)$ are generated.
Step 7: If $S(i,j) = 0$, a number d is randomly selected from $\{1, \ldots, n\}$. The corresponding pixel $G_d(i,j)$ is processed by the proposed RNBED algorithm with noise N_R, and the halftone pixel $R_d(i,j)$ is obtained. The rest $n-1$ halftone pixels are assigned the value of $R_d(i,j)$.
Step 8: The quantization errors are calculated and diffused to the neighboring unprocessed pixels.
Step 9: Output the n RGs $R_1, \ldots, R_n$.

RG-based (k,n) VSS with competitive visual quality
Input: A $M \times N$ binary secret image S and six parameters $u, N_0, N_1, \ldots, N_4$.
Output: n RGs $R_1, \ldots, R_n$.
Step 1: The secret image is divided into non-overlapping blocks whose size is 2×2. All the blocks are classified into five types $B_{4,0}, \ldots, B_{4,4}$.
Step 2: Construct n images $G_1, \ldots, G_n$, where each element in the images is randomly selected from the interval $[0.5-u, 0.5+u]$.
Step 3: Each pixel in the secret image is processed by Steps 4–8 in roast-scan order. Denote the current processing pixel as $S(i,j)$, where $1 \leqslant i \leqslant M$ and $1 \leqslant j \leqslant N$.
Step 4: Let B be the non-overlapping block that contains the current processing pixel. The noise N_R is determined by

$$N_R = N_b, \quad \text{if} \quad B \in B_{4,b}$$

where $0 \leqslant b \leqslant 4$.
Step 5: Randomly select a number $d \in \{1, \ldots, n\}$.
Step 6: The $n-1$ pixels $G_1(i,j), \ldots, G_{d-1}(i,j), G_{d+1}(i,j), \ldots, G_n(i,j)$ are processed by the proposed RNBED algorithm with noise N_R, and $n-1$ halftone pixels $R_1(i,j), \ldots, R_{d-1}(i,j)$, $R_{d+1}(i,j), \ldots, R_n(i,j)$ are generated. The quantization errors are calculated and diffused to the neighboring unprocessed pixels.
Step 7: Randomly choose k numbers $a_1, \ldots, a_k$ from $\{1, \ldots, n\} - d$.

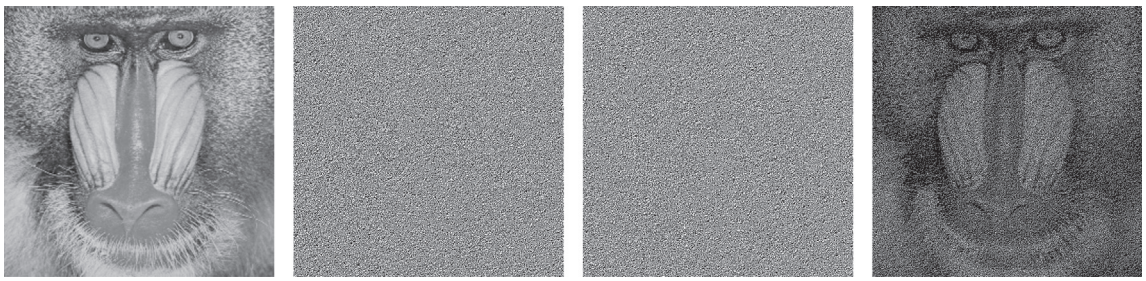

Fig. 7. A (2,2) case for sharing grayscale images by the proposed (k,n) VSS scheme. (a) The secret image, (b)–(c) two RGs R_1 and R_2, and (d) $R_1 \otimes R_2$.

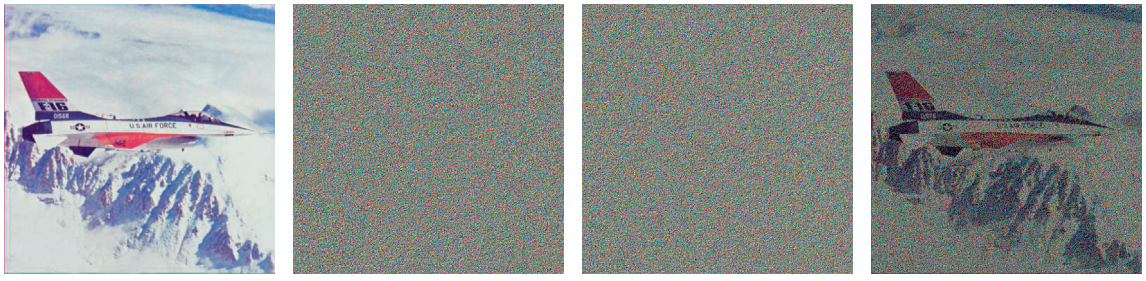

Fig. 8. A (2,2) case for sharing color images by the proposed (k,n) VSS scheme. (a) The secret image, (b) and (c) two RGs R_1 and R_2, and (d) $R_1 \otimes R_2$.

Step 8: Construct the dth pixel $R_d(i,j)$ by

$$R_d(i,j) = S(i,j) \oplus R_{a_1}(i,j) \oplus \cdots \oplus R_{a_k}(i,j)$$

where $\oplus$ denotes the Boolean XOR operation.
Step 9: Output the n RGs $R_1, \ldots, R_n$.

3.4. Extension for grayscale/color images

Grayscale/color images can be shared by extending the two proposed approaches. To encode the grayscale images, halftoning techniques such as order dithering, error diffusion and dot diffusion are adopted to convert the gray-level image into binary. The proposed approaches are then employed to encrypt the halftone image, and the corresponding RGs are constructed.

For encoding the color images, methodologies such as color decomposition, halftone technique and color composition are adopted. To describe the constitution of colors, color model is utilized. In general, there are two types of color models: (1) additive color model, which illustrates a color by mixing with different colors of light, such as RGB (red–green–blue) model; (2) subtractive color model, which displays a color by reflecting light from a surface of an object, such as CMY (cyan–magenta–yellow) model. Herein, the CMY model is adopted. To share the color images, the following four steps should be carried out. 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 algorithms, and some RGs are constructed. Finally, those associated RGs are composed by the CMY color model to generate color RGs.

3.5. Assumptions

It is necessary to mention the difference between reported RG-based VSS schemes [12–16] and the proposed algorithms. In reported RG-based VSS, pixels in the RGs are generated randomly, which means that pixels of different positions in the same RG are uncorrelated. But in the proposed algorithms, pixels in the same RG are generated by RNBED algorithm, and they affect each other via the error diffusion mechanism. In essence, they are correlated.

Analysis on the reported RG-based VSS focuses on average contrast. To prove that a RG-based VSS is a valid construction, two conditions should be satisfied: (1) contrast condition, the secret image can be visually revealed when sufficient shares are stacked, the contrast of the stacked result should be larger than zero, and (2) security condition, the stacked result by insufficient shares gives no clue about the secret, the contrast of the stacked result should be zero.

However, the security condition becomes different in the proposed methods. Since the visual performance of a RG-based VSS is evaluated by both the contrast and variance, variance should be considered as well for the security evaluation. Specifically, the variances calculated from the RGs or stacked results by insufficient shares should be approximately the same, due to the fact that different variances can lead to the leakage of the secret. For the reported RG-based VSS, each pixel is randomly generated and is independent of other pixels in the same RG. The calculated variances would be the same. However, in the proposed methods, each pixel is constructed by the RNBED algorithm and is correlated with the neighboring pixels due to the error diffusing mechanism. The variances would be different when different noises are applied.

As a result, if the proposed algorithms are valid constructions for RG-based VSS, conditions described in Assumptions 1 and 2 must be met.

Assumption 1. The proposed $(2,n)$ VSS is a valid construction of RG-based VSS. Let S be the secret image, and let $R_1, \ldots, R_n$ be the n shares generated by the proposed $(2,n)$ VSS. Denote $S^R_{a_1 \otimes \cdots \otimes a_t} = R_{a_1} \otimes \cdots \otimes R_{a_t}$ as the stacked result of any t shares. The following three conditions are satisfied.

Table 1
The experimental average light transmissions of shares and stacked results by insufficient shares in the $(2,3)$ and $(2,4)$ cases by the proposed $(2,n)$ scheme.

Threshold case	Share	Light transmissions	
		$T(R[S(0)])$	$T(R[S(1)])$
(2,3)	R_1	0.4996	0.5002
	R_2	0.4996	0.4988
	R_3	0.4997	0.5001
(2,4)	R_1	0.4994	0.5007
	R_2	0.4994	0.5006
	R_3	0.4994	0.5001
	R_4	0.4994	0.5007

Table 2
The experimental variances of shares in the $(2,3)$ and $(2,4)$ cases by the proposed $(2,n)$ scheme.

Threshold case	Share	Variance				
		$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
(2,3)	R_1	0.7107	0.7033	0.7104	0.7249	0.6911
	R_2	0.7155	0.6819	0.7229	0.7186	0.6911
	R_3	0.7016	0.7048	0.7214	0.7000	0.6911
(2,4)	R_1	0.7070	0.6710	0.7159	0.6830	0.6818
	R_2	0.7122	0.6716	0.7088	0.6938	0.6818
	R_3	0.7067	0.7068	0.6958	0.6824	0.6818
	R_4	0.7167	0.7128	0.7031	0.6982	0.6818

Table 3
The experimental average light transmissions of shares and stacked results by insufficient shares in the (2,2) and (3,4) cases by the proposed (k,n) scheme.

Threshold case	Share	Light transmissions	
		$T(R[S(0)])$	$T(R[S(1)])$
(2,2)	R_1	0.4998	0.5014
	R_2	0.4998	0.4986
(3,4)	R_1	0.5006	0.4994
	R_2	0.4993	0.4998
	R_3	0.4999	0.4997
	R_4	0.4999	0.5006
	$R_1 \otimes R_2$	0.2489	0.2472
	$R_1 \otimes R_3$	0.2495	0.2489
	$R_1 \otimes R_4$	0.2478	0.2487
	$R_2 \otimes R_3$	0.2490	0.2489
	$R_2 \otimes R_4$	0.2493	0.2497
	$R_3 \otimes R_4$	0.2501	0.2508

Table 4
The experimental variances of shares and stacked results by insufficient shares in the (2,2) and (3,4) cases by the proposed (k,n) scheme.

Threshold case	Share	Variance				
		$\sigma_{4,4}$	$\sigma_{4,3}$	$\sigma_{4,2}$	$\sigma_{4,1}$	$\sigma_{4,0}$
(2,2)	R_1	0.5931	0.5735	0.5745	0.6017	0.6067
	R_2	0.5931	0.6235	0.5879	0.6290	0.6067
(3,4)	R_1	0.4998	0.4794	0.4752	0.4680	0.4846
	R_2	0.4935	0.5041	0.4959	0.4665	0.4880
	R_3	0.4950	0.4681	0.5112	0.5041	0.4955
	R_4	0.4857	0.4972	0.4670	0.5085	0.4926
	$R_1 \otimes R_2$	0.5081	0.5088	0.5292	0.4923	0.5045
	$R_1 \otimes R_3$	0.5090	0.5156	0.5235	0.5070	0.5087
	$R_1 \otimes R_4$	0.5023	0.5252	0.5073	0.5008	0.5057
	$R_2 \otimes R_3$	0.5084	0.4948	0.5254	0.5274	0.5092
	$R_2 \otimes R_4$	0.5132	0.5247	0.5147	0.5220	0.5096
	$R_3 \otimes R_4$	0.5092	0.5211	0.5269	0.5219	0.5096

- Each share R_x $(1 \leqslant x \leqslant n)$ is a RG. That is $T(R_x[S(0)]) = T(R_x[S(1)]) = \frac{1}{2},\ 1 \leqslant x \leqslant n$.
- For each share R_x $(1 \leqslant x \leqslant n)$, the corresponding five variances satisfied $\sigma_{4,0} \approx \sigma_{4,1} \approx \sigma_{4,2} \approx \sigma_{4,3} \approx \sigma_{4,4}$.
- If $t \geqslant 2, T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(0)]) > T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(1)])$. The stacked result reveals the secret.

In Assumption 1, the first and second conditions guarantee that the secret image cannot be revealed by average contrast and variances in a single share, respectively. The third condition makes sure that any two or more shares can visually reconstruct the secret.

Assumption 2. The proposed (k,n) VSS is a valid construction of RG-based VSS. Let S be the secret image, and let $R_1, \ldots, R_n$ be the n shares generated by the proposed (k,n) VSS. Denote $S^R_{a_1 \otimes \cdots \otimes a_t} = R_{a_1} \otimes \cdots \otimes R_{a_t}$ as the stacked result of any t shares. The following five conditions are satisfied.

- Each share R_x $(1 \leqslant x \leqslant n)$ is a RG. That is $T(R_x[S(0)]) = T(R_x[S(1)]) = \frac{1}{2}, 1 \leqslant x \leqslant n$.
- For each share R_x $(1 \leqslant x \leqslant n)$, the corresponding five variances satisfied $\sigma_{4,0} \approx \sigma_{4,1} \approx \sigma_{4,2} \approx \sigma_{4,3} \approx \sigma_{4,4}$.
- If $t < k, T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(0)]) = T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(1)])$. The stacked result gives no clue about the secret.
- If $t < k$, the corresponding five variances of the stacked result satisfied $\sigma_{4,0} \approx \sigma_{4,1} \approx \sigma_{4,2} \approx \sigma_{4,3} \approx \sigma_{4,4}$.
- If $t \geqslant k, T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(0)]) > T(S^R_{a_1 \otimes \cdots \otimes a_t}[S(1)])$. The stacked result reveals the secret.

In Assumption 2, the first two conditions ensure that the average contrast and corresponding variances calculated from each single share give no clue about the secret. The third and fourth conditions guarantee that the stacked result by insufficient shares cannot reveal the secret. The fifth condition makes sure that the secret image can be reconstructed by sufficient shares.

Since the proposed methods are constructed based on the reported $(2,n)$ and (n,n) RG-based VSS schemes, we further conjecture that the contrast of the reconstructed secret image is the same as that by the reported RG-based VSS, as formulated in Assumption 3.

Assumption 3. Denote α as the contrast of the stacked result by any t shares of the two proposed VSS schemes. For the $(2,n)$ VSS, the contrast is

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

where $t \geqslant 2$. For the (k,n) VSS, the contrast is

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

where $t \geqslant k$.

The three assumptions described above will be proved experimentally in Section 4.

4. Experimental results and discussions

Extensive simulation results and discussions are provided in this section. All the images used in this section consist of

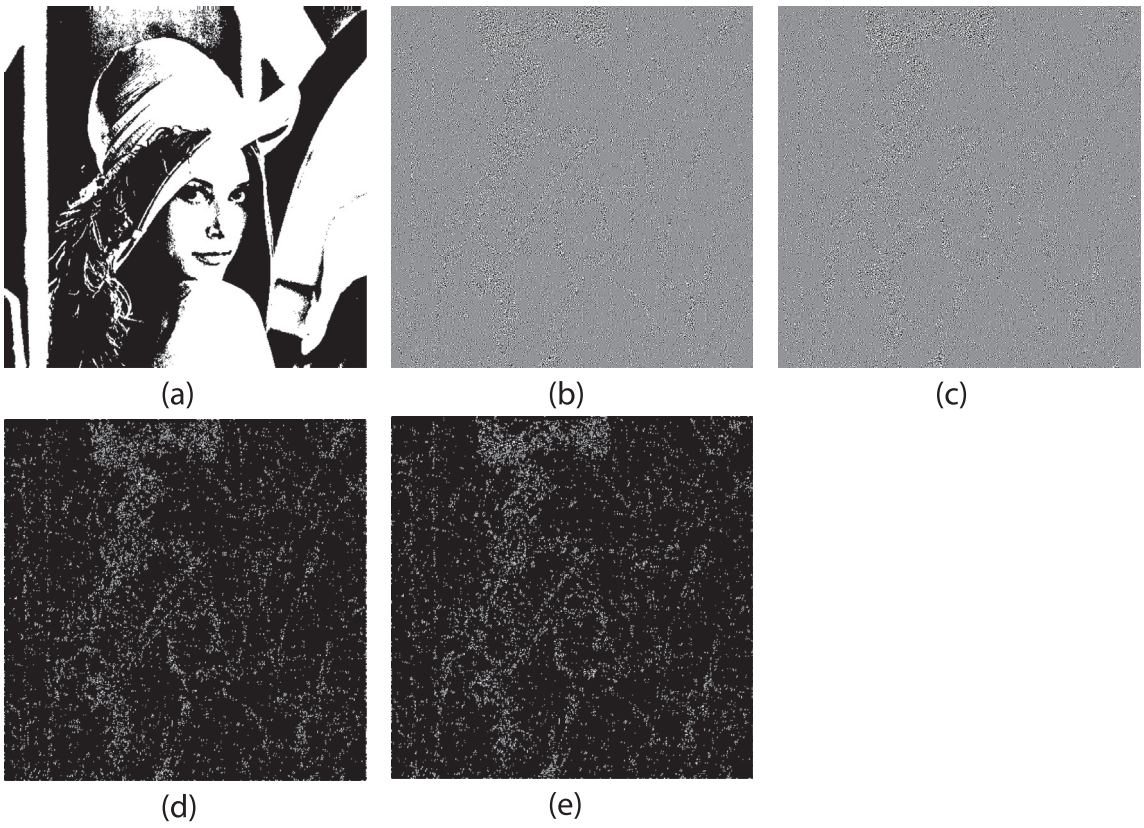

Fig. 9. An example of using the edge detection to attack the shares. (a) The secret image, (b) and (c) two generated shares R_1 and R_2 of a $(2,2)$ case by the proposed (k,n) method, (d) and (e) two attacked results on R_1 and R_2.

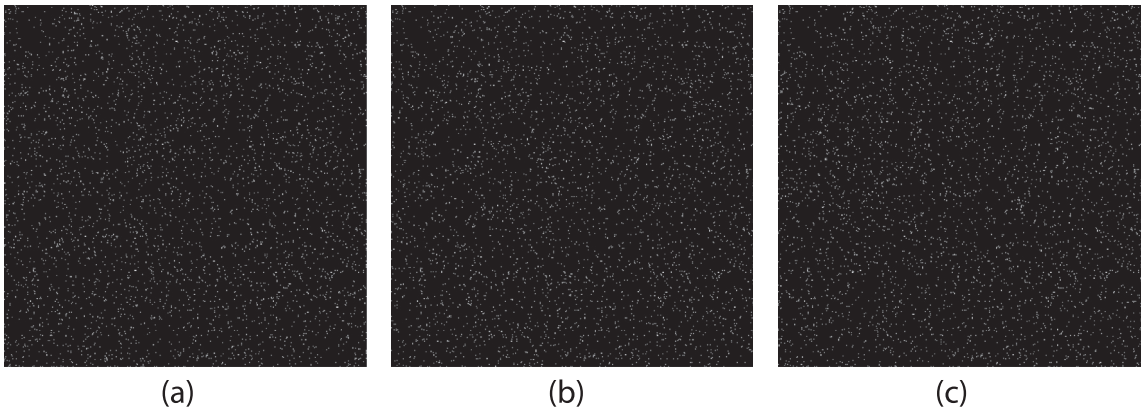

Fig. 10. The attacked results on three RGs of the $(2,3)$ case by the proposed $(2,n)$ method.

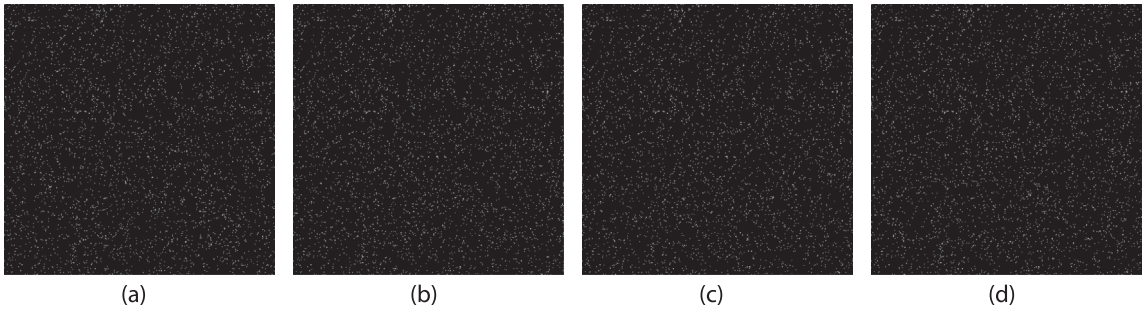

Fig. 11. The attacked results on four RGs of the $(2,4)$ case by the proposed $(2,n)$ method.

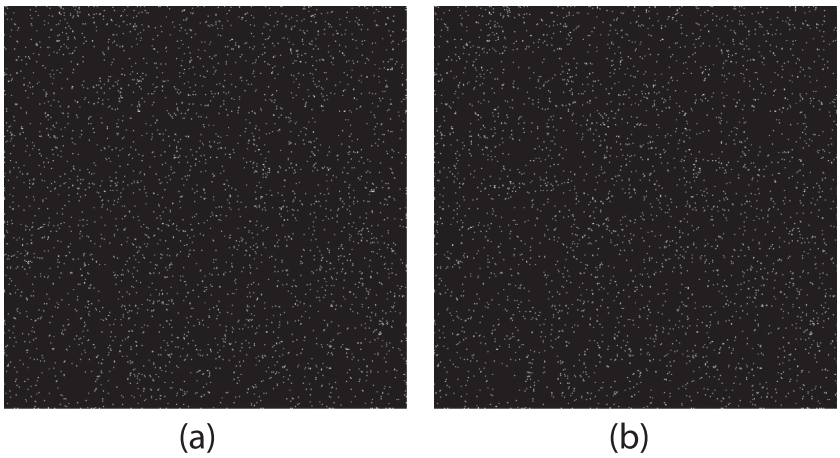

Fig. 12. The attacked results on two RGs of the $(2,2)$ case by the proposed (k,n) method.

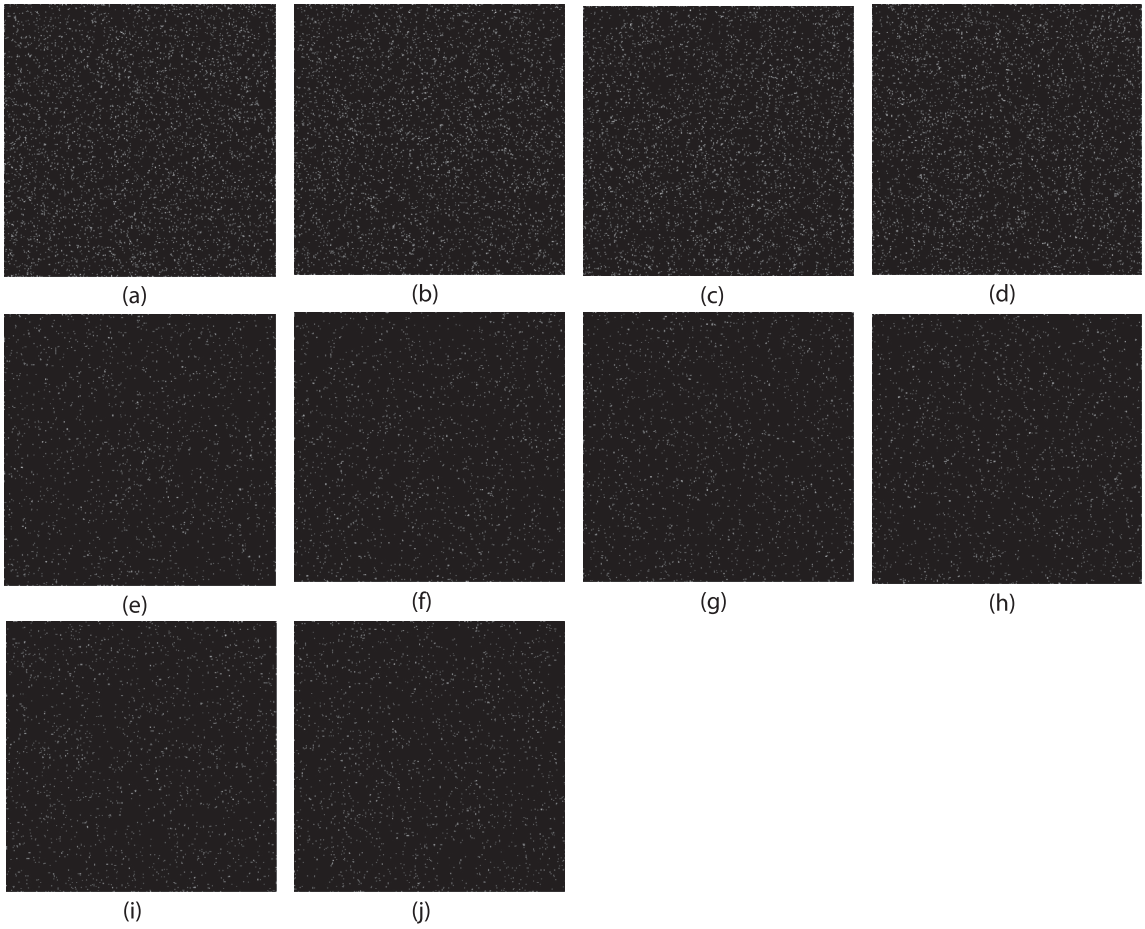

Fig. 13. The attacked results on RGs and stacked results by insufficient RGs of the $(3,4)$ case by the proposed (k,n) method. (a)–(d) The attacked results on the four RGs, (e)–(j) The attacked results on stacked results by insufficient RGs.

512×512 pixels. The parameter u is set to be 0.1, and the interval is $[0.4, 0.6]$.

4.1. Feasibility

4.1.1. Two cases of (2,n) scheme

Two experiments by the proposed $(2,n)$ scheme are provided to demonstrate the effectiveness. The five random noises used in the two experiments are

$$N_0 = N_4 = 0.26, \quad N_1 = N_2 = N_3 = 0.25$$

The first experiment is a $(2,3)$ case, where Fig. 3(a) shows the secret image, and Figs. 3(b)–(d) exhibit the three generated RGs. The stacked results by any two of three RGs are demonstrated in Figs. 3(e)–(g). The superimposed result by three RGs is shown in Fig. 3(h).

A $(2,4)$ case experiment is illustrated in Fig. 4, where the secret image is shown in Fig. 4(a), and four RGs are shown in Figs. 4(b)–(e). The secret image is reconstructed by stacking two or more RGs.

Table 5
The experimental and theoretical contrasts of the recovered secret images in the $(2,3)$ and $(2,4)$ experiments, where t is the number of stacked RGs.

Parameters	(2,3)		(2,4)		
	$t=2$	$t=3$	$t=2$	$t=3$	$t=4$
# of $S^R[S(1)]=1$	96,039	112,036	58,201	68,056	72,972
# of $S^R[S(1)]=0$	32,105	16,108	19,955	10,100	5185
# of $S^R[S(0)]=1$	67,054	67,054	92,096	92,096	92,096
# of $S^R[S(0)]=0$	66,946	66,946	91,892	91,892	91,892
$T(S^R[S(1)])$	0.2505	0.1257	0.2553	0.1292	0.0663
$T(S^R[S(0)])$	0.4996	0.4996	0.4994	0.4994	0.4994
Experimental α	0.1992	0.3321	0.1945	0.3278	0.4064
Theoretical α	$\frac{1}{5}=0.2$	$\frac{1}{3}=0.3333$	$\frac{1}{5}=0.2$	$\frac{1}{3}=0.3333$	$\frac{7}{17}=0.4118$

Table 6
The experimental and theoretical contrasts of the recovered secret images in the $(2,2)$ and $(3,4)$ experiments, where t is the number of stacked RGs.

Parameters	(2,2)	(3,4)	
	$t=2$	$t=3$	$t=4$
# of $S^R[S(1)]=1$	50,140	125,411	138,115
# of $S^R[S(1)]=0$	0	12,704	0
# of $S^R[S(0)]=1$	106,038	104,938	108,879
# of $S^R[S(0)]=0$	105,966	19,091	15,159
$T(S^R[S(1)])$	0	0.0920	0
$T(S^R[S(0)])$	0.4998	0.1539	0.1222
Experimental α	0.4998	0.0567	0.1222
Theoretical α	$\frac{1}{2}=0.5$	$\frac{2}{35}=0.0571$	$\frac{1}{8}=0.125$

Figs. 4(f)–(p) exhibit the stacked results of different combinations of the four RGs.

4.1.2. Two cases of (k,n) scheme

A $(2,2)$ case of the proposed (k,n) VSS algorithm is shown in Fig. 5, where Fig. 5(a) illustrates the secret image, and Figs. 5(b) and (c) shows the two generated RGs. The stacked result by the two RGs are demonstrated in Fig. 5(d), which reveals the secret image. In addition, the five random noises used in this experiment are

$$N_0 = N_4 = 0.3, \quad N_1 = N_2 = N_3 = 0.1.$$

The $(3,4)$ VSS case implemented by the proposed (k,n) scheme is demonstrated in Fig. 6. The five random noises used in this experiment are

$$N_0 = N_1 = N_2 = N_3 = N_4 = 0.15.$$

The secret image and four RGs are shown in Fig. 6 and Figs. 6(b)–(e), respectively. The stacked results of different combinations of the four RGs are illustrated in Figs. 6(f)–(p). We notice that the secret image is revealed by stacking any three or more RGs together.

4.1.3. Two cases for grayscale/color images

Two $(2,2)$ experiments by the proposed (k,n) method for sharing the grayscale and color images are demonstrated in Figs. 7 and 8, respectively. The five random noises used in the two experiments are

$$N_0 = N_4 = 0.27, \quad N_1 = N_3 = 0.2, \quad N_2 = 0.$$

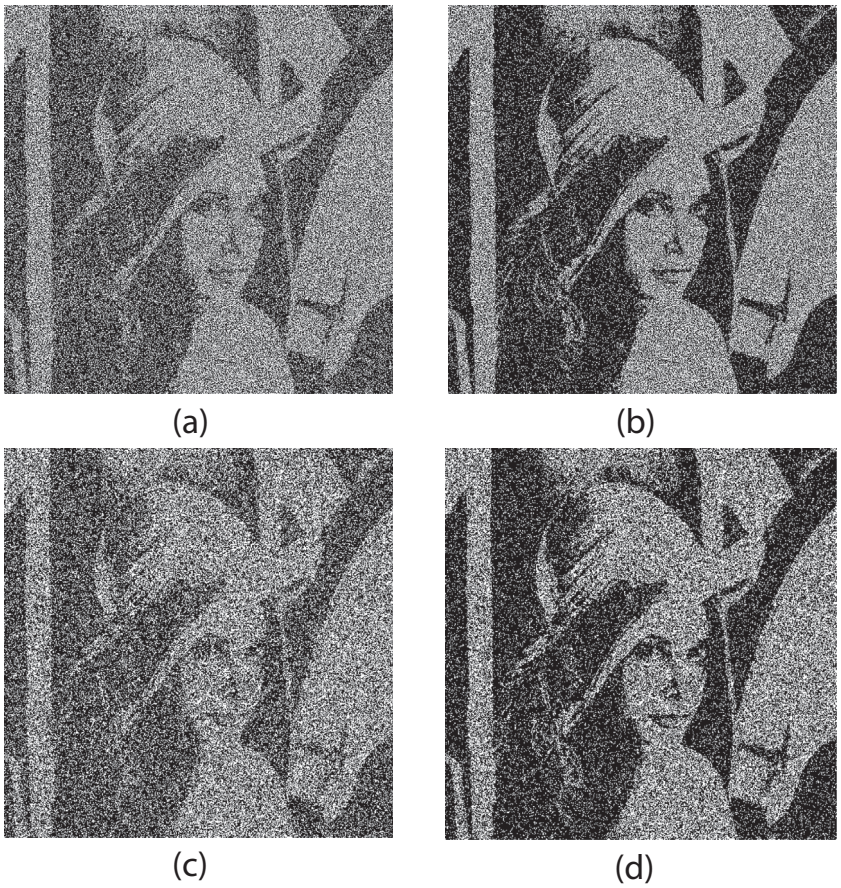

Fig. 14. Comparisons of evenness of the recovered images between the proposed $(2,n)$ scheme and Chen and Tsao's $(2,n)$ scheme [15], when $(2,3)$ case is implemented. (a) and (b) Secret images reconstructed from two RGs and three RGs by the proposed $(2,n)$ scheme, and (c)–(b) secret images reconstructed from two RGs and three RGs by Chen and Tsao's $(2,n)$ scheme.

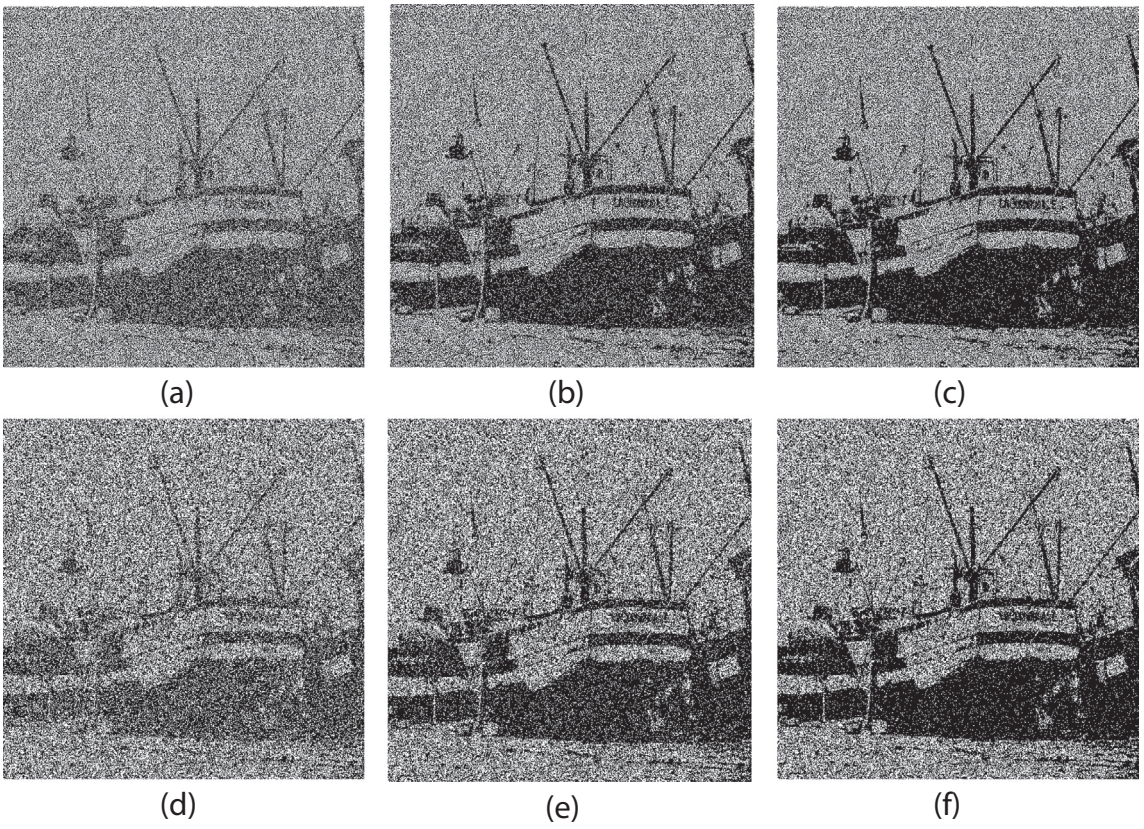

Fig. 15. Comparisons of evenness of the recovered images between the proposed $(2,n)$ scheme and Chen and Tsao's $(2,n)$ scheme [15], when $(2,3)$ case is implemented. (a)–(c) Secret images reconstructed from two RGs, three RGs and four RGs by the proposed $(2,n)$ scheme, and (d)–(f) secret images reconstructed from two RGs, three RGs and four RGs by Chen and Tsao's $(2,n)$ scheme.

Table 7
Comparisons of variances of the recovered image between the proposed $(2,n)$ scheme and Chen and Tsao's $(2,n)$ scheme [15] for the $(2,3)$ case, where t is the number of stacked RGs.

Variance	$t=2$		$t=3$	
	Ours	Ref. [15]	Ours	Ref. [15]
$\sigma_{4,4}$	0.6125	0.7462	0.3871	0.4396
$\sigma_{4,3}$	0.6301	0.8257	0.4927	0.6004
$\sigma_{4,2}$	0.6386	0.8789	0.5568	0.7272
$\sigma_{4,1}$	0.6538	0.8979	0.5996	0.8223
$\sigma_{4,0}$	0.6911	0.9925	0.6911	0.9925

Table 8
Comparisons of variances of the recovered image between the proposed $(2,n)$ scheme and Chen and Tsao's $(2,n)$ scheme [15] for the $(2,4)$ case, where t is the number of stacked RGs.

Variance	$t=2$		$t=3$		$t=4$	
	Ours	Ref. [15]	Ours	Ref. [15]	Ours	Ref. [15]
$\sigma_{4,4}$	0.6181	0.7527	0.3900	0.4303	0.2241	0.2305
$\sigma_{4,3}$	0.6247	0.7971	0.5068	0.5728	0.3922	0.4449
$\sigma_{4,2}$	0.6500	0.8846	0.5447	0.7106	0.4856	0.6234
$\sigma_{4,1}$	0.6388	0.9454	0.5885	0.8358	0.5665	0.7738
$\sigma_{4,0}$	0.6818	1.0026	0.6818	1.0026	0.6818	1.0026

Both the secret images can be visually revealed by stacking two RGs.

4.2. Security analysis

Herein, we discuss the security of the two proposed methods. In reported RG-based VSS, the shared pixels are generated randomly and they are independent of other shared pixels in the same RG. However, the shared pixels are connected with the neighboring pixels in the proposed methods due to the error diffusing mechanism. When different noises are applied, the variances of the RG (or stacked result by insufficient RGs) become different. Visual artifacts would occur in the RG (or stacked result by insufficient RGs) and probably reveal some clues about the secret. Hence, the corresponding variances of a RG (or stacked result by insufficient RGs) should be approximately the same so that those visual artifacts can be prevented.

When discussing the security of the proposed methods, the variances must be considered, as formulated in the second condition of Assumption 1 and the second and fourth conditions of Assumption 2. We prove that the proposed methods are secure by analyzing the experiments.

For the proposed $(2,n)$ scheme, the experimental average light transmissions of the shares in the $(2,3)$ and $(2,4)$ cases are illustrated in Table 1, where $T(R[S(0)])$ (resp. $T(R[S(1)])$) denotes the average light transmission of shares with respect to the associated white (resp. black) area in the secret image. The first condition in Assumption 1 is satisfied. The associated variances calculated from the shares of the $(2,3)$ and $(2,4)$ cases are demonstrated in Table 2. The variances in the same share are approximately the same. The second condition in Assumption 1 is met. In all, the two security conditions are satisfied according to the experimental results.

For the proposed (k,n) approach, Table 3 shows the average light transmissions of the shares and stacked results by insufficient shares in the $(2,2)$ and $(3,4)$ cases. The corresponding variances calculated from the shares and stacked results by insufficient

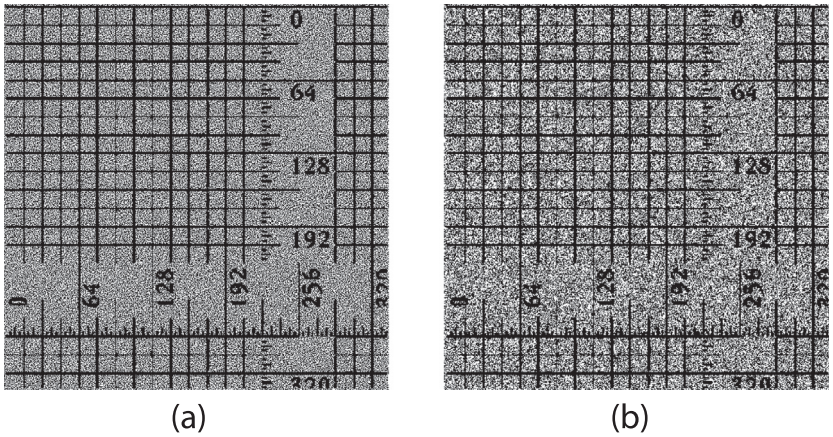

Fig. 16. Comparisons of evenness of the recovered images between the proposed (k,n) scheme and Chen and Tsao's (k,n) scheme [16], when $(2,2)$ case is implemented. (a) Secret image reconstructed from two RGs by the proposed (k,n) scheme, and (b) secret image reconstructed from two RGs by Chen and Tsao's (k,n) scheme.

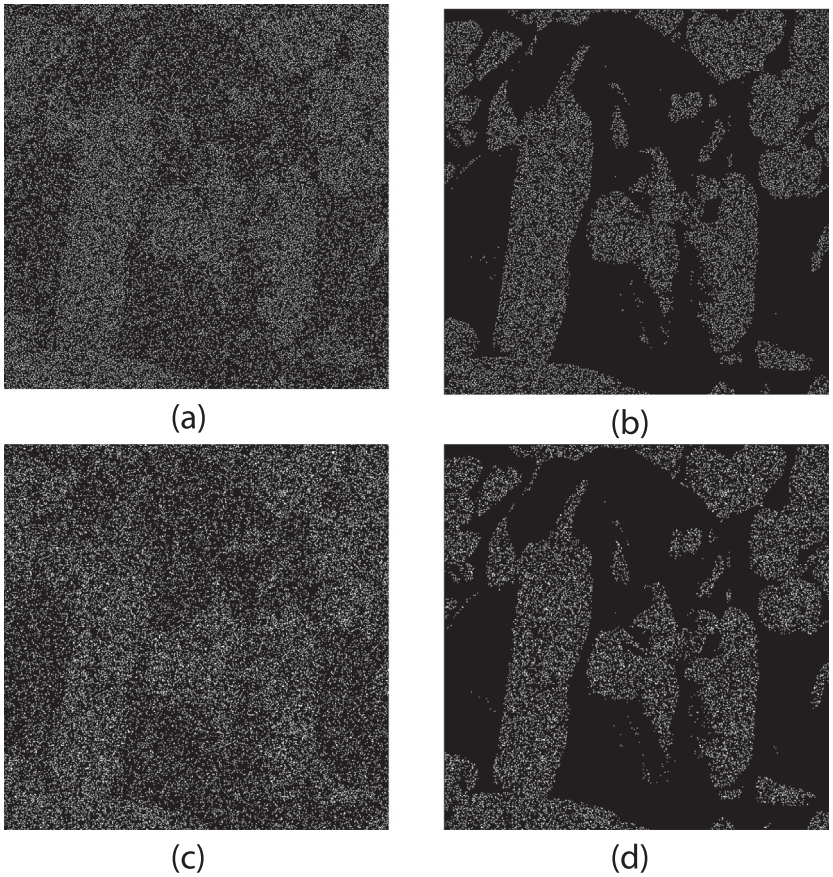

Fig. 17. Comparisons of evenness of the recovered images between the proposed (k,n) scheme and Chen and Tsao's (k,n) scheme [16], when $(3,4)$ case is implemented. (a) and (b) Secret images reconstructed from three RGs and four RGs by the proposed (k,n) scheme, and (c) and (b) secret images reconstructed from three RGs and four RGs by Chen and Tsao's (k,n) scheme.

Table 9
Comparisons of variances of the recovered image between the proposed (k,n) scheme and Chen and Tsao's (k,n) scheme [16] for the $(2,2)$ case.

Variance	Ours	Ref. [16]
$\sigma_{4,4}$	0	0
$\sigma_{4,3}$	0.2499	0.2489
$\sigma_{4,2}$	0.2886	0.4993
$\sigma_{4,1}$	0.3803	0.8289
$\sigma_{4,0}$	0.6067	0.9970

shares in the $(2,2)$ and $(3,4)$ cases are illustrated in Table 4. According to Tables 3 and 4, the first four conditions (security conditions) mentioned in Assumption 2 are satisfied.

Further, attack by using edge detection is employed for analyzing the security of the proposed methods. In the proposed methods, different noises lead to different variances. Meanwhile, some visual artifacts are generated. Usually, those generated visual artifacts are not so clear in the shares or stacked results by insufficient shares. However, they can be detected by edge filtering. Fig. 9

Table 10
Comparisons of variances of the recovered image between the proposed (k,n) scheme and Chen and Tsao's (k,n) scheme [16] for the (3,4) case, where t is the number of stacked RGs.

Variance	$t=3$		$t=4$	
	Ours	Ref. [16]	Ours	Ref. [16]
$\sigma_{4,4}$	0.2799	0.3340	0	0
$\sigma_{4,3}$	0.3145	0.4027	0.1124	0.1135
$\sigma_{4,2}$	0.3573	0.4622	0.2028	0.2194
$\sigma_{4,1}$	0.3816	0.4974	0.2787	0.3387
$\sigma_{4,0}$	0.3870	0.5289	0.3309	0.4374

shows an example of using the edge detection to attack the shares. In this example, the (2,2) case by the proposed (k,n) method is adopted, where the five noises are $N_0 = N_1 = N_2 = N_3 = N_4 = 0$. The secret image used is this example is shown in Fig. 9(a), two generated RGs R_1 and R_2 are illustrated in Figs. 9(b) and (c), respectively. The attacked results on R_1 and R_2 are demonstrated in Figs. 9(d) and(e), respectively. The visual artifacts become more clear in the attacked images, which reveal some clues about the secret.

The same attack is applied to the shares and stacked results by insufficient shares of the four experiments demonstrated in Figs. 3–6. Figs. 10–13 illustrate the associated attacked results. No visual artifact is shown on the attacked images. As a result, the visual artifacts can be suppressed by selecting appropriate noise values, and the proposed methods are secure with these values.

4.3. Correctness of the assumptions

To examine the correctness of the third condition in Assumption 1, the average light transmissions of shares in the $(2,3)$ and $(3,4)$ cases are calculated. Table 5 shows the experimental and theoretical contrasts of the recovered secret images in the $(2,3)$ and $(2,4)$ experiments by the proposed $(2,n)$ scheme, where S^R denotes the stacked result and # represents the counted number of pixels in a specific area. When sufficient shares are stacked, we have $T(S^R[S(0)]) > T(S^R[S(1)])$. The third condition of Assumption 1 is met. Since the first and second conditions of Assumption 1 are proved to be correct in Section 4.2, Assumption 1 is correct.

Similarly, Table 6 demonstrates the experimental and theoretical contrasts of the recovered secret images in the (2,2) and (3,4) cases by the proposed (k,n) method. According to Table 6, we obtain $T(S^R[S(0)]) > T(S^R[S(1)])$. The fifth condition of Assumption 2 is proved to be correct experimentally. In all, Assumption 2 is correct as well.

Further, the correctness of Assumption 3 is substantiated by Tables 5 and 6, where the experimental contrast is approximately the same as the theoretical contrast.

4.4. Visual quality evaluation

Herein, extensive experiments are provided to demonstrate that competitive visual quality of the recovered secret image is obtained by the proposed methods. The recovered image quality is evaluated by the contrast and variances $\sigma_{4,4},\ldots,\sigma_{4,0}$. Comparisons of contrast and variances among the proposed schemes and related methods are illustrated as follows.

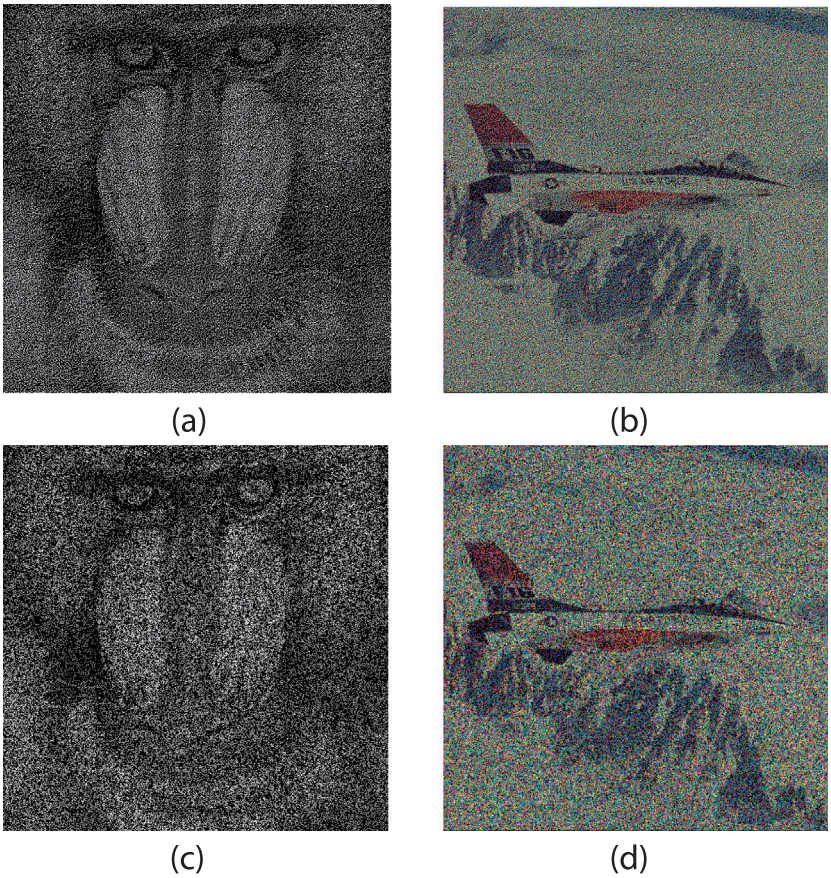

Fig. 18. Comparisons of evenness of the recovered images for sharing grayscale and color images among the proposed (k,n) scheme and related schemes [15,14,16], when (2,2) case is implemented. (a) and (b) Reconstructed secret images by the proposed (k,n) scheme, and (c) and (d) reconstructed secret images by related schemes [15,14,16].

Table 11
Suggested values of N_R for the proposed $(2,n)$ scheme.

Threshold	Available values of N_R $(N_0, N_1, N_2, N_3, N_4)$	
	Binary images	Grayscale/color images
(2,2)	(0.26,0.25,0.25,0.25,0.26)	(0.26,0.25,0.25,0.25,0.26)
(2,3)	(0.26,0.25,0.25,0.25,0.26)	(0.26,0.25,0.25,0.25,0.26)
(2,4)	(0.26,0.25,0.25,0.25,0.26)	(0.26,0.25,0.25,0.25,0.26)
(2,5)	(0.26,0.25,0.25,0.25,0.26)	(0.26,0.25,0.25,0.25,0.26)

Table 12
Suggested values of N_R for the proposed (k,n) scheme.

Threshold	Available values of N_R $(N_0, N_1, N_2, N_3, N_4)$	
	Binary images	Grayscale/color images
(2,2)	(0.3,0.1,0.1,0.1,0.3)	(0.37,0.2,0,0.2,0.37)
(3,3)	(0.35,0.35,0.35,0.35,0.35)	(0.35,0.35,0.350.35,0.35)
(4,4)	(0.25,0.25,0.25,0.25,0.25)	(0.25,0.25,0.25,0.25,0.25)
(3,4)	(0.15,0.15,0.15,0.15,0.15)	(0.15,0.15,0.15,0.15,0.15)

4.4.1. Contrast

Assumption 3 is correct according to the experimental analysis demonstrated in Tables 5 and 6. For the proposed $(2,n)$ algorithm, the contrast is the same as that of Chen and Tsao's $(2,n)$ method [15]. For the proposed (k,n) algorithm, it is the same as that of Chen and Tsao's (k,n) method [16].

4.4.2. Variances

Comparisons of evenness of the recovered secret image between the proposed $(2,n)$ scheme and Chen and Tsao's $(2,n)$ method [15] are illustrated in Figs. 14 and 15, where the $(2,3)$ and $(2,4)$ cases are implemented. The associated variances are demonstrated in Tables 7 and 8.

Comparisons of evenness between the proposed (k,n) scheme and Chen and Tsao's (k,n) scheme [16] are shown in Figs. 16 and 17, where the (2,2) and (3,4) cases are implemented. Moreover, Tables 9 and 10 illustrate the corresponding variances.

Further, when $k=n$, Chen and Tsao's (k,n) scheme [16] reduces to Chen and Tsao's (n,n) scheme [15] and Shyu's (n,n) scheme [14]. Comparisons of evenness for sharing grayscale and color images among the proposed (k,n) scheme and related (n,n) methods are provided in Fig. 18, where the $(2,2)$ case is implemented.

In general, the variances of recovered image by the two proposed methods are obviously smaller than those by reported VSS schemes [14–16]. A more even recovered secret image is achieved by the proposed methods.

4.5. Appropriate values of N_R

Herein, we discuss appropriate values of N_R for different threshold cases. The random noises are mainly used to prevent the artifacts from showing on the RGs or the stacked results by insufficient RGs. In other words, the artifacts on RGs can be removed by selecting appropriate random noises. The variances of every single RG or stacked result by insufficient RGs should be approximately the same. Some suggested appropriate values of N_R are provided in Tables 11 and 12 for the proposed $(2,n)$ and (k,n) methods, respectively. These values are calculated from extensive experiments. For a specific secret image, these values may vary slightly. Note that, grayscale/color images used in this paper are considered to be nature images which are with high entropy, whereas, the binary images excluding the halftone images are with low entropy. As a result, those suggested values of N_R for grayscale/color images are different from those for binary images for certain thresholds.

5. Conclusions

This paper introduces two RG-based VSS schemes which generate recovered secret image with competitive visual quality. The kernel idea to improve the visual quality is to generate RGs whose black pixels are distributed homogeneously. To achieve this goal, a RNBED algorithm is proposed. By combining the proposed RNBED algorithm and existing RG-based VSS schemes, two VSS methods for improving the recovered image quality are presented. Extensive experimental results are provided, demonstrating that the proposed schemes are effective and advanced.

Acknowledgment

The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation. This work was partially supported by Science and Technology Development Fund of Macao Special Administrative Region under Contract 006/2011/A1 and innovative talent training program of Sun Yat-sen University.

References

[1] M. Naor, A. Shamir, Visual cryptography, Lecture Notes in Computer Science 950 (1995) 1–12.
[2] G. Ateniese, C. Blundo, A. De Santis, D. Stinson, Visual cryptography for general access structures, Information and Computation 129 (1996) 86–106.
[3] G. Ateniese, C. Blundo, A. Santis, D. Stinson, Extended capabilities for visual cryptography, Theoretical Computer Science 250 (2001) 143–161.
[4] S. Shyu, S. Huang, Y. Lee, R. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognition 40 (2007) 3633–3651.
[5] J. Feng, H. Wu, C. Tsai, Y. Chang, Y. Chu, Visual secret sharing for multiple secrets, Pattern Recognition 41 (2008) 3572–3581.
[6] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Transactions on Information Forensics and Security 6 (2011) 307–322.
[7] Z. Zhou, G. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Transactions on Image Processing 15 (2006) 2441–2453.
[8] Z. Wang, G. Arce, G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Transactions on Information Forensics and Security 4 (2009) 383–396.
[9] 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.
[10] C. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters 25 (2004) 481–494.
[11] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, The Computer Journal 49 (2006) 97–107.
[12] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Optics letters 12 (1987) 377–379.
[13] S. Shyu, Image encryption by random grids, Pattern Recognition 40 (2007) 1014–1031.
[14] S. Shyu, Image encryption by multiple random grids, Pattern Recognition 42 (2009) 1582–1596.
[15] T. Chen, K. Tsao, Visual secret sharing by random grids revisited, Pattern Recognition 42 (2009) 2203–2217.
[16] T. Chen, K. Tsao, Threshold visual secret sharing by random grids, Journal of Systems and Software 84 (2011) 1197–1208.
[17] R. Floyd, L. Steinberg, An adaptive algorithm for spatial gray-scale, in: Proc. SID, vol. 17, pp. 75–77.
[18] D. Lau, G. Arce, Modern Digital Halftoning, CRC, 2001. vol. 8.
[19] D. Lau, R. Ulichney, G. Arce, Blue and green noise halftoning models, Signal Processing Magazine, IEEE 20 (2003) 28–38.
[20] 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 (2005) 179–192.
[21] F. Liu, C. Wu, L. Qian, et al., Improving the visual quality of size invariant visual cryptography scheme, Journal of Visual Communication and Image Representation 23 (2012) 331–342.