

An enhanced threshold visual secret sharing based on random grids

Xuehu Yan¹ · Xin Liu^{2,3} · Ching-Nung Yang⁴

Received: 28 March 2015 / Accepted: 14 October 2015 / Published online: 27 October 2015
© Springer-Verlag Berlin Heidelberg 2015

Abstract Random grids (RG)-based visual secret sharing (VSS) scheme can easily avoid the pixel expansion problem as well as requires no codebook design. However, previous scheme still suffers from low visual quality. In this paper, a new threshold RG-based VSS scheme aiming at improving the visual quality of the previewed image is presented. Compared with previous schemes, our scheme can gain better visual quality in the reconstructed images as well as (k, n) threshold. In addition, the factor affecting the visual quality is analyzed and the differences between related approaches are discussed.

Keywords Real-time · Visual cryptography · Progressive visual secret sharing · Random grids · Threshold

1 Introduction

Naor and Shamir [13] first proposed the threshold-based visual cryptography scheme (VCS) [2, 11, 16–18, 21, 22, 24]. In their scheme, a binary secret image is shared by generating corresponding n noise-like shadow images. And any k or more noise-like shadow images are stacking to recover the secret image visually based on human visual

system (HVS). However, less than k participants cannot reveal any information of the secret image by inspecting their shares. The main advantage of VCS by [13] is simple recovery, which means the decryption of secret image is completely based on stacking or HVS without any cryptographic computation. However, the scheme suffers from codebook (basic matrices) design and pixel expansion [18]. In order to solve the pixel expansion problem, some previous VCSs without the pixel expansion were proposed. Ito et al. [9] proposed the probabilistic VCS by equally selecting a column from corresponding basic matrix. Probabilistic VCS for different thresholds was presented by Yang [24]. Cimato et al. [2] further extended the generalization probabilistic VCS.

Visual secret sharing (VSS) by random grids (RG) [3, 4, 25] has gained much attention since it can avoid the pixel expansion problem as well as requires no codebook design. Encryption of binary secret images based on RG was first presented by Kafri and Keren [8], each of which is generated into two noise-like RGs (also called shadow images or share images) that have the same size as the original secret image. The decryption operation is the same as traditional VCS. However, the relative RG-based VSS schemes [6, 8, 10, 15, 20, 23] are only for cases $(2, 2)$, $(2, n)$ or (n, n) .

For the case (k, n) , Chen and Tsao [1] proposed a RG-based (k, n) threshold VSS by applying $(2, 2)$ RG-based VSS repeatedly for the first k bits and generating the last $n - k$ bits randomly.

Then, Wu and Sun [19] improved the visual quality of recovered secret image in [1] through changing the last $n - k$ bits from randomly selecting to be equal to the k th bit. Recently, Guo et al. [5] improved the visual quality of Chen and Tsao's scheme [1] in another approach. They applied Chen and Tsao's scheme [1] for every k bits and

✉ Xuehu Yan
publictiger@126.com

¹ Electronic Engineering Institute, 230037 Hefei, China

² School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin, China

³ Modern Educational Technology Center, Harbin University of Science and Technology, 150080 Harbin, China

⁴ Department of CSIE, National Dong Hwa University, Hualien 974, Taiwan

$N_k = \lfloor n/k \rfloor$ times, and set the last $n - N_k \times k$ bits randomly. However, the visual quality of the revealed secret image is still poor in their schemes [5, 19].

In this paper, a new RG-based (k, n) threshold VSS scheme is proposed, which has better visual quality than both Wu and Sun's scheme [19] and Guo et al.'s scheme [5]. In our design, based on analyzing the factors that affect the visual quality, we better utilize the random bits in the n bits to remedy the contrast and the visual quality. The result obtained by the proposed scheme is much better than those obtained by [19] and [5]. In addition, the property of getting higher contrast makes our method also suitable for more complex images, such as gray level and color images.

The rest of the paper is organized as follows. Section 2 introduces some basic requirements and related works for the proposed scheme. In Sect. 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. Finally, Sect. 6 concludes this paper.

2 Preliminaries

In this section, we give some preliminaries and related works, i.e., RG-based [1, 5, 19] VSS, as the basis for the proposed scheme. In what follows, symbols \oplus and \otimes denote the Boolean XOR and OR operations. b is a bit-wise complementary operation of a bit b . The binary secret image S is shared among n shadow images, while the recovered secret image S' is recovered from $t(2 \leq t \leq n, t \in Z^+)$ shadow images by stacking.

For a certain pixel x in binary image X with size of $M \times N$, the probability of pixel color is transparent or white (0), say $P(x=0)$, and the same for pixel color is opaque or black (1). Besides, $P(S=0) = 1 - \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N S(i,j)$, $1 \leq i \leq M, 1 \leq j \leq N$.

AS0 (resp., AS1) denotes the white (resp., black) area of original secret image S defined as $AS0 = \{(i,j) | S(i,j) = 0, 1 \leq i \leq M, 1 \leq j \leq N\}$ (resp., $AS1 = \{(i,j) | S(i,j) = 1, 1 \leq i \leq M, 1 \leq j \leq N\}$).

Definition 1 (Contrast) The visual quality, which will decide how well human eyes could recognize the recovered image, of the recovered secret image S' corresponding to the original secret image S is evaluated by contrast defined as follows [1, 14]:

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S'[AS0] = 0) - P(S'[AS1] = 0)}{1 + P(S'[AS1] = 0)} \quad (1)$$

where α denotes contrast, P_0 (resp., P_1) is the appearance probability of white pixels in the recovered image S' in the corresponding white (resp., black) area of original secret image S , that is, P_0 is the correctly decrypted probability

corresponding to the white area of original secret image S , and P_1 is the wrongly decrypted probability corresponding to the black area of original secret image S .

Definition 2 (Visually recognizable) [1, 13] The recovered secret image S' could be recognized as the corresponding original secret image S if $\alpha > 0$ when $t \geq k$.

Definition 3 (Security) [1, 13] The scheme is secure if $\alpha = 0$ when $t < k$, which means no information of S could be recognized through S'

Generally speaking, a valid VC construction should satisfy two conditions:

1. Security condition corresponding to Definition 3: security condition means that insufficient shares give no clue about secret, i.e., $P_0 = P_1$.
2. Contrast condition corresponding to Definition 2: contrast condition indicates that sufficient shares reveal the secret, i.e., $\alpha > 0$.

Remark Both contrast and evenness can measure the visual quality of the recovered secret image. The evenness is generally represented with the variance of the darkness levels of a block. Contrast is more significant than evenness to evaluate visual quality. Evenness [12] can be the supplementary evaluation measurement for the visual quality when the contrast is nearly the same. Since the contrast of the proposed scheme is different from that of the related methods, which will be shown in Sect. 5, the visual quality of revealed secret image is evaluated by contrast in this paper. The contrast is expected to be as large as possible to obtain better visual quality.

In RG-based VSS [1], shadow images covered secret after sharing are denoted as SC_p . The recovered secret image is denoted as S' . Here 0 denotes white pixel, 1 denotes black pixel. The generation and recovery phases of original (2, 2) RG-based VSS are described below.

Step 1: Randomly generate 1 RG SC_1 .

Step 2: Compute SC_2 as in Eq. (2).

Recovery $S' = SC_1 \otimes SC_2$ as in Eq. (3). If a certain secret pixel $s = S(i,j)$ of S is 1, the recovery result $SC_1 \otimes SC_2 = 1$ is always black. If a certain secret pixel is 0, the recovery result $SC_1 \otimes SC_2 = SC_1(i,j) \otimes SC_2(i,j)$ has half chance to be black or white since SC_1 is generated randomly.

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & \text{if } S = 0 \\ \overline{SC_1(i,j)} & \text{if } S = 1 \end{cases} \quad (2)$$

$$S'(i,j) = SC_1(i,j) \otimes SC_2(i,j) = \begin{cases} SC_1(i,j) \otimes \overline{SC_1(i,j)} & \text{if } S(i,j) = 0 \\ SC_1(i,j) \otimes SC_1(i,j) = 1 & \text{if } S(i,j) = 1 \end{cases} \quad (3)$$

In fact, Eq. (2) is equal to $sc_2 = sc_1 \oplus s$ or $s = sc_1 \oplus sc_2$. Since if $s = 0 \Rightarrow sc_2 = sc_1 \oplus 0 \Rightarrow sc_2 = sc_1$, and if

$s = 1 \Rightarrow sc_2 = sc_1 \oplus 1 \Rightarrow sc_2 = \overline{sc_1}$. The same equation could be extended to $s = sc_1 \oplus sc_2 \oplus \dots \oplus sc_k$ and the same approach can be extended to (k, n) threshold scheme by applying the above process repeatedly for the first k bits and generating the last $n - k$ bits randomly. (k, n) RG-based VSS is described as follows:

3.1 Scheme: visual quality-enhanced threshold VSS based on random girds

Prior to give the detail of the proposed scheme, the diagrammatic design concepts comparison between the proposed scheme and related schemes is shown in Fig. 1.

Algorithm 1: Chen and Tsao's (k, n) RG-based VSS
Input: A $M \times N$ binary secret image S , the threshold parameters (k, n)
Output: n shadow images SC_1, SC_2, \dots, SC_n
Step 1: For each position $(i, j) \in \{(i, j) 1 \leq i \leq M, 1 \leq j \leq N\}$, repeat Steps 2-6
Step 2: Select $b_1, b_2, \dots, b_k \in \{0, 1\}$ randomly.
Step 3: If $S(i, j) = b_1 \oplus b_2 \dots \oplus b_k$, go to Step 5; else go to Step 4
Step 4: Randomly select $p \in \{1, 2, \dots, k\}$ flip $b_p = \overline{b_p}$ (that is $0 \rightarrow 1$ or $1 \rightarrow 0$).
Step 5: Select $b_{k+1}, b_{k+2}, \dots, b_n \in \{0, 1\}$ randomly.
Step 6: Randomly rearrange b_1, b_2, \dots, b_n to $SC_1(i, j), SC_2(i, j), \dots, SC_n(i, j)$
Step 7: Output the n shadow images SC_1, SC_2, \dots, SC_n

In addition, Wu and Sun's scheme [19] improves the contrast of the scheme [1] by change the last $n - k$ bits to be equal to k th bit in step 5 of Chen and Tsao's (k, n) RG-based VSS.

Guo et al. [5] improve the visual quality of Chen and Tsao's scheme [1] in another approach, that is computing every k bits by applying Chen and Tsao's scheme for

There are some random bits, such as the middle $(N_k - 1) \times k$ bits and the last $n - k$ bits in the previous schemes [1, 5, 19], which are applied for improving the visual quality in the proposed scheme.

The shadow images generation architecture of the proposed scheme is illustrated in Fig. 2, the algorithmic steps are described in Algorithm 2.

Algorithm 2. The proposed scheme
Input: A $M \times N$ binary secret image S , the threshold parameters (k, n)
Output: n shadow images SC_1, SC_2, \dots, SC_n
Step 1: For each position $(i, j) \in \{(i, j) 1 \leq i \leq M, 1 \leq j \leq N\}$, repeat Steps 2-4
Step 2: Compute b_1, b_2, \dots, b_k one by one repeatedly using Eq. (2) Where b_x denotes the temporary pixels, $x = 1, 2, \dots, n - 1, n$
Step 3: Set $b_{k+1} = b_1, b_{k+2} = b_2, \dots, b_{2k} = b_k, b_{2k+1} = b_1, \dots$ if $(n \bmod k) = 0, b_n = b_k$ else $b_n = b_{(n \bmod k)}$.
Step 4: Randomly rearrangement b_1, b_2, \dots, b_n to $SC_1(i, j), SC_2(i, j), \dots, SC_n(i, j)$
Step 5: Output the n shadow images SC_1, SC_2, \dots, SC_n

$N_k = \lfloor n/k \rfloor$ times, and setting the last $n - N_k \times k$ bits randomly. The details of the schemes may refer to [5, 19].

Based on the above three RG-based VSS schemes, there are random bits in the corresponding n bits. The random bits are utilized in Wu and Sun's scheme and Guo et al.'s scheme to improve the visual quality in different methods. In this paper, the random bits are better utilized to gain enhanced visual quality. The differences between the proposed scheme and other schemes will be compared and analyzed in Sect. 5.3.

3 The proposed scheme

Here, we propose a novel (k, n) (generally $n, k \in \mathbb{Z}^+, 2 \leq k \leq n$) VSS based on RG.

The secret recovery of the proposed scheme is also based on stacking (\otimes) or HVS.

The idea of Algorithm 2 is described precisely as follows:

There are random bits in the n bits. The random bits could be utilized to gain better properties, such as threshold mechanism, and improving the visual quality. In step 2 of Algorithm 2, the k bits are utilized to gain threshold mechanism [1], i.e., when less than k shadow images are collected, the secret cannot be revealed, which are the same as Chen and Tsao's scheme, Wu and Sun's scheme, and Guo et al.'s scheme. While step 3 of Algorithm 2 aims to improve the visual quality of recovered secret image by a different way to utilize the last $n - k$ bits, through which the probability of covering b_1, b_2, \dots, b_k in the recovered t bits is improved. In

Fig. 1 The design concepts comparison between the proposed scheme and related schemes

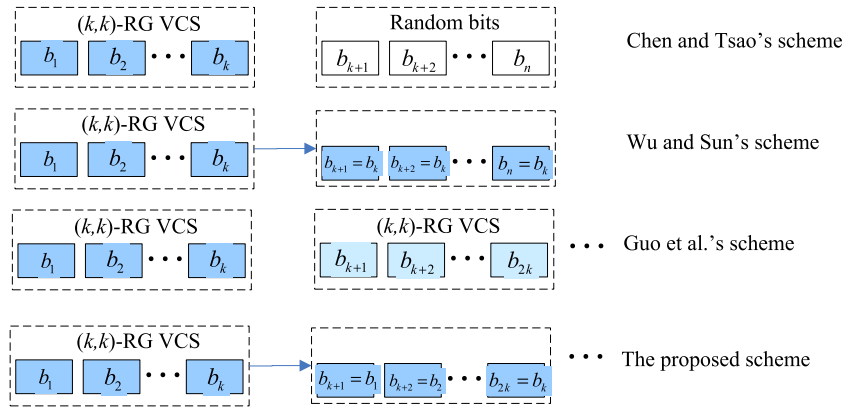
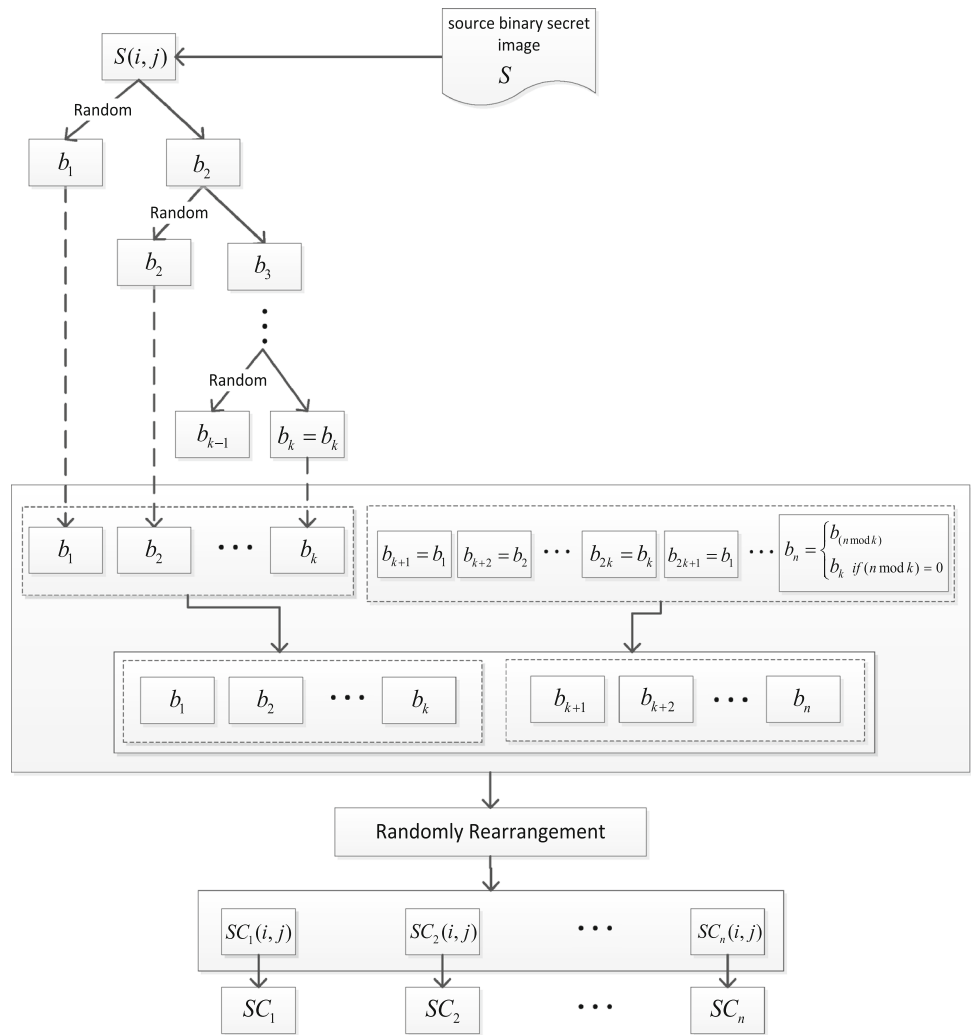


Fig. 2 Shadow images generation architecture of the proposed scheme



step 4 of Algorithm 2, aiming to make all the shadow images be equal to each other, the generated n bits are randomly rearranged to corresponding n shadow images bits.

3.2 Extension to grayscale/color images

The proposed scheme can be extended to share grayscale/color images [1, 7, 19]. To share a grayscale image,

halftone technologies such as error diffusion [17] are applied to convert the grayscale image into binary image, then the proposed scheme could be used.

For sharing a color image, color decomposition, halftone technologies and color composition are applied. A color image can be described by color model. Here, CMY (cyan–magenta–yellow) model will be applied, which is subtractive color model, and displays a color by reflecting light from a surface of an object. Based on the color model, a color image can be processed by three grayscale images (R, G, B) with the same extension methods for sharing grayscale images.

4 Performance analyses

This section gives the performances of the proposed scheme by theoretically analyzing the security and the visual quality. By Theorem 1, we prove that proposed scheme is a valid (k, n) threshold VSS construction when stacking decryption is applied. Before the proof of Theorem 1, two Lemmas are proved.

The essences of the security and performance (visually recognizable) are analyzed as follows:

1. Every single shadow image is secure: which means there is no cross interference of the secret image in every shadow image, i.e. every single shadow image could reveal nothing of the secret image. Aiming to realize this, every bit sc_i in sc_1, sc_2, \dots, sc_n should be random, no relationship with or not decided by corresponding secret bit s .
2. Collusion attack security: which means nothing of the secret image can be revealed with less than k shadow images. Aiming to realize this, any t bits $SC_{j_1}, SC_{j_2}, \dots, SC_{j_t}, t \leq k - 1$ in sc_1, sc_2, \dots, sc_n cannot decide the corresponding secret bit s .
3. Visually recognizable: which means part of the secret image will be revealed with k or more shadow images. Aiming to realize this, any t bits $SC_{j_1}, SC_{j_2}, \dots, SC_{j_t}, t \geq k$ in sc_1, sc_2, \dots, sc_n can decide the corresponding secret bit s in a certain probability.

The random rearrangement in the related schemes will lead to different combinations for the t bits in the corresponding t collected shadow images. In addition, the contrast in Definition 1 is based on statistics, hence there is a certain probability. In the following Sections, we will know that the “certain probability” is the probability of picking up b_1, b_2, \dots, b_k bits from the t bits.

The related RG-based VSS [1, 5, 19] utilizes the random bits to improve the “certain probability” (the visual quality), under the secure condition, where “certain probability” is the probability that can correctly reconstruct the secret pixels, i.e., the probability of introducing the contrast.

Lemma 1 Assume sc_1, sc_2, \dots, sc_k are generated by the proposed scheme, we have $s = sc_1 \oplus sc_2 \oplus \dots \oplus sc_k$.

Proof Taking the first k bits, as an example, for the proof. Intuitively, Eq. (2) is equal to Eq. (4).

$$sc_2 = sc_1 \oplus s \quad \text{or} \quad s = sc_1 \oplus sc_2 \tag{4}$$

Since if $s = 0 \Rightarrow sc_2 = sc_1 \oplus 0 \Rightarrow sc_2 = sc_1$, and if $s = 1 \Rightarrow sc_2 = sc_1 \oplus 1 \Rightarrow sc_2 = \overline{sc_1}$. And the equations will be used in the proposed scheme. The same approach could be extended to

$$s = sc_1 \oplus sc_2 \oplus \dots \oplus sc_k \tag{5}$$

In the recovery phase, in a similar way, the recovered secret bit by stacking any $t (k \leq t \leq n)$ bits of shadow images satisfies to:

$$s = sc_1 \otimes sc_2 \otimes \dots \otimes sc_t \tag{6}$$

Recall that “0” denotes white pixels, “1” denotes black pixels. The first k bits before the rearrangement have the relationship in Eq. (5) of the generation phase, stacking t bits have the relationship in Eq. (6) of the recovery phase.

Without loss of generality, in the following proof, we assume sc_1, sc_2, \dots, sc_n are corresponding to b_1, b_2, \dots, b_n . □

Lemma 2 In the proposed scheme, if $s = 0, P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS0] = 0) = P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0) = (1/2)^{k-1}$. if $s = 1, P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS1] = 0) = 0$. Where $SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}$ denotes $SC_1 \otimes SC_2 \dots \otimes SC_k$.

Proof Generally, the bits $sc_1, sc_2, \dots, sc_{k-1}$ are random and independent with each other and $s \cdot sc_k$ is related with and dependent on $sc_1 \oplus sc_2 \oplus \dots \oplus sc_{k-1}$ and s according to Eq. (5) of Lemma 1.

Hence,

$$\begin{aligned} P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0) &= (1/2)^{k-1}, \\ P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS1] = 0) &= (1/2)^{k-1} \end{aligned} \tag{7}$$

If $s = 0$, based on Eq. (5) and Eq. (6), we will prove:

$$\begin{aligned} P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS0] = 0) &= P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0) \\ &= (1/2)^{k-1} \end{aligned} \tag{8}$$

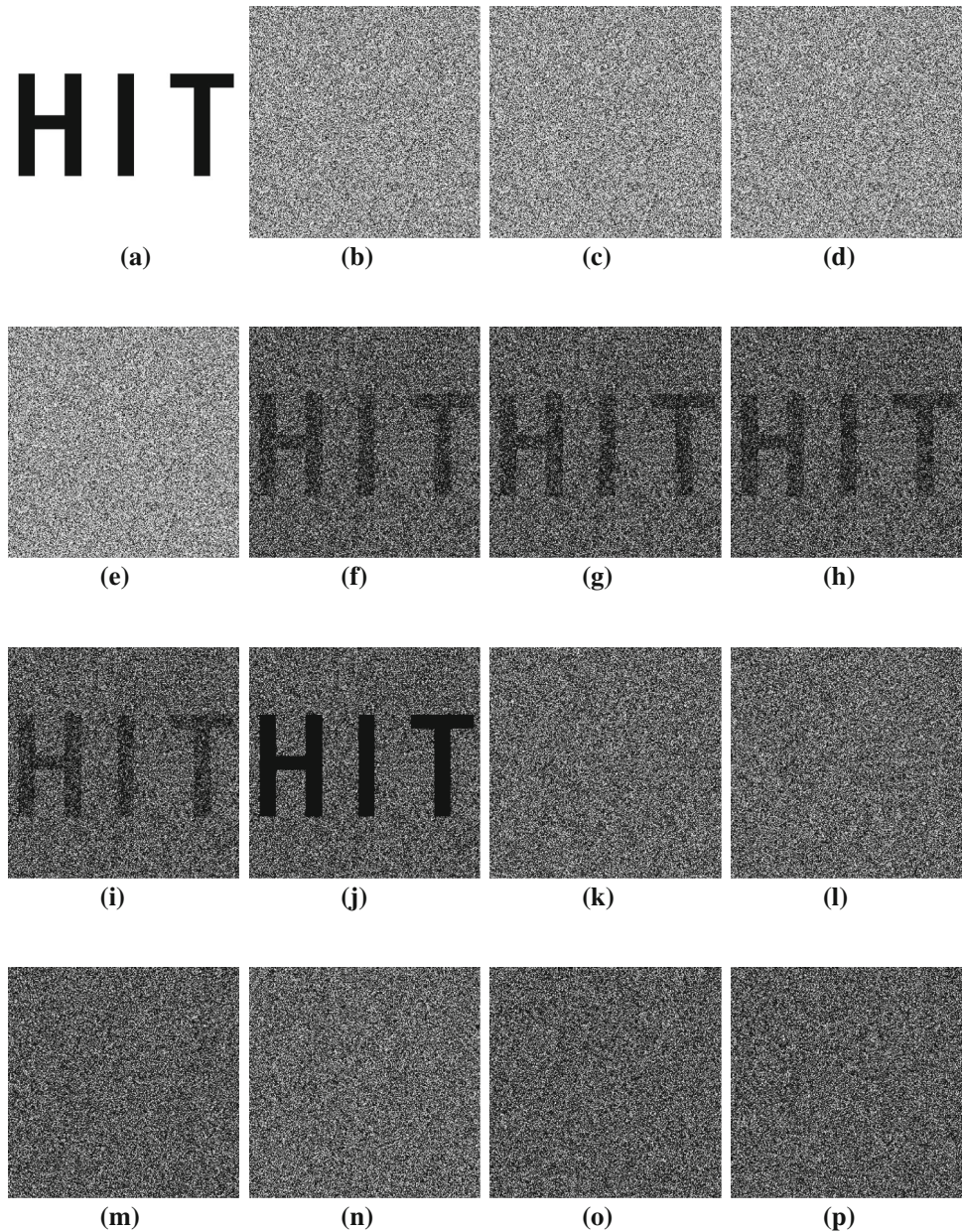
If $sc_k = 0$, then $P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS0] = 0) = P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0)$ sets up.

If $sc_k = 1$, then sc_k is equal to one of $sc_1, sc_2, \dots, sc_{k-1}$. If not, every one of $sc_1, sc_2, \dots, sc_{k-1}$ is complementary to $sc_k \Rightarrow$

$sc_1 = sc_2 = \dots = sc_{k-1} = 0 \Rightarrow s = 0 \oplus 0 \dots \oplus 0 \oplus 1 = 1$ with contradiction to $s = 0$.

Hence sc_k is equal to one of $sc_1, sc_2, \dots, sc_{k-1}$, then $P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS0] = 0) = P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0)$ also sets up.

Fig. 3 Experimental example of the proposed (3, 4) scheme. **a** Secret image I. **b** Shadow image SC_1 . **c** Shadow image SC_2 . **d** Shadow image SC_3 . **e** Shadow image SC_4 . **f** Recovered image $SC_1 \otimes SC_2 \otimes SC_3$. **g** Recovered image $SC_1 \otimes SC_2 \otimes SC_4$. **h** Recovered image $SC_1 \otimes SC_3 \otimes SC_4$. **i** Recovered image $SC_2 \otimes SC_3 \otimes SC_4$. **j** Recovered image $t = 4$. **k** Recovered image $SC_1 \otimes SC_2$. **l** Recovered image $SC_1 \otimes SC_3$. **m** Recovered image $SC_1 \otimes SC_4$. **n** Recovered image $SC_2 \otimes SC_3$. **o** Recovered image $SC_2 \otimes SC_4$. **p** Recovered image $SC_3 \otimes SC_4$



Thus, if $s = 0 \Rightarrow P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS0] = 0) = P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0) \Rightarrow$ Eq. (8) sets up.

In a similar way, if $s = 1$ we have

$$P(SC_{1 \otimes 2 \otimes \dots \otimes k-1 \otimes k}[AS1] = 0) = 0 \tag{9}$$

In order to improve the contrast, based on Lemma 2, the probability of collecting b_1, b_2, \dots, b_k should be as large as possible. Hence, step 3 of the proposed scheme is designed to improve the probability.

Theorem 1 *The proposed scheme is secure and visually recognizable, it is a valid (k, n) RG-based VSS.*

Proof First, every single shadow image that according the proposed scheme is secure. There is no cross interference of the secret image in every shadow image, i.e. every single shadow image could reveal nothing of the secret image. Every bit sc_i in sc_1, sc_2, \dots, sc_n should be random, no relationship with or not decided by corresponding secret bit s .

Second, according to Lemma 2,

$$P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS0] = 0) = (1/2)^{k-1}, P(SC_{1 \otimes 2 \otimes \dots \otimes k-1}[AS1] = 0) = (1/2)^{k-1}. \text{ Hence, } P_0 = P_1 \text{ when } t < k. \text{ As a result, the security condition is satisfied.}$$

Fig. 4 Experimental example of the proposed (2, 5) scheme. **a** Secret image2. **b** Shadow image SC_1 . **c** Recovered image $SC_1 \otimes SC_2$. **d** Recovered image $SC_1 \otimes SC_2 \otimes SC_3$. **e** Recovered image $SC_1 \otimes SC_2 \otimes SC_3 \otimes SC_4$. **f** Recovered image $SC_1 \otimes SC_2 \otimes SC_3 \otimes SC_4 \otimes SC_5$

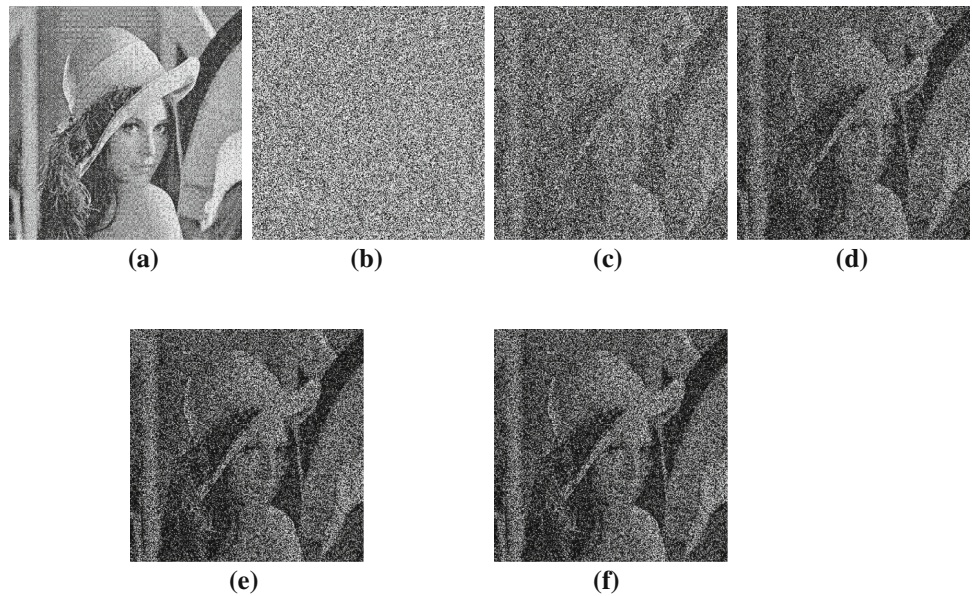


Table 1 Average contrast of the proposed scheme

(k, n)	Average contrast of proposed scheme			
	$t = 2$	$t = 3$	$t = 4$	$t = 5$
(2, 2)	0.50058			
(2, 3)	0.28696	0.49996		
(3, 3)		0.25091		
(2, 4)	0.28571	0.49999	0.49999	
(3, 4)		0.11029	0.24936	
(4, 4)			0.12414	
(2, 5)	0.25104	0.42994	0.50167	0.50167
(3, 5)		0.08736	0.19075	0.25027
(4, 5)			0.04765	0.12571
(5, 5)				0.06353

Moreover, based on Eqs. (8) and (9), $P_0 > P_1$ when $t \geq k$. Thus, the proposed scheme satisfy the contrast condition.

Based on the above discussions, Definitions 2 and 3, the conclusion follows immediately. The proposed scheme is a valid (k, n) RG-based VSS.

We note that, the theoretical contrast of the proposed scheme is not given directly by k, t and n , which is left as an open problem for further studies [5].

5 Experimental results and analyses

In this section, we conduct experiments and analyses to evaluate the effectiveness of the proposed scheme. In the experiments, several secret images are used: original binary secret image1 as shown in Fig. 3a, and original binary

secret image2 as shown in Fig. 4a are used as the binary secret images, with size of 512×512 , to test the efficiency of the proposed scheme.

5.1 Image illustration

In our experiments, (3, 4) (i.e. $k = 3, n = 4$) threshold of scheme with secret image1, (2, 5) threshold of scheme with secret image2 are used to do the test of the proposed scheme.

Figure 3b–e show the 4 shadow images SC_1, SC_2, SC_3 and SC_4 , which are noise like. Figure 3f–j show the recovered secret image with any 3 or 4 shadow images with stacking recovery, from which the secret image recovered from $t = k = 3$ shadow images could be recognized based on stacking. Figure 3k–p show the recovered secret image with any less than k shadow images based on stacking recovery, from which there is no information could be recognized.

The next example, we only give the results by the first t th shadow images for saving pages.

Figure 4b shows one of the 5 shadow images, which is noise like. Figure 4c–f show the recovered binary secret image with any $t (2 \leq t \leq 5)$ (taking the first t shadow images as an example) with stacking recovery, from which better visual of the recovered secret will be gained by stacking more shadow images.

Based on the obtained results we can conclude that:

- The shadow images are noise like, hence the proposed scheme has no cross interference of secret image in single shadow image.
- The progressive visual quality of the recovered secret can be gained for the proposed.

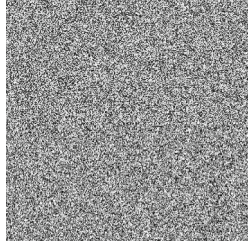
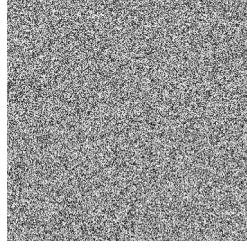
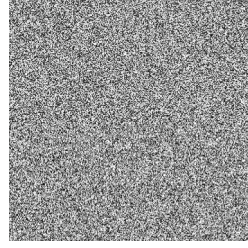
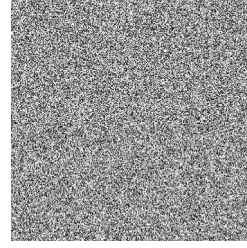
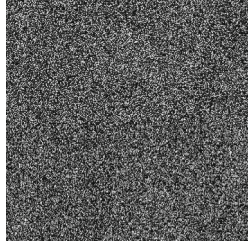
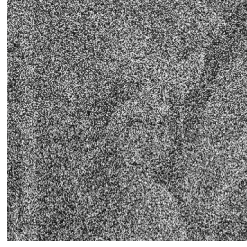
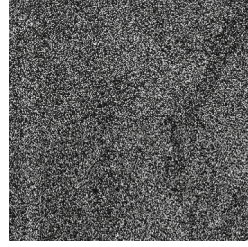
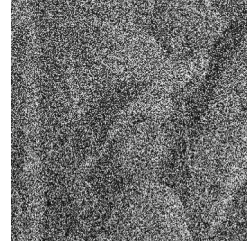
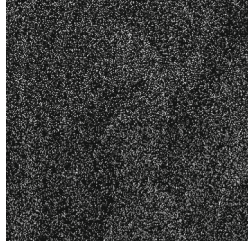







Chen and Tsao's scheme	Wu and Sun's scheme	Guo <i>et al.</i> 's scheme	Proposed scheme
			
(a1) SC_1	(a2) SC_1	(a3) SC_1	(a4) SC_1
			
(b1) $t = 2$	(b2) $t = 2$	(b3) $t = 2$	(b4) $t = 2$
			
(c1) $t = 3$	(c2) $t = 3$	(c3) $t = 3$	(c4) $t = 3$
			
(d1) $t = 4$	(d2) $t = 4$	(d3) $t = 4$	(d4) $t = 4$

Fig. 5 Comparison of (2, 4) threshold between the related schemes

- When $t < k$ shadow images are collected, there is no information of the secret image could be recognized, which shows the security of the proposed scheme.
- When $t (k \leq t \leq n)$ shadow images are recovered by stacking, the secret image could be recognized by HVS.

5.2 Visual quality of the recovered secret images

The visual quality of the recovered secret images is evaluated by contrast in Definition 1. The same original binary

secret image as shown in Fig. 3a is used to do the experiments of contrast.

Average contrast of the proposed (k, n) ($2 \leq k \leq n$) scheme is shown in Table 1. Where t is the number of recovered shadow images.

From Table 1, we can find that, in the proposed scheme, $\alpha > 0$ when $t \geq k$ and contrast increases as t increases for a certain (k, n) with stacking recovery when $2 \leq n \leq 5$. The experimental results of the contrast verify the validity of the performance analysis on the contrast.

5.3 Comparisons with related schemes

Herein, we compare the proposed scheme with other related schemes especially Chen and Tsao’s scheme [1], Wu and Sun’s scheme [19], and Guo et al.’s scheme [5], since both the proposed scheme and [19] and [5] are a continuous and extension work of the schemes [1]. In addition, schemes in [1, 19] and [5] have good features in VSS, such as no codebook design, no pixel expansion and so on.

5.3.1 Image illustration comparison

In this section, (2, 4) threshold with $k \leq t \leq n$ is applied as an example shown in Fig. 5. We can see that Wu and Sun’s scheme [19] and Guo et al.’s scheme [5] both improve the visual quality of Chen and Tsao’s scheme. The proposed scheme has the best visual quality in comparison with the three schemes. Guo *et al.*’s scheme and Chen and Tsao’s scheme are darker, while the darkness of the proposed scheme is acceptable, since $sc_1 \otimes sc_2 \otimes \dots \otimes sc_k \dots \otimes$

$sc_{n-1} \otimes sc_n = sc_1 \otimes sc_2 \otimes \dots \otimes sc_k$ in the proposed scheme.

5.3.2 Contrast comparison

Tables 2 and 3 show contrast comparisons of recovered secret images between the proposed scheme with all $(k, n) (2 \leq n \leq 5, 2 \leq k \leq n, k \leq t \leq n)$ and Chen and Tsao’s scheme [1], Wu and Sun’s scheme [19], and Guo et al.’s scheme [5]. The results indicate the visual quality of proposed scheme is similar as or overall greater than others.

1. If $t = n$ for case (n, n) , the contrast of the proposed scheme is nearly the same as that of the others, since they reduce to the same algorithm.
2. For case $(n - 1, n)$, the contrast of the proposed scheme is similar as that of Wu and Sun’s scheme [19], since

$$\begin{aligned} &sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \otimes sc_n \\ &= sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \otimes sc_k \\ &= sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \end{aligned}$$

Table 2 Contrast of Chen and Tsao’s scheme and Wu and Sun’s scheme

(k, n)	Chen and Tsao’s scheme				Wu and Sun’s scheme			
	$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 2$	$t = 3$	$t = 4$	$t = 5$
(2, 2)	0.498764				0.500775			
(2, 3)	0.141573	0.248554			0.284035	0.499012		
(3, 3)		0.249349				0.249555		
(2, 4)	0.069772	0.118199	0.125201		0.199103	0.332523	0.499348	
(3, 4)		0.057024	0.124764			0.111718	0.250875	
(4, 4)			0.125335				0.124552	
(2, 5)	0.040996	0.068244	0.071745	0.061405	0.153601	0.249553	0.362915	0.498898
(3, 5)		0.021492	0.047373	0.061994		0.062646	0.136758	0.250588
(4, 5)			0.02333	0.061806			0.048006	0.126651
(5, 5)				0.062217				0.063075

Table 3 Contrast of Guo et al.’s scheme and ours

(k, n)	Guo et al.’s scheme				Proposed scheme			
	$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 2$	$t = 3$	$t = 4$	$t = 5$
(2, 2)	0.499947				0.4978			
(2, 3)	0.14449	0.252621			0.28494	0.49927		
(3, 3)		0.250342				0.24965		
(2, 4)	0.142742	0.249916	0.249916		0.28726	0.50181	0.50181	
(3, 4)		0.05811	0.126323			0.11335	0.25314	
(4, 4)			0.124741				0.12451	
(2, 5)	0.084186	0.143391	0.150169	0.124929	0.25015	0.42876	0.50023	0.50023
(3, 5)		0.022415	0.048008	0.062215		0.0854	0.18894	0.24851
(4, 5)			0.023466	0.0616			0.04691	0.12536
(5, 5)				0.062641				0.06285

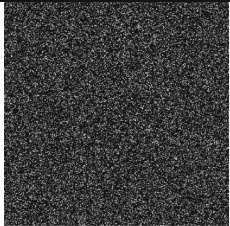
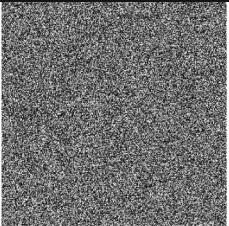
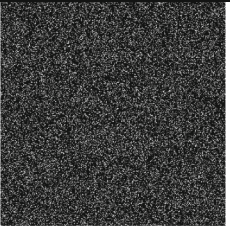
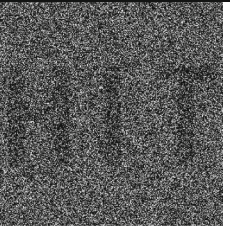
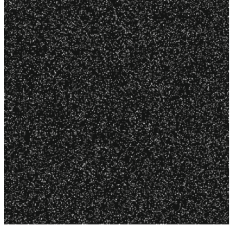
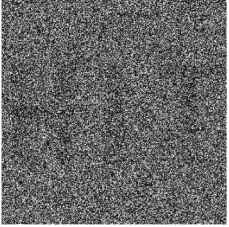
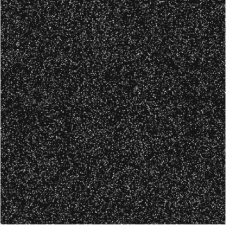
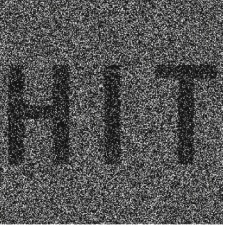
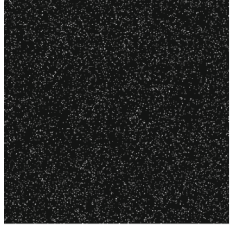
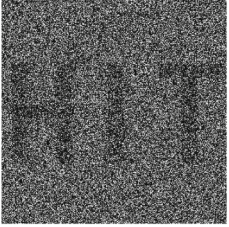
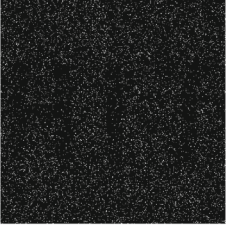

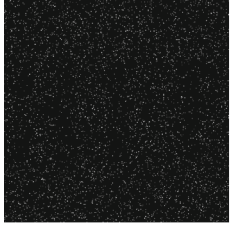
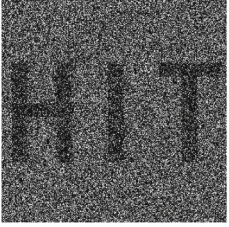
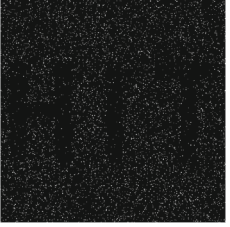
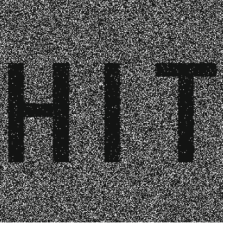
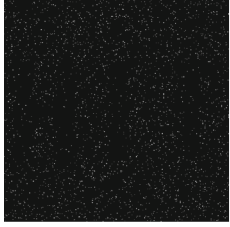
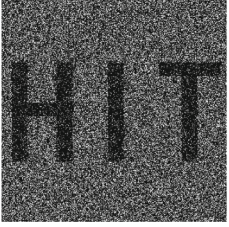

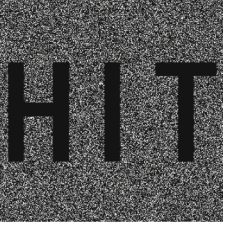

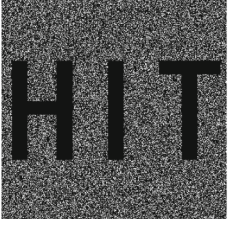


t	Chen and Tsao's scheme	Wu and Sun's scheme	Guo <i>et al.</i> 's scheme	Proposed scheme
3				
4				
5				
6				
7				
8				

Fig. 6 Reconstructed secret image comparison between the related schemes for case (3, 8)

in Wu and Sun’s scheme [19], and in the proposed scheme, we have

$$\begin{aligned} &sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \otimes sc_n \\ &= sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \otimes sc_1 \cdot \\ &= sc_1 \otimes sc_2 \otimes \dots \otimes sc_{k-1} \otimes sc_k \end{aligned}$$

3. The proposed scheme is overall greater than others for the other (k, n) cases when $n - k \geq 2$. Especially for cases (2, 4) and (2, 5), the contrast of the proposed scheme achieves 0.5, since the probability of correctly reconstructing the secret pixels of the proposed scheme is larger than that of the others.
4. The contrast of stacking $t = n - 1$ is the same as that of stacking $t = n$ for cases (2, 4) and (2, 5), since $sc_1 \otimes sc_2 \otimes \dots \otimes sc_k \dots \otimes sc_{n-1} \otimes sc_n = sc_1 \otimes sc_2 \otimes \dots \otimes sc_k$ in the proposed scheme.

Remark The theoretical contrast of the proposed scheme is not given directly by k, t and n , hence the contrast comparisons are given by experiments. In addition, Definition 1 is a statistical result. Thus, the experimental results are close to the theoretical contrast.

The related RG-based VSS [1, 5, 19] is utilizing the random bits to improve the certain probability (the visual quality), under the secure condition. In the proposed scheme, the probability of introducing the contrast is improved as large as possible through step 3 of the proposed scheme.

5.3.3 Further analyses and discussions

The difference between related Algorithms and the proposed scheme lies in step 3 of the proposed scheme. Herein, we discuss why visual quality of the proposed scheme is better than others.

The secret information, i.e., $S(i, j)$, is covered by b_1, b_2, \dots, b_k according to the related Algorithms. Hence, the visual quality of the revealed secret image depends on the probability of picking up b_1, b_2, \dots, b_k bits from the t bits, i.e., a larger probability of collecting b_1, b_2, \dots, b_k will lead to better visual quality of the reconstructed secret image, where t is the number of stacking shares. Thus, detail discussions about the related Algorithms are examined as follows.

1. In Chen and Tsao’s scheme, if the user wants to collect b_1, b_2, \dots, b_k , the user has to pick up exactly b_1, b_2, \dots, b_{k-1} and b_k . So the probability is low.
2. The user can collect b_1, b_2, \dots, b_k and any one of b_k, b_{k+1}, \dots, b_n for obtaining b_1, b_2, \dots, b_k in Wu and Sun’s scheme. Thus, the probability is improved.
3. The user can reveal $S(i, j)$ through collecting any one of $Q_1, Q_2, \dots, Q_{\lfloor \frac{n}{k} \rfloor}$ in Guo et al.’s scheme, where $Q_i (1 \leq i \leq \lfloor \frac{n}{k} \rfloor)$ represents the k pixels generated by the

i -th loop in Guo et al.’s scheme. Hence, the better visual quality is introduced than Chen and Tsao’s scheme. Meanwhile, Q_i will affect Q_j , and the last $n - k \lfloor \frac{n}{k} \rfloor$ bits generated by step 4 don’t cover any secret information, which will restrain the visual quality, where $1 \leq i, j \leq \lfloor \frac{n}{k} \rfloor, i \neq j$.

4. Based on step 3 of the proposed scheme, we can obtain any one of $b_1, b_{k+1}, b_{2k+1}, \dots, b_{\lfloor \frac{n}{k} \rfloor k+1}$, any one of $b_2, b_{k+2}, b_{2k+2}, \dots, b_{\lfloor \frac{n}{k} \rfloor k+2}, \dots$, and any one of $b_k, b_{2k}, b_{3k}, \dots, b_{\lfloor \frac{n}{k} \rfloor k}$ to gain b_1, b_2, \dots, b_k . As a result, the probability is significantly enhanced which will lead to better visual quality.

According to above analyses, the following conclusions are presented.

1. When $k = n$, the related Algorithms are the same.
2. The proposed scheme has the same visual quality as Wu and Sun’s scheme if $n = k + 1$ or $n = t$.
3. The best visual quality is achieved in the proposed scheme when $n - k \geq 2 \wedge t \neq n$.

The above three points are validated in Tables 2 and 3, where few non-conformities are due to randomness. Furthermore, Fig. 6 indicates additional visual quality comparison between the related Algorithms for case (3, 8), where $n - k = 6 > 2$ and corresponding contrast curves are exhibited in Fig. 7. By all appearances, the proposed scheme outperforms the other three methods.

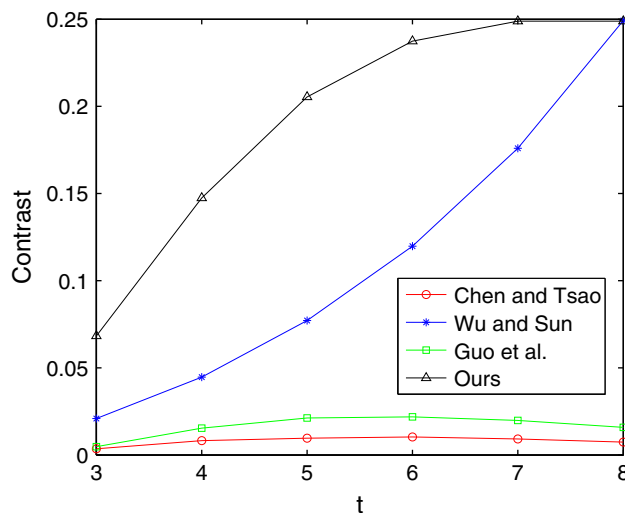


Fig. 7 Contrast curves of the related schemes for case (3, 8)

6 Conclusion

This paper proposed a new RG-based VSS with improved visual quality by specially utilizing the random bits, which outperformed relative schemes, i.e. Chen and Tsao's scheme, Wu and Sun's scheme and Guo et al.'s scheme. The probability of reconstructing the secret pixels is improved as large as possible. The crucial successful points in the proposed scheme lie in: (1) (k, n) threshold, (2) requiring no codebook design, (3) avoiding the pixel expansion problem, (4) larger visual quality than the previous related schemes. However, the contrast of the proposed scheme is not given directly by k , t and n , which is left as an open problem for further studies.

Acknowledgments The authors would like to thank the anonymous reviewers for their valuable discussions and comments. The authors would like to thank to Dr. Feng Liu and Prof. Mohamed Amin for their valuable discussions. This work is supported by the National Natural Science Foundation of China (Grant Numbers: 61100187, 61301099, 61361166006).

References

- Chen, T.H., Tsao, K.H.: Threshold visual secret sharing by random grids. *J. Syst. Softw.* **84**(7), 1197–1208 (2011)
- Cimato, S., De Prisco, R., De Santis, A.: Probabilistic visual cryptography schemes. *Comput. J.* **49**(1), 97–107 (2006)
- De Prisco, R., De Santis, A.: On the relation of random grid and deterministic visual cryptography. *IEEE Trans. Inform. Forensics Secur.* **9**(3–4), 653–665 (2014)
- Fu, Z.X., Yu, B.: Visual cryptography and random grids schemes. In: *Digital-Forensics and Watermarking*, pp. 109–122. Springer, Auckland (2014)
- Guo, T., Liu, F., Wu, C.: Threshold visual secret sharing by random grids with improved contrast. *J. Syst. Softw.* **86**(8), 2094–2109 (2013)
- Guo, T., Liu, F., Wu, C.: k out of k extended visual cryptography scheme by random grids. *Signal Process.* **94**, 90–101 (2014)
- Hou, Y.C.: Visual cryptography for color images. *Pattern Recognit.* **36**(7), 1619–1629 (2003)
- Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. *Opt. Lett.* **12**(6), 377–379 (1987)
- Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **82**(10), 2172–2177 (1999)
- Lee, Y.S., Wang, B.J., Chen, T.H.: Quality-improved threshold visual secret sharing scheme by random grids. *Image Process. IET* **7**(2), 137–143 (2013)
- Li, P., Ma, P.J., Su, X.H., Yang, C.N.: Improvements of a two-in-one image secret sharing scheme based on gray mixing model. *J. Vis. Commun. Image Rep.* **23**(3), 441–453 (2012)
- Liu, F., Wu, C., Qian, L., et al.: Improving the visual quality of size invariant visual cryptography scheme. *J. Vis. Commun. Image Rep.* **23**(2), 331–342 (2012)
- Naor, M., Shamir, A.: Visual cryptography. *Advances in Cryptology EUROCRYPT'94 Lecture Notes in Computer Science. Workshop on the Theory and Application of Cryptographic Techniques*, May 9C12, pp. 1–12. Springer, Perugia (1995)
- Shyu, S.J.: Image encryption by random grids. *Pattern Recognit.* **40**(3), 1014–1031 (2007)
- Shyu, S.J.: Image encryption by multiple random grids. *Pattern Recognit.* **42**, 1582–1596 (2009)
- Wang, D., Zhang, L., Ma, N., Li, X.: Two secret sharing schemes based on boolean operations. *Pattern Recognit.* **40**(10), 2776–2785 (2007)
- Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error diffusion. *IEEE Trans. Inf. Forensics Secur.* **4**(3), 383–396 (2009)
- Weir, J., Yan, W.: A comprehensive study of visual cryptography. In: *Transactions on DHMS V. LNCS 6010*, pp. 70–105. Springer, Berlin (2010)
- Wu, X., Sun, W.: Improving the visual quality of random grid-based visual secret sharing. *Signal Process.* **93**(5), 977–995 (2013)
- Wu, X., Sun, W.: Improved tagged visual cryptography by random grids. *Signal Process.* **97**, 64–82 (2014)
- Yan, X., Wang, S., El-Latif, A.A.A., Niu, X.: Visual secret sharing based on random grids with abilities of and and xor lossless recovery. *Multimed. Tools Appl.* **74**(9), 3231–3252 (2015)
- Yan, X., Wang, S., El-Latif, A.A.A., Niu, X.: Random grids-based visual secret sharing with improved visual quality via error diffusion. *Multimed. Tools Appl.* **74**(21), 9279–9296 (2015)
- Yan, X., Wang, S., Niu, X.: Threshold construction from specific cases in visual cryptography without the pixel expansion. *Signal Process.* **105**, 389–398 (2014)
- Yang, C.N.: New visual secret sharing schemes using probabilistic method. *Pattern Recognit. Lett.* **25**(4), 481–494 (2004)
- Yang, C.N., Wu, C.C., Wang, D.S.: A discussion on the relationship between probabilistic visual cryptography and random grid. *Inform. Sci.* **278**, 141–173 (2014)

Xuehu Yan was born in China, in Feb 1984, received the B.Sc. degree with honor rank in Science in Information and Calculate Science from Harbin Institute of Technology, China in 2006, and M.Sc. degree in Computational Mathematics in 2008. He was an assistant engineer in CHINA AERO-POLYTECHNOLOGY ESTABLISHMENT from Aug 2008 to Oct 2010. He now is a doctoral degree student at Harbin Institute of Technology (H.I.T), Harbin, P. R. China. His areas of interests are cryptography, multimedia security, secret image sharing and information hiding.

Xin Liu was born in China, in Sep 1984, received the B.Sc. degree in Materials Chemistry from Harbin University of Science and Technology, China in 2006, and M.Sc. degree in Computer Application in 2009. He was an assistant researcher in Harbin University of Science and Technology from Apr 2009 to now. And he now is a doctoral degree student at Harbin Institute of Technology (H.I.T), Harbin, P. R. China. His areas of interests are information security, multimedia security and secret image sharing.

Ching-Nung Yang received the B.S. degree and the M.S. degree, both from Department of Telecommunication Engineering at National Chiao Tung University. He received Ph.D. degree in Electrical Engineering from National Cheng Kung University. He is presently a professor in the Department of Computer Science and Information Engineering at National Dong Hwa University, and is also an IEEE senior member. He has published a number of journal and conference papers in the areas of information security, multimedia security and coding theory. He is the guest editor of a special issue on “Visual Cryptography Scheme” for Communication of CCISA, and a coauthor of a series of articles on “Image Secret Sharing” for the

Encyclopedia of Multimedia. He is the coeditor of two books “Visual Cryptography and Secret Image Sharing” published by CRC Press/Taylor & Francis, and “Steganography and Watermarking” published by Nova Science Publishers, Inc. He serves as a technical reviewer for over 30 major scientific journals in the areas of his expertise, and

serves as editorial boards of some journals. Also, has served member of program committees of various international conferences committees. He is the recipient of the 2000, 2006, 2010 and 2012 Fine Advising Award in the Thesis of Master of Science awarded by Institute of Information & Computer Machinery.