Signal Processing 109 (2015) 317–333

Contents lists available at ScienceDirect

Signal Processing

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

Generalized random grids-based threshold visual cryptography with meaningful shares

Xuehu Yan [a,*], Shen Wang [a,*], Xiamu Niu [a], Ching-Nung Yang [b]

[a] School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin, China
[b] Department of CSIE, National Dong Hwa University, Hualien 974, Taiwan

ARTICLE INFO

Article history:
Received 1 July 2014
Received in revised form
20 November 2014
Accepted 1 December 2014
Available online 9 December 2014

Keywords:
Visual cryptography
Visual secret sharing
Random grid
Threshold
Meaningful shares

ABSTRACT

The meaningful share in visual cryptography (VC) is a desired feature because it can increase the efficiency of management and decrease the suspicion of secret image encryptions. Although the traditional user-friendly random grid (RG)-based VC can produce meaningful shares, with the advantages of no pixel expansion and no need for codebook design, current user-friendly RG-based VCs fail to support the general (k, n) threshold and the complementary shares might be required. In this paper, a generalized RG-based VC with meaningful shares is proposed. Besides inheriting the good features of no pixel expansion and no codebook design, the proposed scheme can support (k, n) threshold and provide adaptive visual quality, at the cost of slightly decreasing visual quality of shared images. Our main contribution is to propose a meaningful VC for case (k, n) with no pixel expansion and codebook design. To the best of our knowledge, the proposed scheme is the first method with all of these good features. Both the theoretical analysis and simulation results demonstrate the effectiveness and security of the proposed scheme.

1. Introduction

Along with the wide application and development of internet and multimedia technology, digital images are easily obtained, transmitted and manipulated. Security of digital images protects the sensitive information from the malicious behavior in transmission [1–3]. An alternative method to ensure the confidentiality and high level of security is cryptography [4]. Cryptography deals with the techniques that transform the data between comprehensible and incomprehensible forms by encryption/decryption operations under the control of key(s). It provides the content confidentiality and access control [4]. Even if one bit of the data is destroyed and the whole secret information is not leaked, the data is not available in cryptography. Therefore, retrieving the original data without any distortion is a matter of importance in case of a certain amount of data is lost in the transmission.

Secret image sharing has solved this problem since the method encodes the user data into different secret shadows (shares) and distributes them to multiple participants. Therefore, it has attracted more attention of scientists and engineers. Shamir's polynomial-based scheme [5–8] and visual cryptography(VC) [9–12], are the primary branches in secret sharing.

A (k,n) -threshold secret sharing scheme was first proposed by Shamir in 1979 [5] through encrypting the secret into the constant coefficient of a random $(k-1)-$degree polynomial. The secret image can be perfectly reconstructed using Lagranges interpolation. Inspired by Shamir's scheme. The advantage of Shamir's polynomial-based scheme [5–8] is the secret can be recovered losslessly. Although Shamir's polynomial-based scheme only needs k shares for reconstructing the distortion-less secret image, while it requires

* Corresponding authors.
Tel.: +86 451 86402861; fax: +86 451 86402861 861.
E-mail addresses: ictyanxuehu@163.com, xuehu.yan@ict.hit.edu.cn (X. Yan), shen.wang@hit.edu.cn (S. Wang).

http://dx.doi.org/10.1016/j.sigpro.2014.12.002
0165-1684/

more complicated computations, i.e., Lagrange interpolations, for decoding and known order of shares.

VC was first introduced by Naor and Shamir [9]. VC is a kind of secret sharing scheme [9–12] that allows the decryption of the secret images without cryptographic knowledge and computational devices. In a general (k,n) threshold VC scheme, a secret image is generated into n random shares (also called shadows) which separately reveals nothing about the secret other than the secret size. The n shares are then printed onto transparencies and distributed to n associated participants. The secret image can be visually revealed based on human visual system (HVS) by stacking any k or more shares, while any $k-1$ or less shares give no clue about the secret [9]. VC can be applied in many scenes [12], such as information hiding, watermarking [13], authentication and identification, and transmitting passwords.

The next we will review some traditional VC schemes first, then extended VC(EVC) is discussed which can be divided into two classifications, depending on the pixel expansion is appeared or not.

Inspired by Naor and Shamir's work, the associated VC problems such as contrast, different formats, and pixel expansion were extensively studied by researchers worldwide. Blundo et al. [14] showed an optical threshold VC with perfect black pixels reconstructions. Ateniese et al. [15] proposed a general VC access structure. Color schemes are considered by Krishna et al., Luo et al., Hou et al., and Liu et al. [16–19]. Multiple secrets sharing was given by Shyu et al. [20]. Threshold VC for different whiteness levels was proposed by Eisen [21]. Step construction was proposed by Liu et al. [22] to improve the visual quality in VC. Ito et al. [23] proposed the probabilistic VC by equally selecting a column from corresponding basic matrix. Probabilistic VC for different thresholds was presented by Yang [24]. Cimato et al. [25] further extended the generalization probabilistic VC.

The aforementioned VC schemes all suffer from disadvantage that the shares consisting of noise-like patterns do not take any visual information, which might lead to suspicion of secret image encryption and decrease the shadow management efficiency. To reduce the suspicion of secret information encryption, and to manage the shares efficiently, EVC [26–28], and halftone VC (HVC) [29,11] were presented. Based on the special design of the dithering matrix, Liu et al. [27] proposed an embedded EVC by embedding random shares into meaningful covering shares. To insert the pixels carrying secret information into preexisting encoded halftone shares, Zhou et al. [29] developed HVC based on void and cluster dithering. Furthermore, an error diffusion-based HVC was proposed by Wang et al. [11]. In Wang et al.'s HVC, the secret information is encoded into the halftone images when the grayscale images are halftoned. Since the shares carry both the secret information and visual information with a codebook design in EVC or HVC, they have the limitation that the pixel expansion is large.

Random grid (RG)-based VC maybe an alternative method to overcome the drawbacks, since RG-based VC has no pixel expansion and requires no codebook design. RG-based VC was first presented by Kafri and Keren [30],

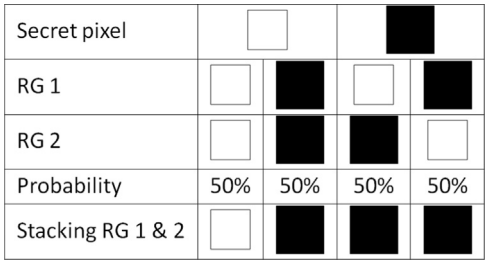

Fig. 1. In a RG-based $(2,2)$ VC, a secret pixel is encrypted into one pixel in each of the two shares (RGs).

which encrypts the secret image into two meaningless RGs. To illustrate the principles of RG-based VC, one of the three distinct encryption algorithms presented by Kafri and Keren is shown in Fig. 1. Each secret pixel taken from a secret binary image is encrypted into one subpixel in each of the two RGs. The subpixels are randomly selected from the two columns tabulated under the certain secret pixel. The selection is random so that each column is selected with the same probabilities (50%). Then, the first subpixel is assigned to RG 1 and the following subpixel is assigned to RG 2. Thus, an individual share gives no clue about the secret image. When the subpixels are stacked, the opaque (black) pixels will cover the transparent (white) pixels. The black secret pixel will be decoded into black pixel, and the white secret pixel will be decoded into white pixel or black pixel with the same probabilities (50%). As a result, the secret could be revealed by HVS. Fig. 2 shows an application example of RG-based $(2,2)$ VC. The secret is encrypted into two random shares which have the same size as the secret image. The revealed image is clearly identified, although some contrast loss occurs.

Follow-up investigations on RG-based VC were discussed to extend the features of RG-based $(2,2)$ VC [31], such as contrast [32,33], color images [34], $(2,n)$ threshold [35–37], (n,n) threshold [31,38] and (k,n) threshold [39,40]. Unfortunately, the previous RG-based VC does not support meaningful shares. To exploit meaningful shares in RG-based VC, Chen and Tsao [31] proposed a friendly RG-based $(2,2)$ VC by designing a procedure of distinguishing different light transmissions on the two shares. However, in Chen and Tsao's user-friendly RG-based $(2,2)$ VC, complementary shares are used to achieve adjustable visual quality. In addition, the method is not for (k,n) threshold, where $k<n$.

The main motivation of this paper is to propose a threshold meaningful VC with no pixel expansion and no codebook design, which can be used in wider applications than traditional VCs. In this paper, a generated RG-based VC with meaningful shares is proposed. The proposed scheme can support (k,n) threshold and provide adaptive visual quality based on RG-based $(2,2)$ VC and RG-based $(2,n)$ VC, at the cost of slightly decreasing the visual quality of shared images. The proposed scheme exploits generated RG to gain different light transmissions on shares, thus meaningful shares are obtained. In addition, the proposed scheme requires no codebook design as well as has no pixel expansion. Simulations results and theoretical analysis are given to show the advantages and effectiveness of the proposed scheme.

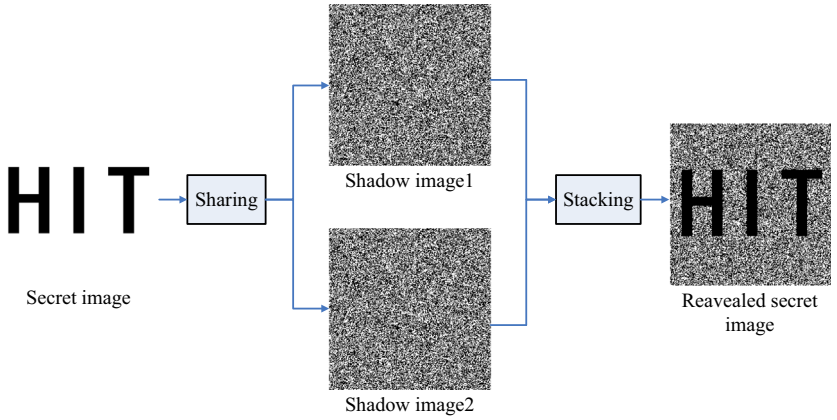

Fig. 2. An application example of RG-based (2, 2) VC. The secret is encrypted into two random shares which have the same size as the secret image. The revealed image shows the secret image with 50% contrast loss.

Table 1
Notations used in this paper.

Notations	Descriptions
0 (resp.1)	A white (resp. black) pixel
$\overline{b}$	The bit-wise complementary operation of a pixel b
$\otimes$	Stacking (OR) operation
$\oplus$	Boolean XOR operation
S	The binary secret image
c	The cover image
$SC_1, SC_2, \ldots, SC_n$	Shares generated by VC schemes
t	Number of stacking shares in the recovery phase
$SC_{[\otimes, i_1, i_2, \ldots, i_t]}$	Stacked result by shares $SC_{i_1}, SC_{i_2}, \ldots, SC_{i_t}$
α	Contrast of the revealed secret image
$S(0)$ (resp. $S(1)$)	The area of all the white (resp. black) pixels in S
$SC[S(0)]$ (resp. $SC[S(1)]$)	The corresponding area of all the white (resp. black) pixels in image SC
$P(x)$	The probability when any event x occurs

The rest of the paper is organized as follows. Section 2 introduces some preliminaries for the proposed scheme. In Section 3, the proposed scheme is presented in detail. Section 4 gives the performance analyses of the proposed scheme. Section 5 is devoted to experimental results and comparisons. Finally, Section 6 concludes this paper.

2. Preliminaries

Before introducing the proposed scheme, some definitions on RG are presented, which are partially borrowed from [34,31,37,39]. Furthermore, notations used in this paper are given in Table 1.

Definition 1 (*Random bit generator [31,37]*). A random bit generator $b = g(w)$ is defined as a bit which is assigned the value 0 (resp.1) with probability w (resp. $1-w$), as follows

$$b = g(w) = \begin{cases} 0 & Prob[g(w)=0] = w \\ 1 & Prob[g(w)=1] = 1-w \end{cases} \quad (1)$$

where $0 < w < 1$.

The probability for a pixel in a share to be white becomes adjustable instead of 0.5 through applying a random bit generator in generalized RG.

Definition 2 (*Average light transmission [34]*). For a certain pixel s in a binary image S whose size is $M \times N$, the light transmission of a transparent (resp. opaque) pixel is defined as $T(s) = 1$ (resp. $T(s) = 0$). Furthermore, the average light transmission of S is defined as

$$T(S) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} T(S(i,j))}{M \times N} \quad (2)$$

Definition 3 (*Contrast [34]*). The contrast of the recovered secret image B for original secret image A is defined as

$$\alpha = \frac{T(B[A(0)]) - T(B[A(1)])}{1 + T(B[A(1)])} \quad (3)$$

Contrast will decide how well human eyes could recognize the reconstructed image, thus it is expected to be as large as possible to gain better visual quality.

Definition 4 (*Visually recognizable [9,39]*). The reconstructed secret image B is recognizable as original secret image A by $\alpha > 0$. Precisely, the case $T(B[A(0)]) > T(B[A(1)])$ means B could be recognized as A visually. Otherwise, it cannot be recognized by any information about A (i.e. $\alpha = 0$).

In general, a valid VC construction means that the VC method satisfies two conditions:

(1) Security condition: Security condition means that insufficient shares give no clue about secret, i.e., $T(B[A(0)]) = T(B[A(1)])$.
(2) Contrast condition: Contrast condition indicates that sufficient shares reveal the secret, i.e., $\alpha > 0$.

3. The proposed scheme

Based on traditional RG-based $(2,2)$ VC [30] and RG-based $(2,n)$ VC [37], a (k,n) threshold is explored. In addition, meaningful shares are gained through exploiting generalized RG. This section describes the details of the proposed (k,n) threshold RG-based VC. A binary secret image is encrypted into n meaningful shares, superimposing at least k shares will reveal the secret, while stacking less than k shares gives no clue about the secret.

Diagram of the share construction is illustrated in Fig. 3. The corresponding algorithm is given in Algorithm 1.

Algorithm 1. (k,n) threshold RG-based VC.

Input: A binary secret image S and a cover binary image C, both with $M \times N$ pixels, the threshold parameters (k,n), and two light transmission parameters w_0, w_1, where $0 < w_1 \le w_0 < 1$
Output: n meaningful shares $SC_1, SC_2, \ldots SC_n$.
Step 1: For each position $(i,j) \in \{(i,j) | 1 \le i \le M, 1 \le j \le N\}$ in the secret image, repeat Steps 2–6.
Step 2: Set $\tilde{b}_1 = S(i,j)$, repeat Step 3 for $k-2$ times, i.e., for $p = 1, 2, \ldots, k-2$, to generate pixels $b_1, b_2, \ldots b_{k-2}, \tilde{b}_{k-1}$ where b_x and $\tilde{b}_x$ denote the temporary pixels, $x = 1, 2, \ldots, n-1, n$
Step 3: If $\tilde{b}_p = 0$, $\tilde{b}_{p+1} = b_p$; otherwise, $\tilde{b}_{p+1} = \overline{b}_p$. Where b_p is generated randomly by flip-coin function.
Step 4: If the corresponding cover image pixel $C(i,j) = 0$, $w = w_0$; otherwise, $w = w_1$.

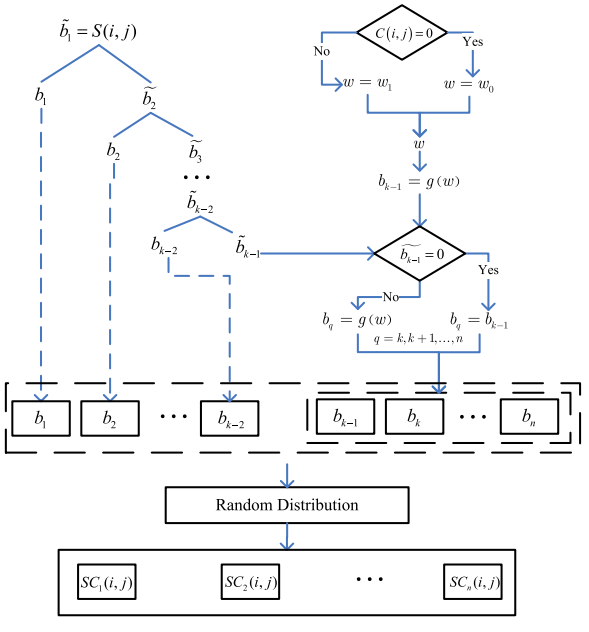

Fig. 3. Shares generation diagram of the proposed scheme.

Step 5: Generate a pixel b_{k-1} by $b_{k-1} = g(w)$. If $\tilde{b}_{k-1} = 0$, $b_q = b_{k-1}, q = k, k+1, \ldots, n$; otherwise, $b_q = g(w), q = k, k+1, \ldots, n$.
Step 6: The order of the n pixels $b_1, b_2, \ldots b_{n-1}, b_n$ are rearranged and the rearranged n pixels are assigned to $SC_1(i,j), SC_2(i,j), \ldots SC_n(i,j)$.
Step 7: Output the n shadow images $SC_1, SC_2, \ldots SC_n$.

In Steps 2 and 3 of Algorithm 1, traditional RG-based $(2,2)$ VC [30] is applied repeatedly $k-2$ times. In Step 5 of Algorithm 1, we explore traditional RG-based $(2, n-k+2)$ VC [37] once. Thus, (k,n) threshold mechanism will be gained.

Steps 4–5 generate the shared $n-k+2$ pixels with respect to a cover image, and introduce different light transmissions parameter w when $w_1 < w_0$, thus, different average light transmissions are obtained. Two different light transmissions in a share are utilized to represent the white and black colors of the cover image, hence meaningful shares will be gained. Furthermore, the shared n pixels carry both the secret information and visual information of the cover image. An example of different light transmissions using different values of w is shown in Fig. 4. Based on the pixel color of cover image C, different values of w are used, which leads to a consequence that meaningful shares are introduced. Besides, when $w_1 = w_0$, the proposed scheme will reduce to a (k,n) threshold RG-based VC with meaningless shares.

In step 6, aiming to make all the shares equally important to each other, the generated n temporary bits are randomly rearranged to corresponding n shadow images bits.

In the generation phase of Algorithm 1, no codebook is applied, thus no codebook design is required in the proposed method. In step 6 of Algorithm 1, since one secret bit is generated and assigned to corresponding one bit for each shadow image, the pixel expansion is avoided in the proposed method.

The secret recovery of the proposed scheme is based on stacking $(\otimes)$ or HVS when directly stacking k or more shares. Besides, if less than k shares are stacked, the original secret image will not be revealed.

Furthermore, the complexity of image splitting stage and revealing is evaluated as follows. The probability of random steps is assumed to be 0.5.

In the generation phase, sharing every secret bit, there are k equal judgments, $(k-2)/2$ complemented operations, $(k-2)/2+1+1+n-k+1+n = 2n-k/2+2$ assignments, and $1+(n-k+1)/2$ random bit generations. We assumed that the size of the secret is $M \times N$, there are totally $k \times MN$ equal judgments, $(k-2)/2 \times MN$ complemented operations, $(2n-k/2+2) \times MN$ assignments, and $(1+(n-k+\ 1)/2) \times MN$ random bit generations, which all

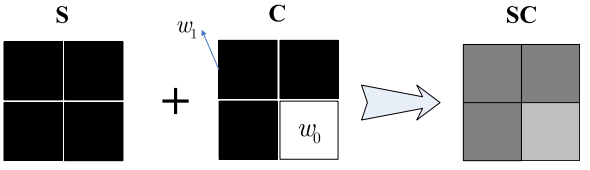

Fig. 4. Example of different light transmissions using different values of w, where each block may cover several pixels. According to different pixel color of cover image C, different values of w are utilized, thus meaningful shares and different light transmissions of the reconstructed results are introduced. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this paper.)

are simple operations. For the recovery phase, there is no computation since stacking recovery.

On the other hand, the proposed scheme has higher generation computation than traditional codebook-based VC [41,42]. As a result, the proposed scheme requires no codebook design at the cost of increasing generation computation.

4. Performance analyses

In this section, the performances of the proposed scheme are given through theoretically analyzing the security and the visual quality. First, we prove that the proposed scheme is a valid (k, n) threshold VC construction by Theorem 1 when stacking decryption is applied, which will show the security of our method. Second, we prove that every share is a meaningful image which looks like the cover image [37] in Theorem 2, i.e., $T(SC_i[C(0)]) > T(SC_i[C(1)])$, where $i = 1, 2, \ldots, n$. Finally, Theorem 3 gives the contrast of the proposed scheme, and the contrast of each share with regard to the cover image is presented in Theorem 4. Before the proof of the Theorems, some Lemmas are presented [39] as the basis for the proof of the theorems. Before the proof of Theorem 2 we assume that $w_1 = w_0$ (denoted as w), which will not affect the proof of Lemmas and Theorems.

Lemma 1. *Each share gives no clue about the secret image*: $T(SC_i[S(0)]) = T(SC_i[S(1)])$ *where* $i = 1, 2, \ldots, n-1, n$.

Proof. Refer Appendix 1. □

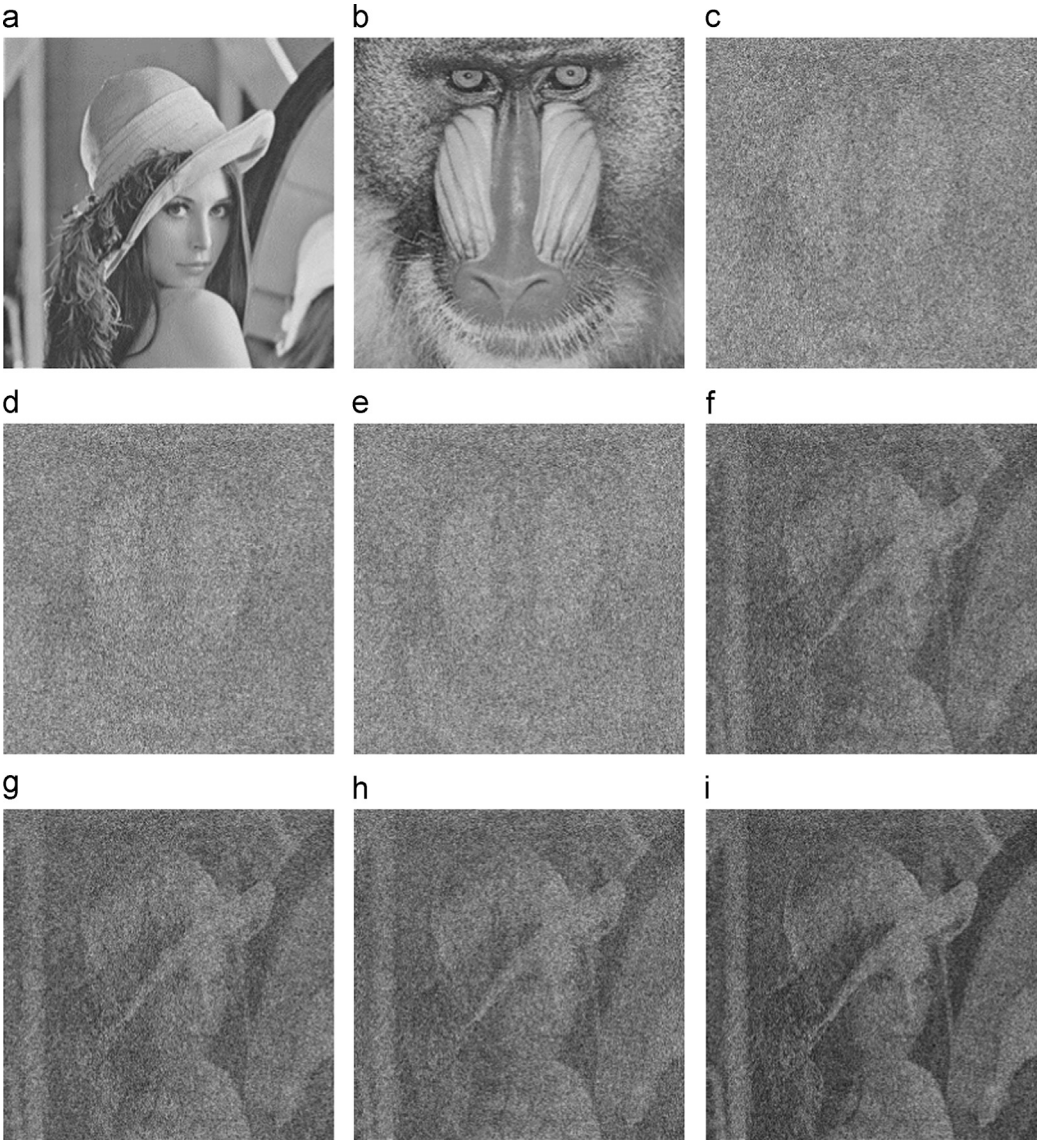

Fig. 5. Simulation results of the proposed (2, 3) threshold RG-based VC, where $w_0 = 0.59$, $w_1 = 0.41$. (a) The secret image; (b) the cover image; (c)–(e) three meaningful shares; (f)–(h) stacking results by any two of the three shares; (i) stacking result by three shares.

Lemma 2. *The stacking result by any $t<k$ shares cannot disclose the secret*: $T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]) = T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])$.

Proof. Refer Appendix 2. □

Lemma 3. *The stacking result by any $t\geq k$ shares visually reveals the secret*: $T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]) > T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])$.

Proof. Refer Appendix 3. □

Theorem 1. *The proposed scheme is a valid construction of RG-based (k,n) threshold VC. The following conditions are satisfied*:

(1) *Each share gives no clue about the secret image*: $T(SC_i[S(0)]) = T(SC_i[S(1)])$, *where* $i=1,2,\ldots,n-1,n$
(2) *The stacking result by any $t<k$ shares cannot disclose the secret*: $T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]) = T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])$.
(3) *The stacking result by any $t\geq k$ shares visually reveals the secret*: $T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]) > T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])$.

Proof. Based on Lemmas 1–3, the mentioned three conditions are satisfied. The proposed scheme is a valid construction of RG-based (k,n) threshold VC. □

Theorem 2. *Each share is a meaningful image which looks like the cover image C*: $T(SC_i[C(0)]) > T(SC_i[C(1)])$, *where* $i=1,2,\ldots,n$.

Proof. When the cover image pixel $C(i,j)=0$ (resp. $C(i,j)=1$), by Lemma 1, the average light transmissions of the shared pixels are $(\frac{1}{2}(k-2)+w_0(n-k+2))/n$ (resp. $(\frac{1}{2}(k-2)+w_1(n-k+2))/n$). Since $w_1<w_0$, we have $T(SC_i[C(0)]) > T(SC_i[C(1)])$ where $i=1,2,\ldots,n$. By Definition

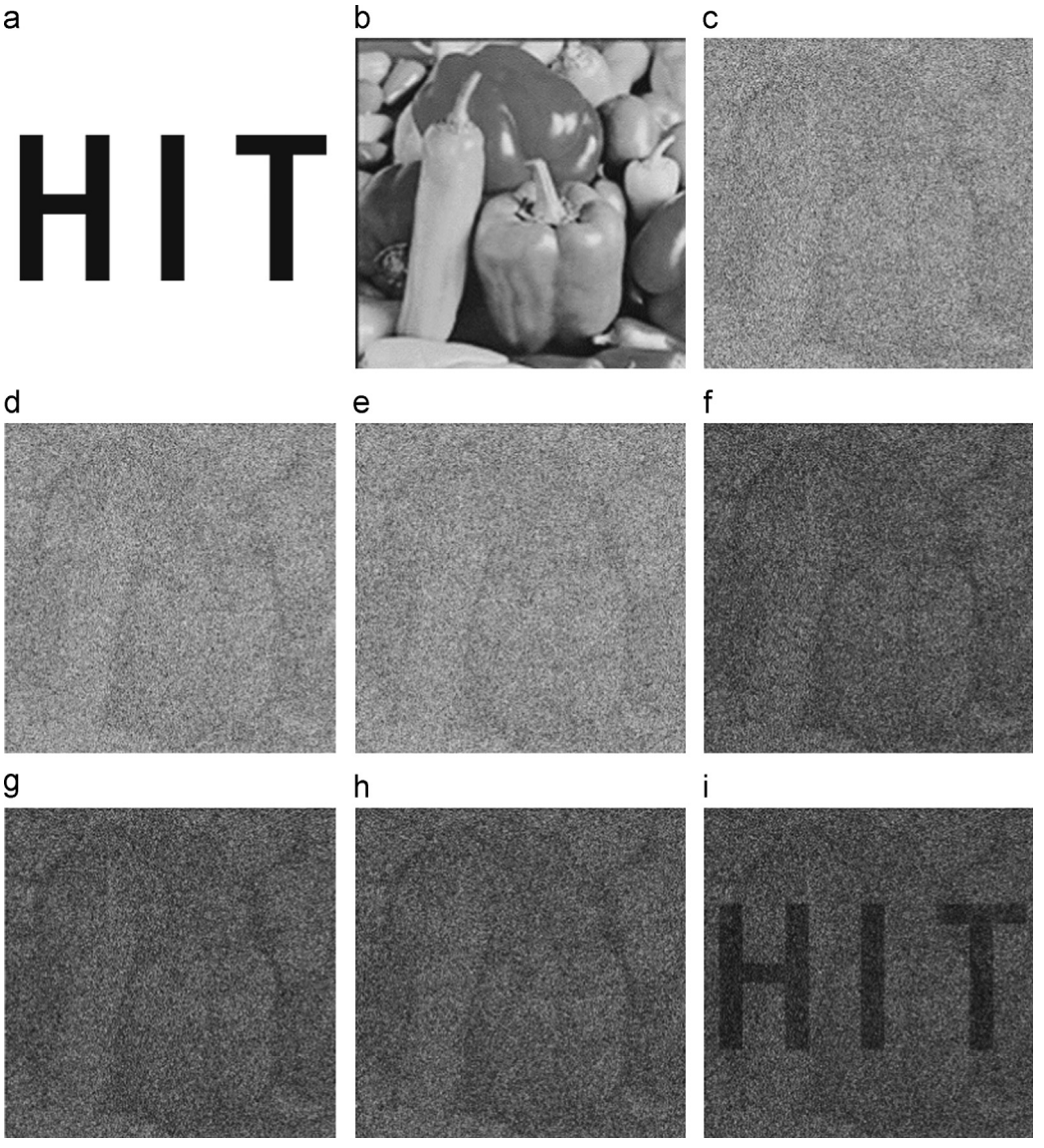

Fig. 6. Simulation results of the proposed (3, 3) threshold RG-based VC, where $w_0=0.58$, $w_1=0.42$. (a) The secret image; (b) the cover image; (c)–(e) three meaningful shares; (f)–(h) stacking results by any two of the three shares; (i) stacking result by three shares.

4, every share is a meaningful image which resembles the cover image. □

Theorem 3. *Contrast of the reconstructed secret image by stacking any t shares constructed by the proposed scheme is*

$$\alpha=\frac{\left[\binom{t}{k-2}\begin{pmatrix}T(C)\times(w_0-w_0^{t-k+2})\\+(1-T(C))\times(w_1-w_1^{t-k+2})\end{pmatrix}\right]}{\left[\begin{matrix}2^{k-2}\binom{n}{k-2}+\binom{t}{k-2}\\(T(C)\times w_0^{t-k+2}+(1-T(C))\times w_1^{t-k+2})\end{matrix}\right]} \tag{4}$$

Proof. By Lemma 3, we have a probability

$$\binom{k-2}{k-2}\times\binom{n-k+2}{t-k+2}\Big/\binom{n}{t}.$$

to pick up $k-2$ bits from the $k-2$ ones generated by Step 3 and $t-k+2$ bits from the $n-k+2$ ones generated by Step 5.

Furthermore,

$$\frac{\binom{k-2}{k-2}\times\binom{n-k+2}{t-k+2}}{\binom{n}{t}}=\frac{\binom{n-k+2}{t-k+2}}{\binom{n}{t}}$$

$$=\frac{\frac{(n-k+2)!}{(t-k+2)!(n-t)!}}{\frac{n!}{t!(n-t)!}}=\frac{\frac{(n-k+2)!}{(t-k+2)!}}{\frac{n!}{t!}}$$

$$=\frac{\frac{t!}{(t-k+2)!}}{\frac{n!}{(n-k+2)!}}=\frac{\frac{t!}{(k-2)!(t-k+2)!}}{\frac{n!}{(k-2)!(n-k+2)!}}$$

$$=\frac{\binom{t}{k-2}}{\binom{n}{k-2}}$$

Based on Lemma 3 and Definition 2,

$$T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)])=\frac{\binom{t}{k-2}}{\binom{n}{k-2}}\times\left(\frac{1}{2}\right)^{k-2}\times(T(C)\times w_0+(1-T(C))\times w_1) \tag{5}$$

$$T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])=\frac{\binom{t}{k-2}}{\binom{n}{k-2}}\times\left(\frac{1}{2}\right)^{k-2}\times(T(C)\times w_0^{t-k+2}+(1-T(C))\times w_1^{t-k+2}) \tag{6}$$

By Definition 3, we have

$$\alpha=\frac{\frac{\binom{t}{k-2}}{\binom{n}{k-2}}\times\left(\frac{1}{2}\right)^{k-2}\times\left(T(C)\times\left(w_0-w_0^{t-k+2}\right)+(1-T(C))\times\left(w_1-w_1^{t-k+2}\right)\right)}{1+\frac{\binom{t}{k-2}}{\binom{n}{k-2}}\times\left(\frac{1}{2}\right)^{k-2}\times\left(T(C)\times w_0^{t-k+2}+(1-T(C))\times w_1^{t-k+2}\right)}$$

$$=\frac{\binom{t}{k-2}(T(C)\times(w_0-w_0^{t-k+2})+(1-T(C))\times(w_1-w_1^{t-k+2}))}{2^{k-2}\binom{n}{k-2}+\binom{t}{k-2}(T(C)\times w_0^{t-k+2}+(1-T(C))\times w_1^{t-k+2})}$$

Thus, the theorem is correct. □

Theorem 4. *Contrast of the shares with regard to the cover image is*

$$\alpha_C=\frac{2(n-k+2)(w_0-w_1)}{2n+k-2+2(n-k+2)w_1} \tag{7}$$

Proof. By Theorem 2 and Definition 3,

$$\alpha_C=\frac{T(SC_i[C(0)])-T(SC_i[C(1)])}{1+T(SC_i[C(1)])}=\frac{\frac{(n-k+2)}{n}(w_0-w_1)}{1+\frac{\frac{1}{2}(k-2)+w_1(n-k+2)}{n}}=\frac{2(n-k+2)(w_0-w_1)}{2n+k-2+2(n-k+2)w_1}$$

where $i=1,2,\ldots,n$. □

By Theorem 3, when $w_0=w_1=w$, we have

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

which is the contrast of the proposed RG-based (k,n)

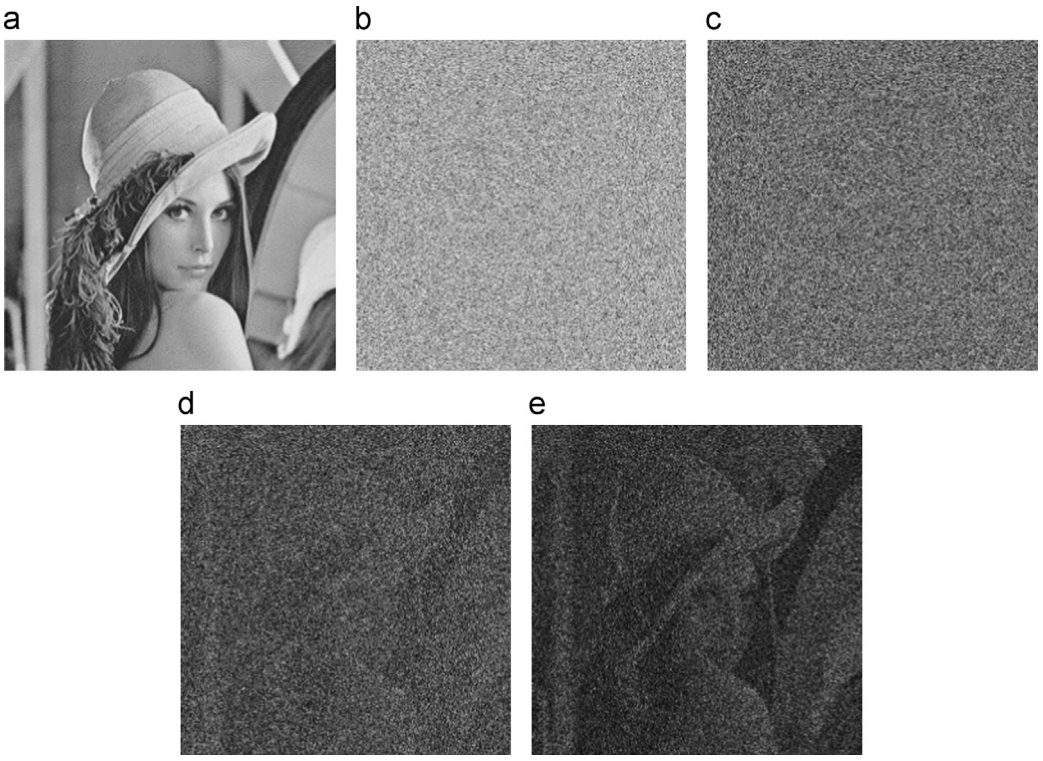

Fig. 7. Simulation results of (3, 4) case by the proposed RG-based VC, where $w_0 = w_1 = w = 0.6$. (a) The secret image; (b) one of the four generated shares, (c)–(e) stacked results by two, three and four shares, respectively.

threshold VC with meaningless shares, i.e., each share does not take any visual information of the cover image.

Furthermore, when $w_0 = w_1 = w$ and $k = 2$, we have $\alpha = (w - w^t)/(1 + w^t)$, which is the same as the contrast of Wu and Sun's $(2, n)$ VC [37]. As a result, when $w_0 = w_1 = w$ and $k = 2$, the proposed scheme reduces to Wu and Sun's $(2, n)$ VC [37].

According to Theorems 3 and 4, the shares take both the secret information and visual information of the cover image. Thus, different values of w_0 and w_1 will introduce different visual quality. Possible values of α and α_C are discussed as follows:

On the one hand, if $w_0 \to 1 \wedge w_1 \to 0$, we have $\alpha \to 0 \wedge \alpha_C \to 2(n-k+2)/(2n+k-2)$, then $\alpha > 0 \wedge \alpha_C < 2\ (n-k+2)/(2n+k-2)$.

On the other hand, if $w_0 = w_1 = w$, then $\alpha = \alpha_w \wedge \alpha_C = 0$.

As a result, $\alpha \in (0, \alpha_w], \alpha_C \in [0, 2(n-k+2)/(2n+k-2)t)$.

Furthermore, available values for w_0 and w_1 will be analyzed in Section 5.3.

5. Experimental results and analysis

In this section, experiments and analysis are conducted to evaluate the effectiveness of the proposed scheme. In addition, some comparisons and discussions are provided. First, we show the effectiveness of the proposed scheme in Section 5.1. Second, we prove the correctness of our theoretical analysis in Section 5.2. Third, Section 5.3 discusses the suitable values for w_0 and w_1. Finally, Section 5.4 gives the comparisons between our method and other related methods.

5.1. Simulations

Simulation results by the proposed scheme for constructing meaningful VC are presented in Figs. 5 and 6, where Figs. 5 and 6 show the (2, 3) and (3, 3) cases, respectively. In the (2, 3) case, the two parameters are with the following configurations: $w_0 = 0.59$, $w_1 = 0.41$. The secret image and cover image are illustrated in Fig. 5(a) and (b) respectively. Three generated meaningful shares which look like the cover image are demonstrated in Fig. 5(c)–(e). The meaningful shares can be identified, although some contrast loss occurs. The stacking results by any two of the three shares are shown in Fig. 5(f)–(h), which reveal the secret. The secret is also reconstructed by stacking three shares, which is shown in Fig. 5(i). The size of the shadow image is the same as that of the secret image, so there is no pixel expansion occurred in the proposed scheme.

The two parameters used in the (3, 3) case are configured as $w_0 = 0.58$, $w_1 = 0.42$. Fig. 6(a) and (b) shows the secret image and cover image used in the (3, 3) case, respectively. The meaningful shares are demonstrated in Fig. 6(c)–(e). The stacking results by any two of the three shares are illustrated in Fig. 6(f)–(h), which give no clue about the secret. The secret is reconstructed by conducting stacking operation on the three shares, as shown in Fig. 6(i).

A (3, 4) generalized RG-based VC with meaningless shares by the proposed scheme is demonstrated in Fig. 7, where

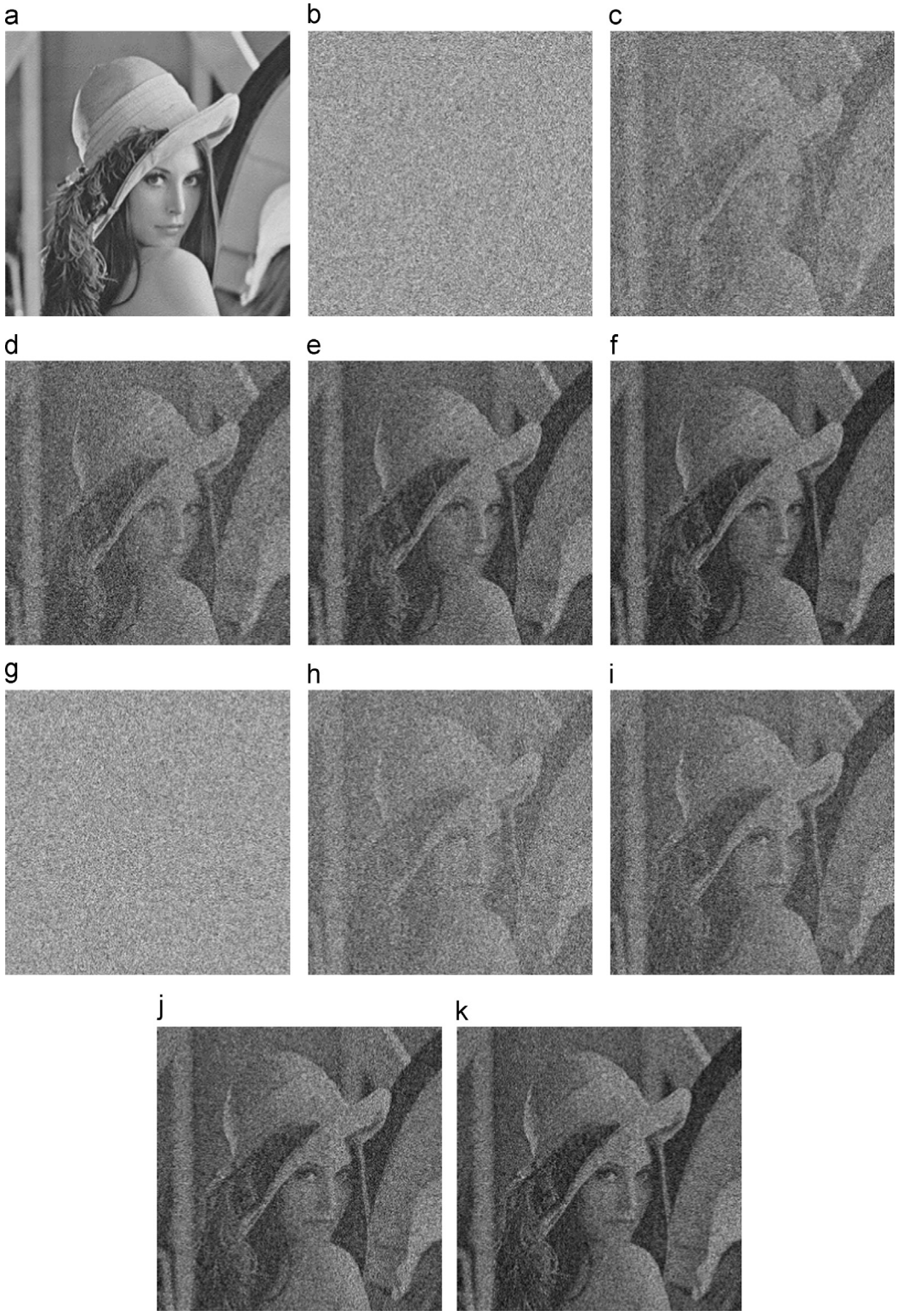

Fig. 8. Comparison of visual quality between the proposed RG-based VC and Wu and Sun's $(2, n)$ RG-based VC [37], where $k = 2$ and $w_0 = w_1 = w = 0.6$. (a) The secret image; (b) one of the generated shares by the proposed scheme; (c)–(f) stacked results by two, three, four and five shares of the proposed scheme, respectively. The contrast is 0.1757, 0.3155, 0.4155 and 0.4840, respectively; (g) one of the generated shares by [37]; (h)–(k) stacked results by two, three, four and five shares from [37], respectively. The contrast is 0.1757, 0.3154, 0.4160 and 0.4840, respectively.

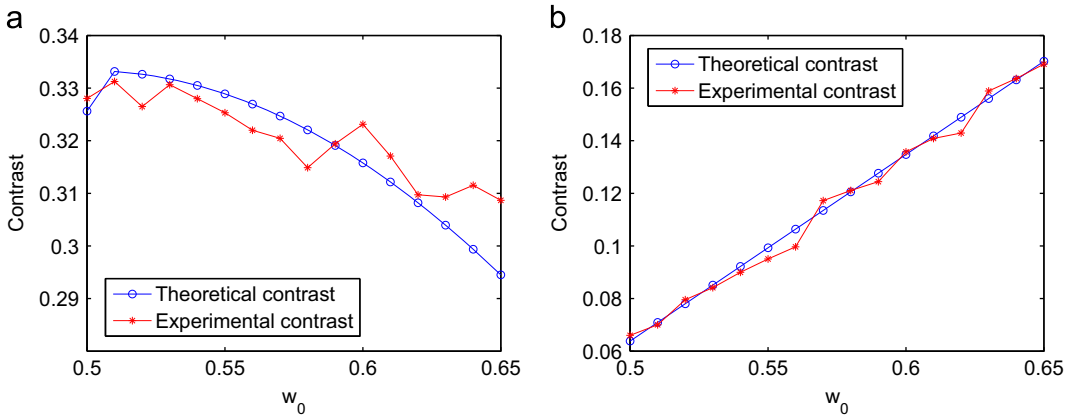

Fig. 9. Comparison between theoretical contrast and experimental contrast of the proposed RG-based meaningful VC for (2, 3) case under $w_1 = 0.41$, when possible values of w_0 are used, where $t=3$ and $T(C) = 0.4458$. (a) contrast curves of the reconstructed secret image; (b) contrast curves of the share image.

$w_0 = w_1 = w = 0.6$. The secret image is shown in Fig. 7(a) and one of the four generated shares is illustrated in Fig. 7(b). One of the stacking results by any two of the four shares is illustrated in Fig. 7 (c), which gives no clue about the secret. By stacking any three or more shares, the secret image is visually revealed, as demonstrated in Fig. 7(d)–(e).

Another experiment by the proposed (2, 5) threshold RG-based VC with meaningless shares is exhibited in Fig. 8 with parameters $w_0 = w_1 = w = 0.6$, where the secret image is shown in Fig. 8(a) and one of the generated shares is demonstrated in Fig. 8(b). The secret image is visually reconstructed by superimposing any two or more shares together, where the revealed secret images and the corresponding contrast are illustrated in Fig. 8(c)–(f). In addition, Wu and Sun's (2, 5) RG-based VC [37] is given in Fig. 8 as well, where the same parameters as ours are used. One of the generated shares in their method is demonstrated in Fig. 8(g) as well as the revealed secret images are illustrated in Fig. 8(h)–(k) by stacking any two or more shares together, where the corresponding contrast is also shown. Based on Fig. 8, the visual quality of the two methods is approximately the same.

5.2. Theoretical contrast validation

Herein, Fig. 9 is presented for validating theoretical contrast analysis. Fig. 9 (a) shows the theoretical contrast and experimental contrast curves of the reconstructed secret image for (2, 3) case under $w_1 = 0.41$, when possible values of w_0 are used, where $t=3$. Furthermore, contrast curves of the share image are illustrated in Fig. 9 (b). Fig. 9 indicates experiment results accord with academic analysis.

5.3. Available values for w_0 and w_1

The shares of the proposed (k,n) threshold RG-based meaningful VC are meaningful since different values of w are utilized. While different values of w would introduce different light transmissions of the reconstructed results. The light transmissions may vary from each other significantly, and lead to a consequence that the reconstructed secret image is not homogeneous. An example is shown in Fig. 10 with the four parameters configured as $w_0 = 0.54$, $w_1 = 0.46$ and $w_0 = 0.65$, $w_1 = 0.35$, where the corresponding contrast and light transmissions, i.e., $T(SC_{\{\otimes,1,2\}}[S(0) \cap C(0)])$ (denoted as $T^{w_0}(SC_{\{\otimes,1,2\}}[S(0)])$ for short), $T^{w_0}(SC_{\{\otimes,1,2\}}[S(1)])$ and $T(SC_{\{\otimes,1,2\}}[S(0) \cap C(1)])$ (shortly denoted as $T^{w_1}(SC_{\{\otimes,1,2\}}[S(0)])$, $T^{w_1}(SC_{\{\otimes,1,2\}}[S(1)])$, are also given. Obviously, some reconstructed pixels which belong to the black area of the original secret image are darker than the others, and the reconstructed image contains cross interference from the share images.

The reason of resulting in inhomogeneous recovered secret image is that the light transmissions ($T^{w_0}(SC_{\{\otimes,1,2\}}[S(0)])$ and $T^{w_0}(SC_{\{\otimes,1,2\}}[S(1)])$) of the recovered secret image by value w_0 are different from the light transmissions ($T^{w_1}(SC_{\{\otimes,1,2\}}[S(0)])$ and $T^{w_1}(SC_{\{\otimes,1,2\}}[S(1)])$) of the recovered secret image by value w_1 [37].

In order to obtain homogeneous recovered secret image for the proposed (k,n) threshold RG-based meaningful VC, the four light transmissions should satisfy the following conditions [37]:

$$T^{w_0}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]] = T^{w_1}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]] \tag{8}$$

and

$$T^{w_0}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]] = T^{w_1}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]] \tag{9}$$

Furthermore, the visual quality of the share increases while that of the revealed secret image decreases, hence there is a tradeoff between the contrast of the reconstructed image and the contrast of the share image. Fig. 11 (a) shows the contrast curves of the reconstructed secret image and share image for (2, 3) case under $w_1 = 0.41$, when possible values of w_0 are used, where $t = 2$. Based on Fig. 11 (a), the contrast variable trend of the reconstructed secret image is opposite to that of share image.

The reason of the visual quality tradeoff is further analyzed as follows:

On the one hand, according to Eq. (7), $\partial\alpha_C/\partial w_0 = 2(n-k+2)/(2n+k-2+2(n-k+2)w_1) \geq 0$ and $\partial\alpha_C/\partial w_1 = -2(n-k+2)(2n+k-2)/(2n+k-2+2(n-k+2)\quad w_1)^2 \leq 0$. As a result, α_C is a monotonically increasing function of w_0 and a monotonically decreasing function of w_1, i.e.,

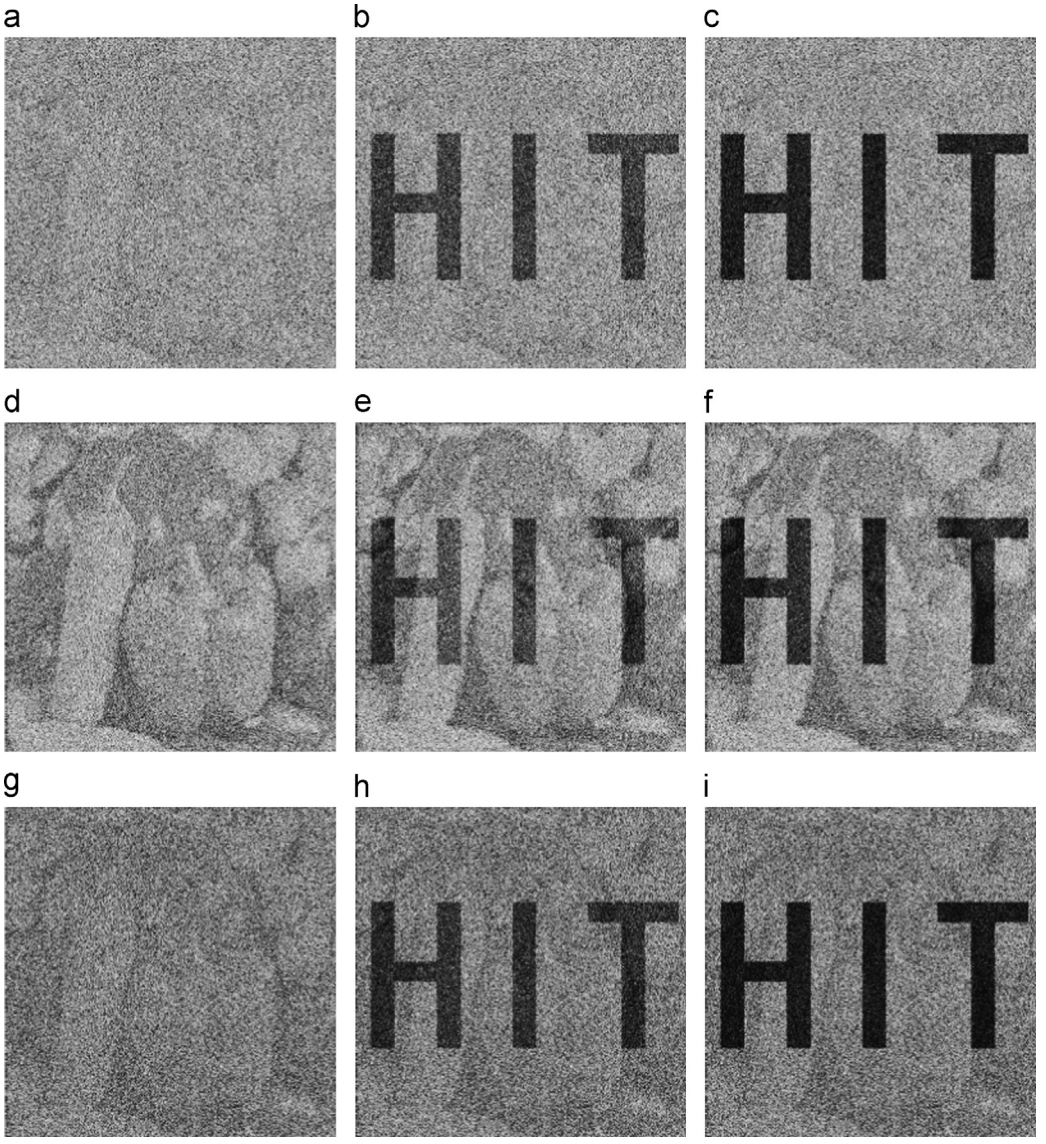

Fig. 10. Comparison of visual quality between $w_0=0.54,\ w_1=0.46, w_0=0.65,\ w_1=0.35$ the suitable values of $w_0=0.4845, w_1=0.3645$, for (2, 3) case. (a) One of the generated shares by $w_0=0.54,\ w_1=0.46$, where the contrast is 0.0543. (b)–(c) stacked results by two and three shares under $w_0=0.54, w_1=0.46$, respectively. The contrast is 0.2017 and 0.3329, respectively. The light transmissions stacked by two shares are 0.5400, 0.2890 and 0.4601, 0.2118, respectively; (d) One of the generated shares by $w_0=0.65,\ w_1=0.35$, where the contrast is 0.2222. (e)–(f) stacked results by two and three shares under $w_0=0.65,\ w_1=0.35$, respectively. The contrast is 0.1864 and 0.3009, respectively. The light transmissions stacked by two shares are 0.6510, 0.4240 and 0.3513, 0.1241, respectively. (g) One of the generated shares by the suitable values of $w_0=0.4845, w_1=0.3645$, where the contrast is 0.0895. (h)–(i) stacked results by two and three shares under $w_0=0.4845, w_1=0.3645$, respectively. The contrast is 0.2049 and 0.3165, respectively. The light transmissions stacked by two shares are 0.4849, 0.2355 and 0.3633, 0.1328, respectively.

the visual quality of each share with regard to the cover image, increases as w_0 increases and decreases as w_1 increases. Hence, a larger value of α_C requires a larger value of $|w_0-w_1|$.

On the other hand, based on Eq. (4) excluding the difference of $T(C)$.

$$\alpha''(w) = \frac{a(t-k+2)w^{t+k}}{(bw^k+aw^{t+2})^3}$$

$$\begin{bmatrix} ((a^2-a^2k+a^2t)w^{t+3}+(3ab-abk+abt)w^{t+2}) \\ -((b^2-b^2k+b^2t)w^k+(3ab-abk+abt)w^{k+1}) \end{bmatrix} \le 0,$$

where

$$a=\binom{t}{k-2}, \quad b=2^{k-2}\binom{n}{k-2}.$$

Hence, α is a concave upward function of w, when $0<w<1$. As an example, contrast curve of the reconstructed secret image for (2, 3) case under $w_0=w_1=w$ and $t=2$, when possible values of w are used, is illustrated in

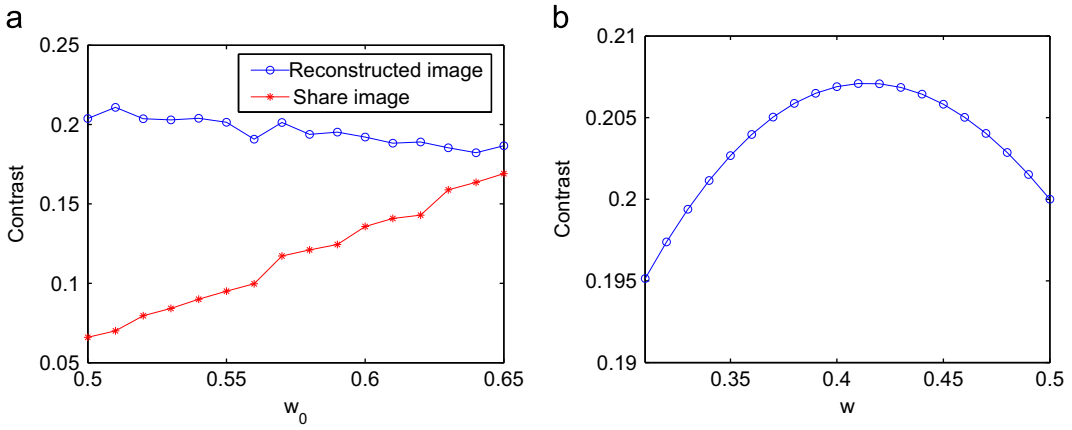

Fig. 11. Contrast curves of the proposed RG-based meaningful VC for (2, 3) case when possible values of w_0 and w_1 are used, where $t=2$. (a) contrast curves of the reconstructed secret image and share image under $w_1=0.41$, when possible values of w_0 are used; (b) contrast curve of the reconstructed secret image under $w_0=w_1=w$, when possible values of w are used.

Fig. 11(b). According to Fig. 11(b), α is a concave upward function of w.

Moreover, Eqs. (8) and (9) are equal to

$$|T^{w_0}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]]-T^{w_1}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]]|\lesssim\varepsilon \tag{10}$$

and

$$|T^{w_0}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]]-T^{w_1}[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]]|\lesssim\varepsilon \tag{11}$$

where ε is a adjustable parameter which can be used for the user to control the light transmissions difference, and acceptable range of ε is $0<\varepsilon\le 0.2$ which is obtained through extensive experiments.

In general applications, the visual quality of the reconstructed image is more important than that of the share image. We can balance the tradeoff problem and simultaneously satisfy homogeneous conditions in Eqs. (8) and (9), through conducting the following steps:

Step 1: w^* can be obtained by solving the equation '$\alpha'(w)=0$', i.e., w^* is the maximum point of $\alpha(w)$.

Step 2: For $\forall\ \varepsilon>0$, according to Eqs. (5)–(6), $T[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]]$ (denoted as T_0 for short) and $T[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]]$ (denoted as T_1 for short) are continuous and differentiable functions of w when $w_0=w_1=w$, as a result $\exists\xi_0,\xi_1\in(w_1,w_0)$ satisfy $T_0'(\xi_0)=T_0(w_0)-T_0(w_1)/\ (w_0-w_1)$ and $T_1'(\xi_1)=T_1(w_0)-(T_1(w_1))/(w_0-w_1)$, respectively.

Hence, we have

$$\begin{aligned}&\max(w_0-w_1)\\&=\min\left(\frac{T_0(w_0)-T_0(w_1)}{T_0'(\xi_0)},\frac{T_1(w_0)-T_1(w_1)}{T_1'(\xi_1)}\right)\\&\lesssim\min\left(\frac{\varepsilon}{T_0'(\xi_0)},\frac{\varepsilon}{T_1'(\xi_1)}\right).\end{aligned}$$

Since w_1,w_0 are approximately equal to w^*, we can approximately obtain $\max(w_0-w_1)=\min(\varepsilon/T_0'(w^*),\varepsilon/T_1'(w^*))$.

Step 3: Compute

$$\delta_0=\frac{\left|\frac{\partial\alpha_C}{\partial w_0}\right|\Big|_{w^*}}{\left|\frac{\partial\alpha_C}{\partial w_0}\right|\Big|_{w^*}+\left|\frac{\partial\alpha_C}{\partial w_1}\right|\Big|_{w^*}}\max(w_0-w_1)$$

and

$$\delta_1=\frac{\left|\frac{\partial\alpha_C}{\partial w_1}\right|\Big|_{w^*}}{\left|\frac{\partial\alpha_C}{\partial w_0}\right|\Big|_{w^*}+\left|\frac{\partial\alpha_C}{\partial w_1}\right|\Big|_{w^*}}\max(w_0-w_1),$$

respectively.

Step 4: Suitable values of $w_0=w^*+\delta_0$ and $w_1=w^*-\delta_1$ are obtained.

Remark. Suitable values of w_0,w_1 gained by the above steps are the approximately preferable values, which may be not the best values.

As an example, the proposed RG-based meaningful VC for (2, 3) case is utilized to show how to gain suitable parameters values of w_0 and w_1, where $t=2$.

Step 1: Based on $\alpha'(w)=((1-2w)(1+w^2)-2w(w-\ w^2))/(1+w^2)^2=0$, we can obtain $w^*=\sqrt{2}-1$.

Step 2: We assume $\varepsilon=0.12>0$, we have $\max(w_0-w_1)=\min((T_0(w_0)-\ T_0(w_1))/T_0'(w^*),\ (T_1(w_0)-T_1(w_1))/T_1'(w^*))=\min(\varepsilon/1,\varepsilon/2w^*)=\varepsilon$.

Step 3:

$$\delta_0=\frac{\left|\frac{1}{1+w_1}\right|\Big|_{w^*}}{\left|\frac{1}{1+w_1}\right|\Big|_{w^*}+\left|\frac{1}{(1+w_1)^2}\right|\Big|_{w^*}}\varepsilon=\frac{\sqrt{2}}{1+\sqrt{2}}\varepsilon$$

and

$$\delta_1=\frac{\left|\frac{1}{(1+w_1)^2}\right|\Big|_{w^*}}{\left|\frac{1}{1+w_1}\right|\Big|_{w^*}+\left|\frac{1}{(1+w_1)^2}\right|\Big|_{w^*}}\varepsilon=\frac{1}{1+\sqrt{2}}\varepsilon,$$

respectively.

Step 4: Finally, we get suitable values of $w_0=(\sqrt{2}-1)+\sqrt{2}/(1+\sqrt{2})\varepsilon\approx 0.4845$ and $w_1=(\sqrt{2}-1)-(1/(1+\sqrt{2}))\varepsilon\approx 0.3645$.

According to the suitable values of $w_0=0.4845$ and $w_1=0.3645$, Fig. 10 (g)–(i) presents an example with the

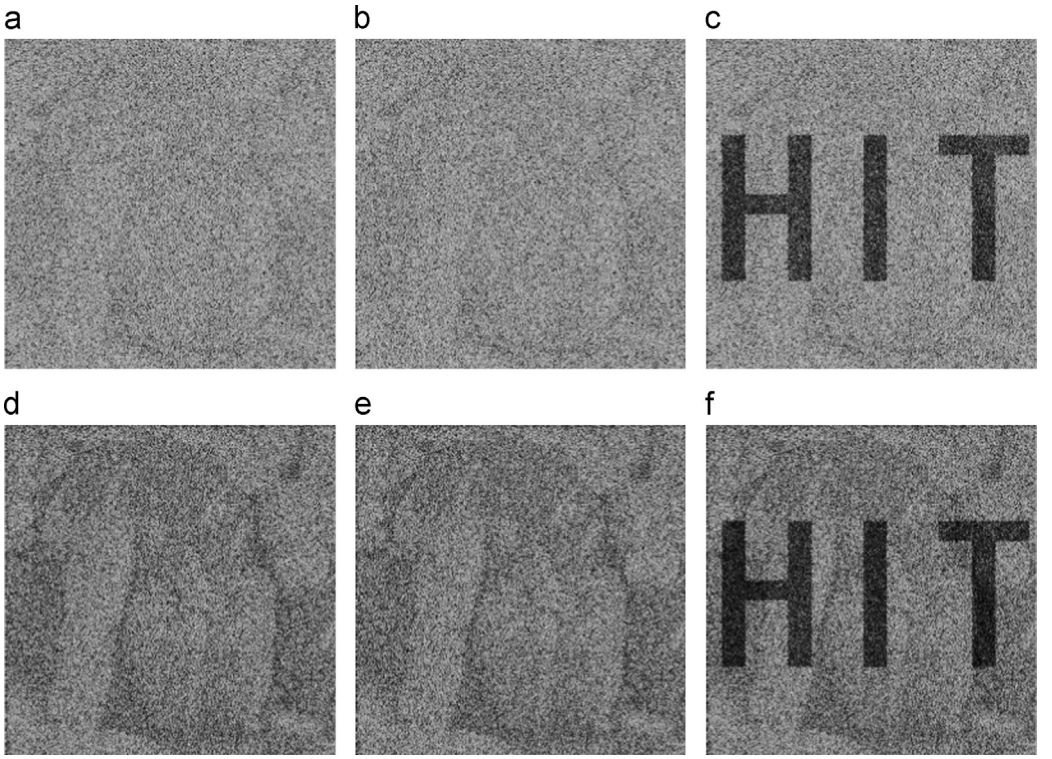

Fig. 12. Visual quality comparison of (2, 2) case by the proposed RG-based VC between values of $w_0=0.54,\ w_1=0.46$ and the suitable values of $w_0=0.50,\ w_1=0.34$. (a)–(b) the generated shares by $w_0=0.54,\ w_1=0.46$. The contrast is 0.0543 and 0.0545, respectively. (c) stacked results by two shares when $w_0=0.54,\ w_1=0.46$, where the contrast is 0.2016. The light transmissions stacked by two shares are 0.5404, 0.2894 and 0.4605, 0.2124, respectively. (d)–(e) the generated shares by $w_0=0.50,\ w_1=0.34$. The contrast is 0.1186 and 0.1177, respectively. (f) stacked results by two shares when $w_0=0.50,\ w_1=0.34$, where the contrast is 0.2032. The light transmissions stacked by two shares are 0.4195, 0.1797 and 0.5070, 0.3482, respectively.

suitable values, where the corresponding contrast and light transmission, i.e., $T^{w_0}(SC_{\{\otimes,1,2\}}[S(0)])$, $T^{w_0}(SC_{\{\otimes,1,2\}}[S(1)])$ and $T^{w_1}(SC_{\{\otimes,1,2\}}[S(0)])$, $T^{w_1}(SC_{\{\otimes,1,2\}}[S(1)])$, are also given. Based on Fig. 10(a)–(b) and Fig. 10(g)–(i), larger contrast of both the revealed secret image by two shares and shared image is obtained with the above suitable values, where $T^{w_0}(SC_{\{\otimes,1,2\}}[S(0)])-T^{w_1}(SC_{\{\otimes,1,2\}}[S(0)])=0.4849-0.3633=0.1216\approx\varepsilon$ and $T^{w_0}(SC_{\{\otimes,1,2\}}[S(1)])-T^{w_1}(SC_{\{\otimes,1,2\}}[S(1)])=0.2355-0.1328=0.1027\approx\varepsilon$, i.e., homogeneous conditions in Eqs. (8) and (9) are simultaneously satisfied.

Fig. 12 presents another example to show visual quality comparison of (2, 2) case by the proposed RG-based VC between arbitrary values of $w_0=0.54,\ w_1=0.46$ and the suitable values of $w_0=0.50,\ w_1=0.34$, where $\varepsilon=0.16>0$. The better results are also gained by the suitable values.

5.4. Comparisons

When $w_0=w_1=w\wedge k=2$, Fig. 8 illustrates the comparison between the proposed $(2,n)$ threshold RG-based meaningless VC and Wu and Suns $(2,n)$ RG-based meaningless VC [37], refer Section 5.1.

Comparison of visual quality between the proposed (k,n) threshold RG-based meaningful VC and Chen and Tsao's meaningful RG-based VC [31] is demonstrated in Fig. 13(a–f), where complementary shares are used in Chen and Tsao's approach to gain adjustable visual quality. In their method [31], the parameter which defines the portion of shared pixels in the meaningful share is set to be 0.5, where $\rho=1$, $T_S^W=0.5$ and corresponding contrast is also shown. In the proposed scheme, the two parameters are configured as $w_0=0.53,\ w_1=0.33$, where corresponding contrast is given as well. The contrasts of the reconstructed image are approximately the same, while lower contrasts of shared image quality is obtained by the proposed scheme. As a result, the proposed (k,n) threshold RG-based meaningful VC supports (k,n) threshold at the price of decreasing the visual quality of shared images. However, adopting complementary shares is not suitable for practical applications, since the complementary share does not resemble natural image. More comparison of visual quality between the proposed scheme and Chen and Tsao's method [31] is presented in Fig. 13(d–i), where complementary shares are not used in Chen and Tsao's approach and corresponding contrast is also given. Larger contrast of the revealed secret image is gained by the proposed scheme. In addition, the visual quality of Chen and Tsao's method for case $(2,n)$ is not adjustable. Above all, Chen and Tsao's meaningful RG-based VC [31] is not for (k,n) threshold.

Remark: evenness [43] can be the supplementary evaluation measurement of the visual quality when the contrast is nearly the same. Since in the above example, the contrast of

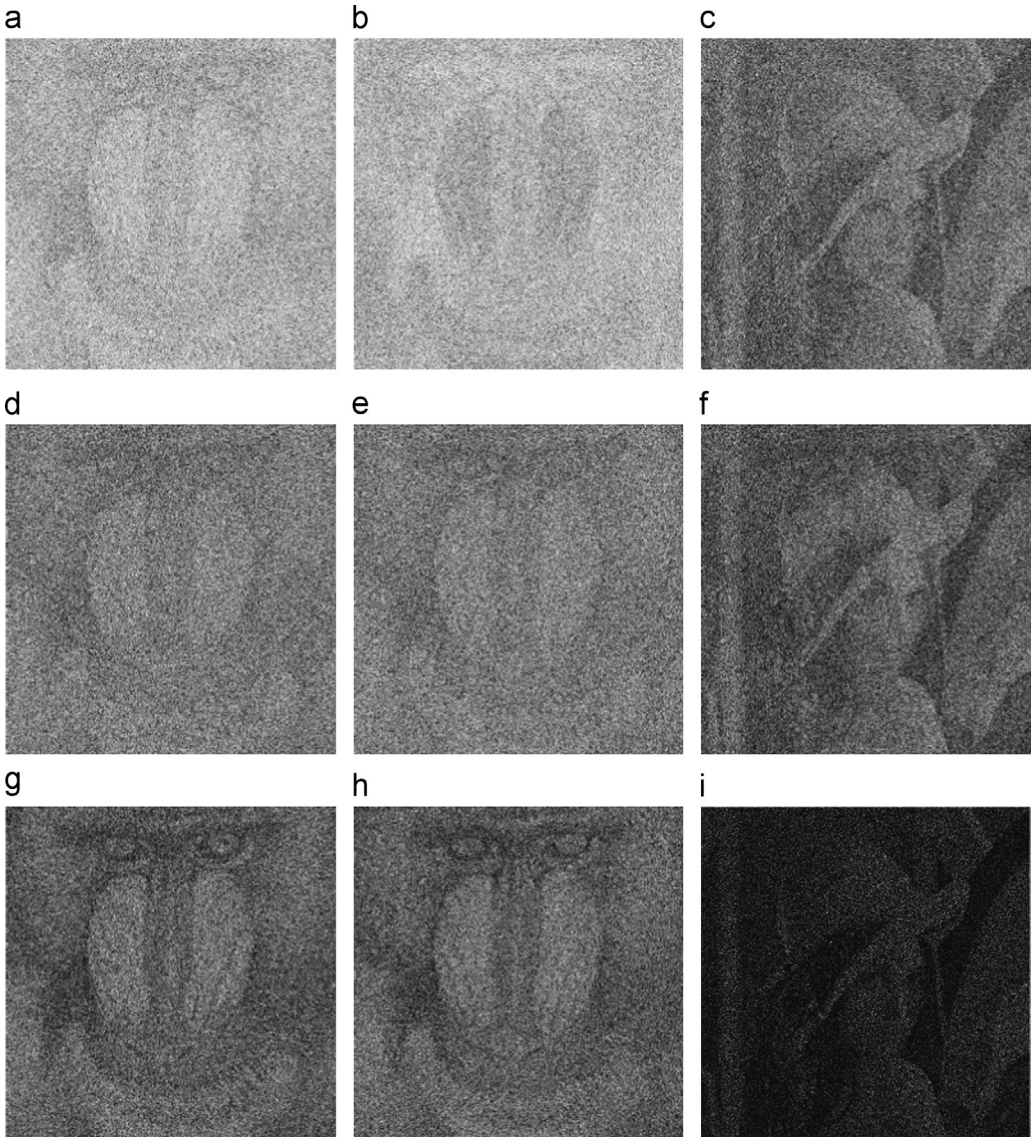

Fig. 13. Comparison of visual quality between the proposed RG-based VC and Chen and Tsao's meaningful RG-based VC [31]. (a)–(b) Two shares generated from [31], where $\alpha = 0.5$, $\rho = 1$, $T_S^W = 0.5$ and complementary shares are used in their method. The contrast is 0.1682 and -0.1431, respectively; (c) the recovered secret image by (a) and (b), where the contrast is 0.2003; (d)–(e) two shares generated from $(2, 2)$ case by the proposed RG-based VC, where $w_0 = 0.53, w_1 = 0.33$. The contrast is 0.1493 and 0.1484, respectively; (f) the recovered secret image by (d) and (e), where the contrast is 0.1945. (g)–(h) Two shares generated from [31], where complementary shares are not used in their approach. The contrast is 0.2869 and 0.2862, respectively; (c) the recovered secret image by (g) and (h), where the contrast is 0.1662.

the proposed scheme is different from that of Chen and Tsao's method [31], the visual quality comparison is evaluated by contrast in this paper.

Feature comparison, among the proposed scheme and related methods is shown in Table 2, where item 'Different cover images' denotes that different shares take visual information of different cover images, which maybe more efficient to manage different participants. Table 2 indicates, the proposed scheme has better properties than other competitive schemes. In addition, from the feature comparison among the proposed scheme and related methods with meaningful shares based on stacking decryption (Boolean OR operation), major advantages of the proposed scheme are that (1) shares are with meaningful contents, (2) (k, n) threshold is achieved and (3) no pixel expansion is obtained. Meanwhile, merits such as stacking decryption and no code book required are also maintained. While the disadvantage of ours is that each share takes the same visual information of the same one cover image instead of n. Visual information of one cover image is introduced by one pair of w_0 and w_1. Since only one pair of w_0 and w_1 is allowed and it is too hard to support more pairs, supporting n cover images is difficult in our framework.

We note that, we may establish a possible scheme by adopting probabilistic VCS approach on (k, n)−EVCS. The possible scheme may have similar features as the proposed scheme. However, our scheme does not require any encoding basis matrix, which is necessary in the probabilistic approach of EVCS.

Table 2
Comparison of feature among the proposed scheme and related methods.

Schemes	Threshold	Decryption	Pixel expansion	Codebook design	Meaningful share	Different cover images
Ref. [9]	(k,n)	Stacking	Yes	Yes	No	No
Ref. [24]	(k,n)	Stacking	No	Yes	No	No
Ref. [29]	(k,n)	Stacking	Yes	Yes	Yes	Yes
Ref. [10]	(k,n)	Boolean	No	No	No	No
Ref. [11]	(k,n)	Stacking	Yes	Yes	Yes	Yes
Ref. [27]	(k,n)	Stacking	Yes	Yes	Yes	Yes
Ref. [31]	$(2,2)/(2,n),(n,n)$	Stacking	No	No	Yes	No/Yes,Yes
Ref. [37]	$(2,n)/(n,n)$	Stacking/XOR	No	No	No/Yes	No
Ours	(k,n)	Stacking	No	No	Yes	No

6. Conclusion

This paper proposed a (k,n) threshold RG-based meaningful VC with meaningful shares, by exploiting generated RG to gain different light transmissions on shares at the cost of decreasing visual quality of shared images. Moreover, available values for the parameters are discussed. Simulations results and theoretical analysis show that the proposed (k,n) threshold RG-based meaningful VC is quality-adaptive without codebook design and pixel expansion. Improving the visual quality and supporting different cover images will be the future work.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable discussions. This work is supported by the National Natural Science Foundation of China (Grant number: 61100187, 61301099, 61361166006). The authors wish to thank Dr. Liyang yu, Dr. Jianzhi Sang, Prof. Qiong Li and Dr. Mahmoud Emam for their suggestions to improve this paper.

Appendix A. Proof of Lemma 1

Without losing of generality, $b_1, b_2, \ldots b_{k-2}, \tilde{b}_{k-1}$ are generated according to the secret pixel $S(i,j)$ in S by Step 3 and the other bits by Step 5.

According to Step 3, the shared pixel b_p is independent of the secret pixel $S(i,j)$, no matter the secret pixel is black or white, where $p=1,2,\ldots,k-2,\tilde{k-1}$ and $\tilde{k-1}$ denotes the subscript of $\tilde{b}_{k-1}$. Hence, $P(b_p=0)=\frac{1}{2}$ is achieved since b_p is generated randomly by flip-coin function, where $p=1,2,\ldots,k-2,\tilde{k-1}$.

Based on Step 5, the shared pixel b_q, where $q=k-1,k,k+1,\ldots,n$, is independent of the secret pixel $S(i,j)$. As a result, $P(b_q=0)=w$ is obtained.

From Step 6, the n pixels $b_1, b_2, \ldots b_{n-1}, b_n$ are evenly assigned to $SC_1(i,j), SC_2(i,j), \ldots SC_n(i,j)$. By Definition 2, we have $T(SC_i[S(0)])=T(SC_i[S(1)])=(\frac{1}{2}(k-2)+w(n-k+2))/n$. Thus, Lemma 1 is proved to be met. □

Appendix B. Proof of Lemma 2

Assume t pixels $b_{i_1}, b_{i_2}, \ldots b_{i_t}$ is a subset of $b_1, b_2, \ldots b_{n-1}, b_n$, $t=t_1+t_2$, the first t_1 pixels $b_{i_1}, b_{i_2}, \ldots b_{i_{t_1}}$ are generated by Step 3, and the last t_2 pixels $b_{i_{t_1+1}}$, $b_{i_{t_1+2}}, \ldots b_{i_{t_1+t_2}}$ are introduced by Step 5, where $0 \le t_1 \le k-2, 0 \le t_2 \le n-k+2$, and $1 \le t \le k-1$.

In order to prove the stacked pixels $b_{\{\otimes,i_1,i_2,\ldots i_t\}}$ gives no clue about the secret pixel $S(i,j)$ for any subset of integers $\{i_1,i_2,\ldots i_t\} \subseteq \{1,2,\ldots,n\}$, two cases are considered: Case 1: $t_2>1$ and Case 2: $t_2 \le 1$.

Case 1: $t_2>1$. In this case, the bit $\tilde{b}_{k-1}$ should be recovered by $b_{\{\otimes,i_{t_1+1},i_{t_1+2},\cdots i_{t_1+t_2}\}}$. $b_{\{\otimes,i_{t_1+1},i_{t_1+2},\cdots i_{t_1+t_2}\}}$ probabilistically looks like the independent pixel $\tilde{b}_{k-1}$ and the probability is $(w+w^{t_2})/2$ by Lemma 1.

We consider $b_u \otimes \cdots \otimes b_v \otimes \tilde{b}_{k-1}$ with $u,\ldots,v$ being the indices in $\{i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}$ besides $\tilde{k-1}$. The bit $\tilde{b}_{k-2}$ should be recovered by b_{k-2} and $\tilde{b}_{k-1}$.

Assume that $k-2 \in \{i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}$, then $b_{\{\otimes,i_1,i_2,\ldots i_t\}}=b_u \otimes \cdots \otimes b_v \otimes b_{k-2} \otimes b_z \otimes \tilde{b}_{k-1}=b_u \otimes \cdots \otimes b_{v-1} \otimes \tilde{b}_{k-2}$ with $u,\ldots,z$ being the indices in $\{i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}$ besides $k-2$ and $\tilde{k-1}$, where $b_{k-2} \otimes \tilde{b}_{k-1}$ probabilistically looks like the independent pixel $\tilde{b}_{k-2}$ and the light transmission $T[b_{k-2} \otimes \tilde{b}_{k-1}]=(1/2)^2$ by Lemma 1.

Actually, the pixels $b_1, b_2, \ldots b_{k-2}, \tilde{b}_{k-1}$ are generated by flip-coin function except $\tilde{b}_{k-1}$ so that $b_1, b_2, \ldots b_{k-2}$ are independent of the corresponding secret pixel $S(i,j)$. Hence, by stacking any t pixels the light transmissions are obtained as

$$\begin{aligned}
&T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]\right]\\
&=T\left[b_{\{\otimes,i_1,i_2,\ldots i_{t_1},i_{t_1+1},i_{t_1+2},\cdots i_{t_1+t_2}\}}[S(0)]\right]\\
&=T\left[b_{\{\otimes,i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}}[S(0)]\right]\times(w+w^{t_2})/2\\
&=T\left[b_{\{\otimes,u,u+1,\ldots v-1,k-2,\tilde{k-1}\}}[S(0)]\right]\times(w+w^{t_2})/2\\
&=(1/2)^{t_1-1}\times(1/2)^2\times(w+w^{t_2})/2\\
&=(1/2)^{t_1+2}\times(w+w^{t_2})
\end{aligned}$$

and $T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]\right]=(1/2)^{t_1+1}\times(w+w^{t_2})$ by Lemma 1.

If $k-2 \notin \{i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}$, then all the t_1+1 pixels $b_{i_1}, b_{i_2}, \ldots b_{i_{t_1}}, \tilde{b}_{k-1}$ are independent and $T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]\right]=T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]\right]=(1/2)^{t_1+1}\times(w+w^{t_2})$ by Lemma 1.

Case 2: $t_2 \le 1$. Except for $\tilde{b}_{k-1}$ the pixels $b_1, b_2, \ldots b_{k-2}$ are generated by flip-coin function and independent of the corresponding secret pixel $S(i,j)$ so that the result of stacking any t_1+1 bits of indicates $\{i_1,i_2,\ldots i_{t_1},\tilde{k-1}\}$

with $T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]\right]=T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]\right]=(1/2)^{t_1+1}\times(w+w^{t_2})$ by Lemma 1.

By Definition 4, stacking less than k shares cannot disclose the secret. □

Appendix C. Proof of Lemma 3

By Lemma 2, when $t_1=k-2$, then $2\le t_2$.

First, we prove when $S(i,j)=0$, $T\left[b_{\{\otimes,1,2,\ldots,k-2,\ \tilde{k-1}\}}\right]=T\left[b_{\{\otimes,1,2,\ldots,k-2\}}\right]=(1/2)^{k-2}$, while when $S(i,j)=1$, $T\left[b_{\{\otimes,1,2,\ldots,k-2,\tilde{k-1}\}}\right]=0$.

When $S(i,j)=0$, if $\tilde{b}_{k-1}=0$, then $b_{\{\otimes,1,2,\ldots,k-2,\ \tilde{k-1}\}}=b_{\{\otimes,1,2,\ldots,k-2\}}$ sets up.

Else if $\tilde{b}_{k-1}=1$, then $\tilde{b}_{k-1}$ should be equal to one of $b_1,b_2,\ldots b_{k-2}$. If not, each of $b_1,b_2,\ldots b_{k-2}$ is complementary to $\tilde{b}_{k-1}$ so that $b_1=b_2=\cdots=b_{k-2}=0$. In addition, $S(i,j)=b_1\oplus b_2\oplus\cdots\oplus b_{k-2}\oplus\tilde{b}_{k-1}$ [32]. As a result $S(i,j)=0\oplus 0\cdots\oplus 0\oplus 1=1$ with contradiction to $S(i,j)=0$. Hence, $\tilde{b}_{k-1}$ is equal to one of $b_1,b_2,\ldots b_{k-2}$, then $b_{\{\otimes,1,2,\ldots,k-2,\tilde{k-1}\}}=b_{\{\otimes,1,2,\ldots,k-2\}}$ also sets up.

Thus, if $S(i,j)=0$, we have $T\left[b_{\{\otimes,1,2,\ldots,k-2,\tilde{k-1}\}}\right]=T\left[b_{\{\otimes,1,2,\ldots,k-2\}}\right]=(1/2)^{k-2}$ by Lemma 1.

In a similar way, when $S(i,j)=1$, we have $T\left[b_{\{\otimes,1,2,\ldots,k-2,\tilde{k-1}\}}\right]=0$

Second, by the Case 1 of Lemma 2, the bit $\tilde{b}_{k-1}$ should be recovered by $b_{\{\otimes,i_{t_1+1},i_{t_1+2},\cdots i_{t_1+t_2}\}}$.

If $S(i,j)=0$, when $b_{k-2}=0\wedge\tilde{b}_{k-2}=0$, as a result $\tilde{b}_{k-1}=0$ according to Step 3. By step 5, $P\left(b_{\{\otimes,i_{t_1+1},i_{t_1+2},\ldots i_{t_1+t_2}\}}=0\right)=w$.

Hence, $T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)]\right]=T\left[b_{\{\otimes,1,2,\ldots k-2,\tilde{k-1}\}}[S(0)]\right]\times w=(1/2)^{k-2}\times w$.

While if $S(i,j)=0$, when $b_{k-2}=0\wedge\tilde{b}_{k-2}=1$, as a result $\tilde{b}_{k-1}=1$ according to Step 3. By step 5, $P(b_{\{\otimes,i_{t_1+1},i_{t_1+2},\ldots i_{t_1+t_2}\}}=0)=w^{t_2}$.

Hence, $T\left[b_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)]\right]=T\left[b_{\{\otimes,1,2,\ldots k-2,\tilde{k-1}\}}[S(1)]\right]\times w^{t_2}=(1/2)^{k-2}\times w^{t_2}$.

Finally, since $w<1$, we have $T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(0)])>T(SC_{\{\otimes,i_1,i_2,\ldots i_t\}}[S(1)])$. As a result, based on Defi;nition 4, the stacking result by any $t\ge k$ shares visually reveals the secret. □

References

[1] L. An, X. Gao, Y. Yuan, D. Tao, Robust lossless data hiding using clustering and statistical quantity histogram, Neurocomputing 77 (1) (2012) 1–11.

[2] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng, F. Ji, Content-adaptive reliable robust lossless data embedding, Neurocomputing 79 (2012) 1–11.

[3] L. An, X. Gao, X. Li, D. Tao, C. Deng, J. Li, Robust reversible watermarking via clustering and enhanced pixel-wise masking, IEEE Trans. Image Process. 21 (8) (2012) 3598–3611.

[4] L. Li, A.A.A. El-Latif, Z. Shi, X. Niu, A new loss-tolerant image encryption scheme based on secret sharing and two chaotic systems, Res. J. Appl. Sci. Eng. Technol. 4 (2012) 877–883.

[5] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[6] C.-C. Thien, J.-C. Lin, Secret image sharing, Comput. Graph. 26 (5) (2002) 765–770.

[7] C.-N. Yang, C.-B. Ciou, Image secret sharing method with two-decoding-options: lossless recovery and previewing capability, Image Vis. Comput. 28 (12) (2010) 1600–1610.

[8] P. Li, P.-J. Ma, X.-H. Su, C.-N. Yang, Improvements of a two-in-one image secret sharing scheme based on gray mixing model, J. Vis. Commun. Image Represent. 23 (3) (2012) 441–453.

[9] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques, May 9–12, Springer, Springer, Perugia, Italy, 1995, pp. 1–12.

[10] D. Wang, L. Zhang, N. Ma, X. Li, Two secret sharing schemes based on boolean operations, Pattern Recognit. 40 (10) (2007) 2776–2785.

[11] Z. Wang, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 383–396.

[12] J. Weir, W. Yan, A comprehensive study of visual cryptography, in: Transactions on DHMS V, Lecture Notes in Computer Science, vol. 6010, Springer-Verlag, Springer, Berlin, Heidelberg, 2010, pp. 70–105.

[13] S. Lee, C.D. Yoo, T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 321–330.

[14] C. Blundo, A. De Bonis, A. De Santis, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24 (3) (2001) 255–278.

[15] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inf. Comput. 129 (2) (1996) 86–106.

[16] N. Krishna Prakash, S. Govindaraju, Visual secret sharing schemes for color images using halftoning, in: International Conference on Conference on Computational Intelligence and Multimedia Applications, vol. 3, IEEE, IEEE, Karachi, 2007, pp. 174–178.

[17] H. Luo, F. Yu, J.-S. Pan, Z.-M. Lu, Robust and progressive color image visual secret sharing cooperated with data hiding, in: Eighth International Conference on Intelligent Systems Design and Applications, ISDA'08, vol. 3, IEEE, IEEE, Kaohsiung, Taiwan, 2008, pp. 431–436.

[18] Y.-C. Hou, Visual cryptography for color images, Pattern Recognit. 36 (7) (2003) 1619–1629.

[19] F. Liu, C.K. Wu, X.J. Lin, Colour visual cryptography schemes, IET Inf. Secur. 2 (4) (2008) 151–165.

[20] S.J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, K. Chen, Sharing multiple secrets in visual cryptography, Pattern Recognit. 40 (12) (2007) 3633–3651.

[21] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Cryptogr. 25 (1) (2002) 15–61.

[22] F. Liu, C. Wu, X. Lin, Step construction of visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 5 (1) (2010) 27–38.

[23] H. Kuwakado, H. Tanaka, Image size invariant visual cryptography, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 82 (10) (1999) 2172–2177.

[24] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognit. Lett. 25 (4) (2004) 481–494.

[25] S. Cimato, R. De Prisco, A. De Santis, Probabilistic visual cryptography schemes, Comput. J. 49 (1) (2006) 97–107.

[26] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor. Comput. Sci. 250 (1) (2001) 143–161.

[27] F. Liu, C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Secur. 6 (2) (2011) 307–322.

[28] C.-N. Yang, Y.-Y. Yang, New extended visual cryptography schemes with clearer shadow images, Inf. Sci. 271 (2014) 246–263.

[29] Z. Zhou, G.R. Arce, G. Di Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15 (8) (2006) 2441–2453.

[30] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (6) (1987) 377–379.

[31] T.H. Chen, K.H. Tsao, User-friendly random-grid-based visual secret sharing, IEEE Trans. Circuit Syst. Video Tech. 21 (11) (2011) 1693–1703.

[32] X. Wu, W. Sun, Improving the visual quality of random grid-based visual secret sharing, Signal Process. 93 (5) (2013) 977–995.

[33] T. Guo, F. Liu, C. Wu, Threshold visual secret sharing by random grids with improved contrast, J. Syst. Softw. 86 (8) (2013) 2094–2109.

[34] S.J. Shyu, Image encryption by random grids, Pattern Recognit. 40 (3) (2007) 1014–1031.

[35] T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, Pattern Recognit. 42 (11) (2009) 2203–2217.

[36] T.-H. Chen, Y.-S. Lee, W.-L. Huang, J.S.-T. Juan, Y.-Y. Chen, M.-J. Li, Quality-adaptive visual secret sharing by random grids, J. Syst. Softw. 86 (5) (2013) 1267–1274.

[37] X. Wu, W. Sun, Generalized random grid and its applications in visual cryptography, IEEE Trans. Inf. Forensics Secur. (2013) 1541–1553.

[38] T.-H. Chen, K.-H. Tsao, Image encryption by (n,n) random grids, in: Proceedings of Eighteenth Information Security Conference, IEEE, IEEE, Hualien, 2008.
[39] T.-H. Chen, K.-H. Tsao, Threshold visual secret sharing by random grids, J. Syst. Softw. 84 (7) (2011) 1197–1208.
[40] X. Yan, S. Wang, X. Niu, Threshold construction from specific cases in visual cryptography without the pixel expansion, Signal Process. 105 (2014) 389–398.
[41] C.-N. Yang, C.-C. Wu, D.-S. Wang, A discussion on the relationship between probabilistic visual cryptography and random grid, Inf. Sci. 278 (2014) 141–173.
[42] X. Yan, S. Wang, X. Niu, Equivalence proof of two (2, n) progressive visual secret sharing, in: The Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP-2014).
[43] F. Liu, C. Wu, L. Qian, et al., Improving the visual quality of size invariant visual cryptography scheme, J. Vis. Commun. Image Represent. 23 (2) (2012) 331–342.