

# Threshold progressive visual cryptography construction with unexpanded shares

Xuehu Yan<sup>1,2</sup> · Shen Wang<sup>2</sup> · Xiamu Niu<sup>2</sup>

Received: 10 May 2014 / Revised: 24 February 2015 / Accepted: 25 June 2015 /

Published online: 2 August 2015

© Springer Science+Business Media New York 2015

**Abstract** Differently from traditional secret sharing, progressive secret sharing can gain clearer recovered secret image with more shares. However, previous progressive visual secret sharing (PVSS) schemes with unexpanded shares are only for case  $(2, n)$  other than general threshold (case), which will restrict the application range. In this paper, a general threshold PVSS construction method from case  $(2, n)$  with unexpanded shares is proposed. It has the feature of  $(k, n)$  threshold with no pixel expansion, which could be loss-tolerant and control access for a wider application. Based on the proposed construction method, a new threshold PVSS scheme is constructed. Compared with relative approaches, the proposed scheme has improved performances.

**Keywords** Visual secret sharing · Progressive visual cryptography · Progressive visual secret sharing · Threshold · Pixel expansion · Quality-adaptive

## 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 is an application layer technology to protect the sensitive information from the malicious behavior while in transit. Secret image sharing protects digital images through sharing the user data into different secret shares (also called shadows) and distributing them into multiple participants. Secret image sharing has attracted more attention from scientists and engineers. Visual secret sharing (VSS) also called visual cryptographic scheme (VCS) [1–5], is one branch in secret image sharing.

---

✉ Xuehu Yan  
xuehu.yan@ict.hit.edu.cn

✉ Shen Wang  
768588166@qq.com

Xiamu Niu  
xiamu.niu@ict.hit.edu.cn

<sup>1</sup> Electronic Engineering Institute, 230000 Hefei, China

<sup>2</sup> School of Computer Science and Technology, Harbin Institute of Technology, 150001 Harbin, China

Naor and Shamir [4] first proposed the threshold-based VCS. In their scheme, a binary secret image is shared by generating corresponding  $n$  noise-like shadow images (shares). Any  $k$  or more noise-like shadow images are superposed to recover the secret image visually based on human visual system (HVS) and probability. While less than  $k$  participants cannot reveal any information of the secret image by inspecting their shares. The main properties of the VCS by [4] are that the decryption of secret image is completely based on HVS without any cryptographic computation, and alternative order of the shadow images.

Indeed, traditional VSS, has the property of “All-or-Nothing”, i.e., the secret information could be revealed only when  $k$  or more shares are stacked together, and nothing if less than  $k$  shares are obtained. In many applications like pay-per-view videos, Pay-TV/Music and art-work image vending, video on demand (VoD), the following feature namely “progressive” is very useful. This feature requires that the quality of visual secret data is partially degraded after the sharing phase. First, such feature makes it possible for potential users to view low-quality copies of the media data before buying them. Second, the owner of the secret image can show different image quality of the secret by a different number of superposed shadow images, depending on the importance of the charge case or character. While “progressive VSS” can improve the clarity of a secret image progressively by stacking more and more shares.

Progressive visual secret sharing (PVSS), based on the ideas of VCS [6–9], has better perceptual quality for the recovered secret images when more shadows are available. PVSS can be used in the applications in different visual quality or with different importance. Here in this paper we will give two examples.

In the process of displaying and selling works of art., because the details are very important for the works of art, details need to be protected. After sharing artwork once, without computational devices the owner can decode and show different visual quality to different people in different occasions, instead of repeating sharing. For example, in the exhibition, first he can demonstrate the general visual quality to prove the owner of the art, then for the moment to reach a purchase agreement he can show high visual quality by stacking more shares.

In a city’s planning and design, the team design manager needs to have the highest authority. He can view the highest resolution map. He further distributes different privileges (clarity or visual quality) to team members. For example, a certain member who designs the streets, he would not need to see the details of the map, so the manager can distribute him a low visual quality. This provides the ability to distribute a different resolution (that is, different number of the shadow images) corresponding to different member by sharing the map only one time.

Previous PVSS overall suffers from the drawbacks such as pixel expansion, and poor visual quality of the recovered secret image [10]. In order to solve the pixel expansion problem, Hou and Quan [11] proposed a  $(2, n)$  PVSS with unexpanded shares by designing two basic sharing matrices. In Hou and Quan’s scheme, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is close to  $1/n$ . And more shares are stacking (Boolean OR operation) clearer and clearer secret will be gained. Recently, Chen et al. [12] proposed a quality-adaptive  $(2, n)$  random grids (RG)-based VSS for improving the visual quality of reconstructed images. Unfortunately, Hou and Quan’s scheme and Chen et al.’s scheme fail to support  $(k, n)$  threshold, which will restrict the application range.

In this paper, a general  $(k, n)$  threshold PVSS construction method from case  $(2, n)$  is proposed, which improves traditional  $(2, n)$  PVSS with unexpanded shares to be  $(k, n)$  threshold PVSS. By the construction method, as an example, a new threshold PVSS scheme is constructed based on applying Hou and Quan's  $(2, n)$  PVSS. Although our construction method is described by Hou and Quan's  $(2, n)$  PVSS, the proposed threshold construction method is a general method. Chen et al.'s scheme is also tested to evaluate the efficiency of the proposed construction method. The secret could be recovered by HVS with no cryptographic computation. Experimental results and security analysis show the effectiveness of the proposed scheme in terms of security and overall performances. Comparisons with previous approaches show the improved performances of the proposed scheme.

The rest of the paper is organized as follows. Section 2 introduces the preliminary techniques as the basis for the proposed scheme. The proposed scheme is introduced in Section 3. Section 4 gives the performance analyses of the proposed scheme. Section 5 is devoted to experimental results. Finally, Section 6 concludes this paper.

## 2 Review of the related work

In this section, we review Hou and Quan's scheme [11] as the basis for the proposed scheme. In what follows, symbol  $\otimes$  denotes the Boolean OR operation.  $\bar{x}$  is a bit-wise complementary operation of a pixel  $x$ . The binary secret image  $S$  with size of  $M \times N$  is shared among  $n$  shadow images, while the recovered secret image  $S'$  is recovered from  $t$  ( $2 \leq t \leq n$ ,  $t \in \mathbb{Z}^+$ ) shadow images.

Hou and Quan [11] designed two  $n \times n$  matrices denoted by  $C^0$  and  $C^1$  (the codebook is shown in Table 1), which represent the sharing basic matrix for white and black pixels of the secret image, respectively. Here, 0 is for white and 1 is for black.

The shadow images generation procedure is stated as follows:

- (1) One basic matrix is selected according to the color of secret image current processing pixel.
- (2) Randomly select  $L$  from  $1, 2, \dots, n$ .
- (3) Attribute the  $L$ th row of the current basic matrix to the corresponding  $n$  pixels of the  $n$  shadow images.

From Table 1, any column in  $C^0$  or  $C^1$  only has single "1" that means the probability for the corresponding  $n$  pixels of the  $n$  shadow images to appear 1 is the same as to  $1/n$ , regardless the color of the current pixel of the secret image is white or black, hence, every shadow image gives no clue to the secret. Furthermore, there is no pixel expansion for the shadow images.

The recovery method is based on stacking (Boolean OR operation) 2 or more shadow images, hence the scheme is a  $(2, n)$  threshold scheme. When recovering a black secret pixel, after stacking more shadow images the chance of being black for black area of the secret image will be increased. While a white pixel will remain as  $1/n$ , hence the secret will be progressively revealed. However, Hou and Quan's scheme [11] fails to support  $(k, n)$  threshold.

A general threshold PVSS construction method from case  $(2, n)$  with unexpanded shares will be proposed. Based on the proposed construction method, a new threshold PVSS scheme is constructed, which will achieve the feature of  $(k, n)$  threshold by extending and repeatedly applying Hou and Quan's  $(2, n)$  PVSS.

### 3 The proposed scheme

In this section, a general  $(k, n)$  threshold PVSS construction method from case  $(2, n)$  is described in detail, which improves traditional  $(2, n)$  PVSS to be  $(k, n)$  threshold PVSS. Although our construction method is described by Hou and Quan’s  $(2, n)$  PVSS, the proposed threshold construction method is a general method.

#### 3.1 Threshold progressive visual cryptography with unexpanded shares

Aiming to improve Hou and Quan’s scheme, i.e., to support  $(k, n)$  threshold, the proposed  $(k, n)$  scheme will apply repeatedly Hou and Quan’s  $(2, n)$  sharing scheme, hence the algorithmic steps of the  $(2, n)$  scheme are described in Algorithm 1. First, the two basic matrices are generated according to Table 1. Second, for every position  $(i, j)$  of  $S$ , select  $L$  from  $1, 2, \dots, n$  randomly and choose the current basic matrix depending on  $S(i, j)$ . Finally, attribute the  $L$ th row of the chosen basic matrix to the corresponding  $n$  pixels of the  $n$  shadow images.

**Algorithm 1.** The  $(2, n)$  PVSS.

**Input:** A  $M \times N$  binary secret image  $S$ , the threshold parameters  $n$

**Output:**  $n$  shadow images  $SC_1, SC_2, \dots, SC_n$ .

**Step 1:** Generate two basic matrices  $C^0$  and  $C^1$ .





















**Step 2:** For each position  $(i, j) \in \{(i, j) \mid 1 \leq i \leq M, 1 \leq j \leq N\}$ , repeat Steps 3–4.

**Step 3:** Select  $L \in \{1, 2, \dots, n\}$  randomly.

**Step 4:** If  $S(i, j) = 0$ ,  $SC_m(i, j) = C^0(L, m)$ . Else  $SC_m(i, j) = C^1(L, m)$ ,  $m = 1, 2, \dots, n$ .

**Step 5:** Output the  $n$  shadow images  $SC_1, SC_2, \dots, SC_n$ .

**Table 1** Two  $n \times n$  secret sharing basic matrices of Hou and Quan’s scheme [11]

Secret pixel	Basic matrices	Matrix collections				Probability	Shadow images				Recovery method	
		1	2	...	$n$		1	2	...	$n$		
 (0)	$C^0 = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}_{n \times n}$	1	1	...	1	$1/n$			...		Stacking (OR)	
		0	0	...	0	$1/n$			...			
		⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		⋮
		0	0	...	0	$1/n$			...			
 (1)	$C^1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}_{n \times n}$	1	0	...	0	$1/n$			...			
		0	1	...	0	$1/n$			...			
		⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮		
		0	0	...	1	$1/n$			...			

In order to improve Hou and Quan's scheme to be a general  $k$  out of  $n$  mechanism, the shadow images generation architecture of the proposed scheme is illustrated in Fig. 1.

In Fig. 1 of the proposed scheme, if  $k=2$ , the above  $(2, n)$  PVSS will be applied to generate the shadow images.

If  $k > 2$ , for each  $S(i, j)$ ,  $1 \leq i \leq M$ ,  $1 \leq j \leq N$ , repeat the same operations as follows. Using  $S(i, j)$  to get  $b_{0,1}$  and  $b_{0,2}$  through  $(2, 2)$  PVSS. Divide the  $(k, n)$  threshold mechanism into  $(\lfloor \frac{k}{2} \rfloor, \lfloor \frac{n}{2} \rfloor)$ ,  $(\lceil \frac{k}{2} \rceil, \lceil \frac{n}{2} \rceil)$  mechanisms by dichotomy repeatedly. As a result,  $(k, n)$  threshold mechanism can be represented by  $(2, n_x)$  PVSS and  $(3, n_y)$  PVSS. Furthermore,  $(3, n_y)$  PVSS also can be represented by  $(2, n_x)$  PVSS through dividing the  $(3, n_y)$  threshold into two bits, where one bit is held, another bit is generated into  $n_y-1$  bits through  $(2, n_y-1)$  PVSS. Figure 2 shows an example to represent  $(3, n_y)$  PVSS by  $(2, n_x)$  PVSS. Finally, aiming to make all the shares be equal to each other, the order of the generated  $n$  temporary bits  $b_1, b_2, \dots, b_{n-1}, b_n$  is rearranged and the rearranged  $n$  pixels are assigned to  $SC_1(i, j), SC_2(i, j), \dots, SC_n(i, j)$ . Based on the recursion method,  $(k, n)$  threshold mechanism is represented by  $(2, n_x)$  PVSS recursively.

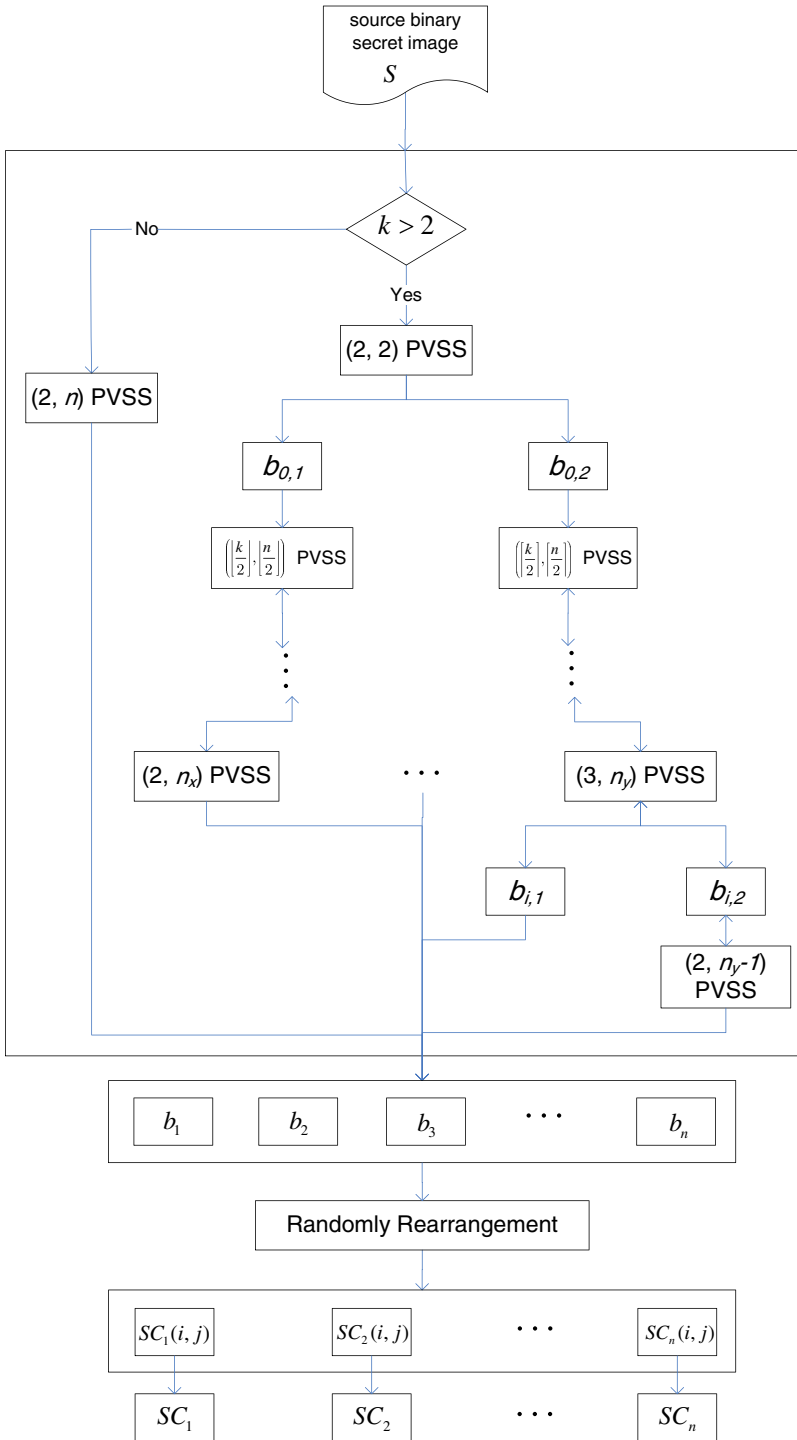
Here, we take  $(4, 5)$  threshold as an example shown in Fig. 3 to show the steps of the proposed  $(k, n)$  threshold scheme. 1) Using  $S(i, j)$  to get  $b_{0,1}$  and  $b_{0,2}$  through  $(2, 2)$  PVSS. 2) Dividing the  $(4, 5)$  threshold mechanism into  $(2, 2), (2, 3)$  mechanisms by dichotomy. 3) Then using  $b_{0,1}$  to get  $b_1$  and  $b_2$  through  $(2, 2)$  PVSS, using  $b_{0,2}$  to get  $b_3, b_4$  and  $b_5$  through  $(2, 3)$  PVSS. 4) The generated 5 temporary bits  $b_1, b_2, b_3, b_4, b_5$  are randomly rearranged to corresponding  $n$  shadow images bits  $SC_1(i, j), SC_2(i, j), \dots, SC_5(i, j)$ . Here, we call  $b_1$  and  $b_2$  are the down generation bits of  $b_{0,1}$ , while  $b_{0,1}$  is the up generation bit of  $b_1$  and  $b_2$ .

We take the above  $(4, 5)$  threshold to give a short explanation to show why the proposed scheme is secure. First, if one wants to recover  $S(i, j)$ , one should collect both  $b_{0,1}$  and  $b_{0,2}$  since  $b_{0,1}$  and  $b_{0,2}$  are generated from  $S(i, j)$  by  $(2, 2)$  PVSS. Second, if one wants to collect  $b_{0,1}$ , one should collect both  $b_1$  and  $b_2$  since  $b_1$  and  $b_2$  are generated from  $b_{0,1}$  through  $(2, 2)$  PVSS. If one wants to collect  $b_{0,2}$ , one should collect at least two of  $b_3, b_4$  and  $b_5$  since  $b_3, b_4$  and  $b_5$  are generated from  $b_{0,2}$  through  $(2, 3)$  PVSS. Finally, one should collect  $b_1, b_2$  and at least two of  $b_3, b_4$  and  $b_5$ . Above all, if one wants to recover  $S(i, j)$ , one should collect  $b_1, b_2$  and at least two of  $b_3, b_4$  and  $b_5$ , i.e., at least 4 of the 5 bits corresponding to the 5 shadow images. In addition, more than 4 bits will increase the probability of collecting the 4 bits, thus a larger contrast will be obtained. Hence, the example of the proposed scheme is  $(4, 5)$  threshold, secure and progressive.

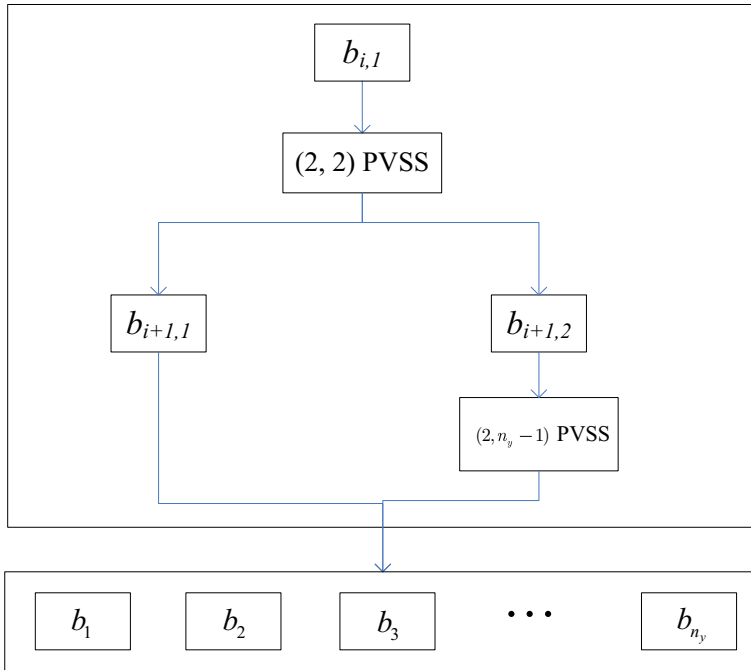
Herein, we adopt  $(2, 2)$  PVSS and dichotomy it into two parts in order to improve the visual quality. In addition, the up-rounding or the down-rounding is adopted for  $k$  and  $n$  to make all the results be integers. So, the threshold  $k$  could be decomposed into the addition of 2 and 3. As a result, the  $(k, n)$  threshold mechanism can be combined by  $(2, n_x)$  PVSS and  $(3, n_y)$  PVSS. In addition,  $(3, n_y)$  PVSS also can be represented by  $(2, n_x)$  PVSS stated above.

Based on the above discussions, we can see that the proposed scheme maintains good security as Hou and Quan's scheme, progressive VSS and no pixel expansion. Besides, it is a general  $k$  out of  $n$  mechanism, which outperforms Hou and Quan's scheme. The security proof will be shown in Section 4.

From the above analysis, the proposed threshold construction method can also be applied for threshold construction from other  $(2, n)$  PVSS as well, i.e., the proposed



**Fig. 1** Shadow images generation architecture of the proposed threshold PVSS with unexpanded shares



**Fig. 2**  $(3, n_y)$  PVSS is represented by  $(2, n_x)$  PVSS

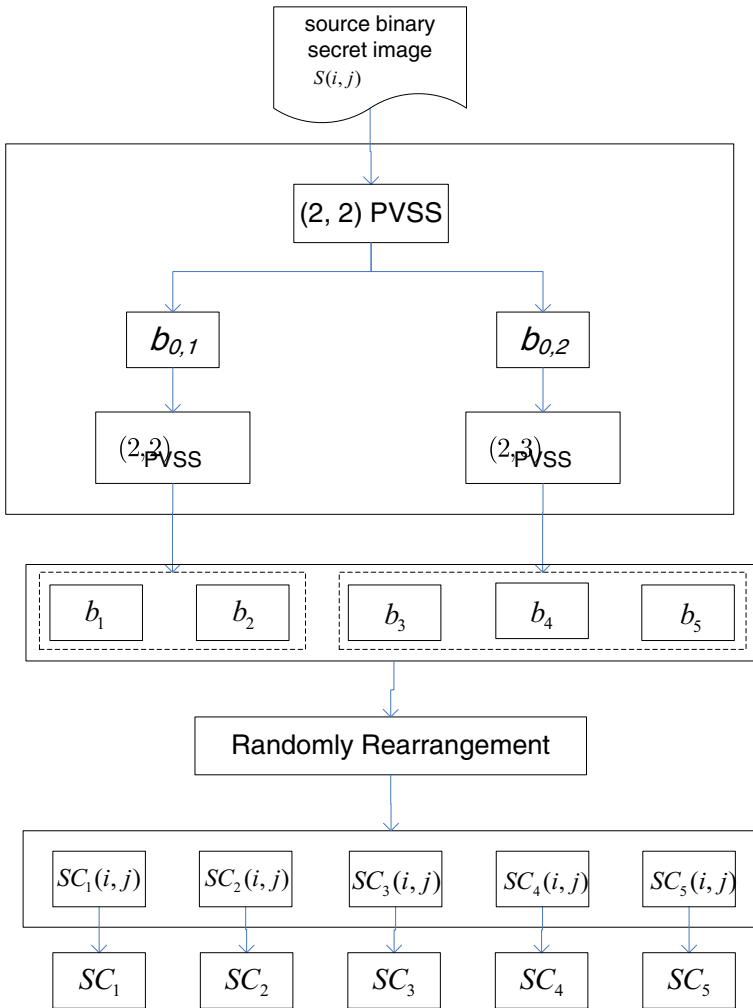
threshold construction method is a general method. More examples will be given in Section 5, which shows that Chen et al.’s scheme can also be extended by the proposed construction method.

### 3.2 Extension for grayscale/color images

The proposed scheme can be extended to share grayscale/color images [13–16]. To share a grayscale image, halftone technologies such as error diffusion [3] 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, such as CMY (cyan–magenta–yellow) model, which is subtractive color model, and displays a color by reflecting light from a surface of an object. The process to share a color secret image includes four steps as follows:

- Step 1 The color secret image (CS) is decomposed by the color model to three color components, i.e.,  $CS_c, CS_m$  and  $CS_y$ .
- Step 2  $CS_c, CS_m$  and  $CS_y$  are converted into a binary image ( $HCS_c, HCS_m$  and  $HCS_y$ ) by applying the error diffusion technology.
- Step 3  $HCS_c, HCS_m$  and  $HCS_y$  are shared by the proposed scheme, to generate  $3n$  shadow images ( $HCS_c C_i, HCS_m C_i, HCS_y C_i, i=1, 2, \dots, n$ ).



**Fig. 3** Shadow images generation architecture of the proposed (4, 5) PVSS

Step 4 The shadow images ( $HCSC_i, HCSmC_i, HCSyC_i, i=1, 2, \dots, n$ ) are composed by the color model to form eight-color shadow images  $HCSC_i, i=1, 2, \dots, n$ .

**In the recovery phase**, for input  $t$  shadow images  $HCSC_{j_1}, HCSC_{j_2}, \dots, HCSC_{j_t}$ ,  $CS' = HCSC_{j_1} \otimes HCSC_{j_2} \otimes \dots \otimes HCSC_{j_t}$ .

### 4 Performance analyses

This section introduces the performances of the proposed scheme by theoretically analyzing the security and the visual quality.



**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 [17, 13, 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  $\alpha$  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)** [4, 13, 14] 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)** [4, 13, 14] The scheme is secure if  $\alpha = 0$  when  $t < k$ , which means no information of  $S$  could be recognized through  $S'$

We note that, definition 1 on the contrast partially borrowed from [17, 14], has been widely accepted and used in some reported VSS schemes [18, 17, 13].

Other definition on contrast used in traditional VSS [11] and probabilistic VSS [19] is given by

$$\alpha = \frac{P_0 - P_1}{m}$$

Where  $m$  is referred to the pixel expansion. It merely evaluates the absolute difference rate between secret and background.

However, From HVS, when the same difference is achieved, better image quality is obtained when  $P_1$  becomes smaller [14]. Hence, Definition 1 is adopted in this paper for evaluating the contrast.

For conventional VSS, whether the secret image can be revealed or not, as well as the security, can be determined by the contrast. Such definitions are the same as Definitions 2 and 3, since the contrast is bigger than zero or equal to zero if and only if the difference is bigger than zero or equal to zero.

Although our  $(2, n)$  PVSS is exactly the same as Hou and Quan's scheme, since different definitions are adopted, Theorem 1 is presented.

**Theorem 1** The proposed scheme is secure and visually recognizable. The contrast of the recovered secret image recovered by any  $t(2 \leq t \leq n)$  shadow images, which are generated by  $(2, n)$  PVSS, is computed as follows:

$$\alpha = \frac{t-1}{2n-t} \quad (2)$$

**Proof** In the proposed  $(2, n)$  PVSS, when  $t(2 \leq t \leq n)$  shadow images are stacking, the probability for the white part of the secret image to appear as black remains  $1/n$ , while for

the black part, the probability increases to  $t/n$ . Based on Definition 1, we have:

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{\frac{n-1}{n} - \frac{n-t}{n}}{1 + \frac{n-t}{n}} = \frac{t-1}{2n-t}$$

Next we prove the proposed scheme is secure, visually recognizable and progressive.

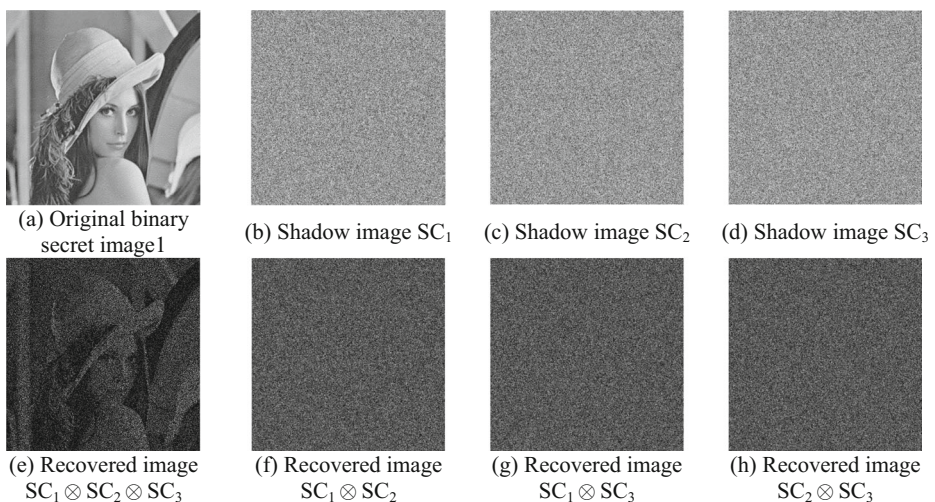
From Algorithm 1, the proposed  $(2, n)$  PVSS is the same as Hou and Quan's  $(2, n)$  scheme. Hence, the proposed  $(2, n)$  PVSS is secure, which means a single could reveal nothing about the secret, and visually recognizable when  $t(2 \leq t \leq n)$  shadow images are stacking, based on Definitions 2 and 3.

For a general  $k$  out of  $n$  mechanism, similarly as the explanation of the above  $(4, 5)$  threshold, we prove that in another way. Based on the dichotomy and decomposition method, in the last generated  $n$  bits, when  $k$  bits are collected, there will exist at least one or some combinations which could recover the up generation bits since  $(k, n)$  threshold mechanism can be recursively represented by  $(2, n_x)$  PVSS. While if less than  $k$  bits are collected, there is not any combination which could recover the up generation bits. In addition, if more than  $k$  bits are collected, the probability of the combinations which could recover the up generation bits and the visual quality of the recovered up generation bits will increase. Hence, based on the discussion and properties of  $(2, n)$  PVSS, the proposed scheme is secure, visually recognizable and progressive.

We note that, the theoretical contrast of the proposed scheme is not given directly by  $k, t$  and  $n$  for case  $(k, n)$ , which is left as an open problem for further studies [20].

## 5 Experimental results and analysis

In this section, several experiments and analysis are performed to evaluate the effectiveness of the proposed scheme. In the experiments, several secret images are used: original binary secret image1 as shown in Fig. 4a, original binary secret image2 as shown in Fig. 5a, and original color secret image3 as shown in Fig. 6a are used as the binary secret images to test the efficiency of the proposed scheme. All the secret images have size of  $1024 \times 1024$ .



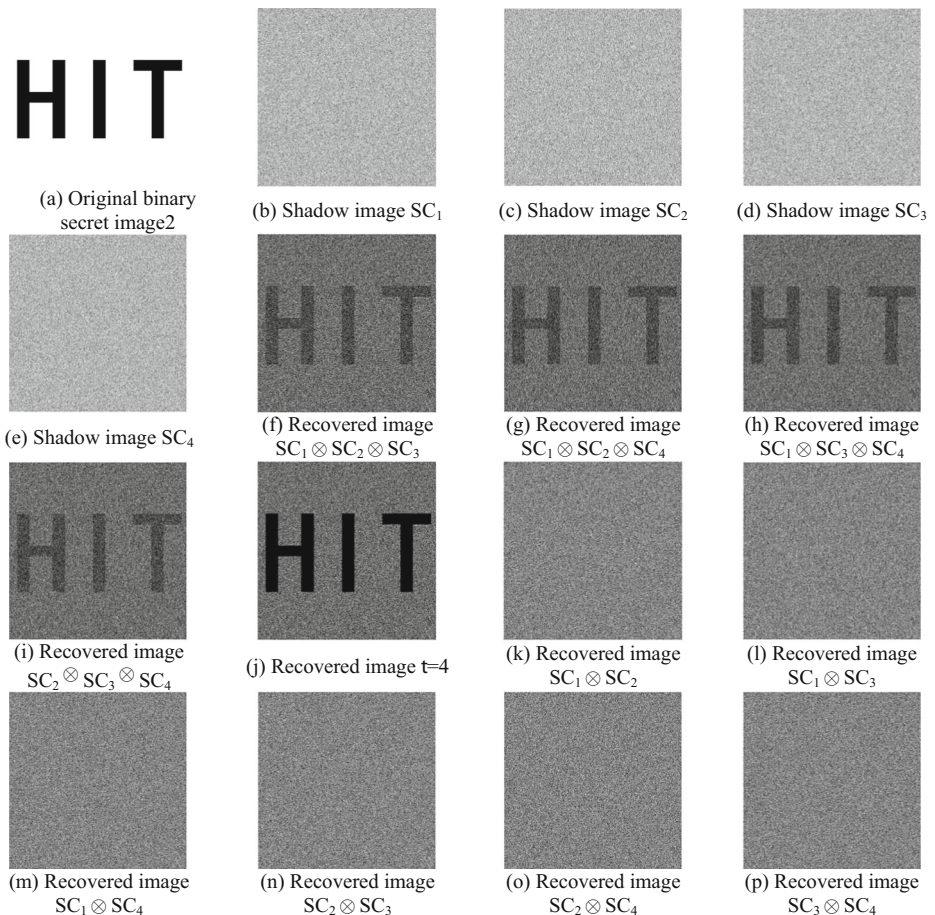
**Fig. 4** Experimental example of the proposed  $(3, 3)$  scheme for binary secret image1

### 5.1 Image illustration

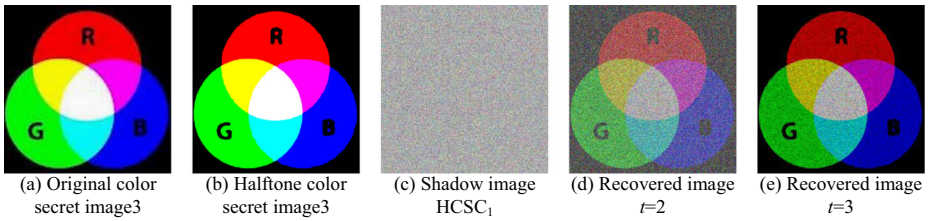
In our experiments, (3, 3) (i.e.,  $k=3, n=3$ ) threshold with secret image1, (3, 4) threshold with secret image2, (2, 3) threshold with color secret image3, are used to do the test of the proposed scheme. The (3, 3) threshold and (3, 4) threshold aim to show the effectiveness and security of the proposed  $(k, n)$  PVSS where  $k$  is more than 2, while (2, 3) threshold is to show the extension.

Figure 4b–d show the 3 shadow images, which are random noise-like. Figure 4e shows the recovered binary secret image with stacking recovery, from which the recovered secret can be revealed by stacking 3 shadow images. Figure 4f–h show the recovered binary secret image with any  $t=2$  with stacking recovery, from which there is no information of secret can be revealed by stacking less than  $k$  shadow images.

Figure 5b–e show the 4 shadow images, which are random noise-like. Figure 5f–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;



**Fig. 5** Experimental example of the proposed (3, 4) scheme for binary secret image2



**Fig. 6** Experimental example of the proposed (2, 3) scheme for color secret image3

The secret image recovered by  $t=n=4$  shadow images is better than by  $t=3$  shadow images. Figure 5k–p shows the recovered secret image with any less than  $k$  shadow images based on stacking recovery, from which there is no information could be recognized.

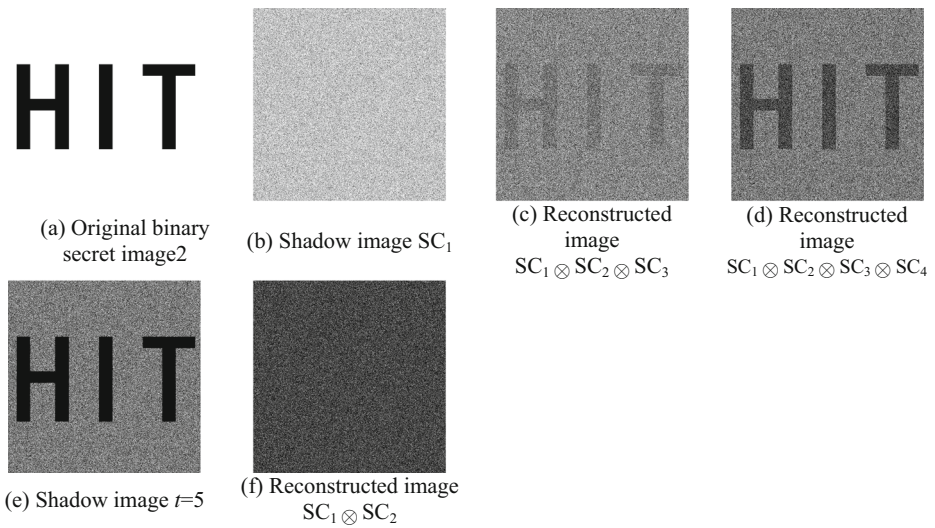
Figure 6b–c show the halftone color secret image and one shadow image  $HCSC_1$  for color secret image 4, which are random noise-like. Figure 6d, e show the recovered secret image with any 2 (taking 1, 2 as an example) or 3 shadow images with stacking recovery, from which the progressive visual quality will be gained and the secret image recovered by  $t=k=2$  shadow images could be recognized based on stacking; The visual quality of secret image recovered by  $t=n=3$  shadow images is better than by  $t=2$  shadow images.

From the results shown in Figs. 4, 5 and 6, we can conclude that:

- The shadow images are random noise-like, hence the proposed scheme has no cross interference from secret image in the shadow images.
- The progressive visual quality of the recovered secret can be gained for the proposed scheme.
- 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.
- The proposed scheme can also be applied for grayscale and color images.
- Although the visual quality of the proposed scheme is low and maybe worse than related researches, the proposed scheme is  $(k, n)$  threshold PVSS, since VC is lossy by nature, there will cause some contrast loss in recovering.
- The shadow images are equal to each other. The order is alternative during the reconstruction phase and one share is requested to be held by each participant.

Based on the proposed construction method, a more threshold PVSS scheme is constructed from Chen et al.'s  $(2, n)$  PVSS to evaluate the efficiency of the proposed construction method. One example is illustrated in Fig. 7, which shows that Chen et al.'s scheme can also be extended by the proposed construction method.

Figure 7b shows one shadow image  $SC_1$ , which is noise-like. Figure 7c–e show the reconstructed secret image with any 3 or more shadow images by stacking recovery, from which the secret image could be recognized based on stacking. Figure 7f shows the reconstructed secret image with any less than 3 shadow images based on stacking recovery, from which there is no information could be recognized.



**Fig. 7** Experimental example of the proposed (3, 5) threshold construction from Chen et al.’s (2, n) PVSS

### 5.2 Visual quality of the recovered secret images

In this section, the visual quality of the recovered secret images is evaluated by contrast in Definition 1. The same original binary secret images as shown in Figs. 4 (a) and 5 (a) are used to do the experiments of contrast.

Average contrast of the proposed (k, n) scheme for binary secret images 1 and 2 is shown in Table 2. Where t is the number of recovered shadow images.

From Table 2, we can find that, in the proposed scheme, the contrast increases as t increases for a certain (k, n) with stacking recovery when  $2 \leq n \leq 5, 2 \leq k < n$ , the progressive visual quality can be achieved.

**Table 2** Average contrast of the proposed scheme with stacking recovery for binary secret images 1 and 2

(k, n)	Secret image 1				Secret image 2			
	t=2	t=3	t=4	t=5	t=2	t=3	t=4	t=5
(2, 2)	0.50002				0.49989			
(2, 3)	0.24991	0.66654			0.25068	0.66758		
(3, 3)		0.24949				0.24966		
(2, 4)	0.16685	0.40022	0.75028		0.16581	0.39897	0.74871	
(3, 4)		0.10336	0.33341			0.10237	0.33193	
(4, 4)			0.12516				0.12515	
(2, 5)	0.12461	0.28527	0.49948	0.79937	0.12554	0.28633	0.50071	0.80086
(3, 5)		0.05564	0.17024	0.3749		0.05574	0.1705	0.37544
(4, 5)			0.04465	0.16647			0.04526	0.1673

### 5.3 Comparisons with related schemes

In the section, we compare the proposed scheme with other related PVSS schemes [7, 8, 11] especially [11], since the proposed scheme is a continuous and extension work of the schemes [11]. In addition, scheme in [11] has good features in PVSS, such as no pixel expansion and so on.

Furthermore, we compare the proposed scheme with other related  $(k, n)$  VSSs especially Chen and Tsao's scheme [13], and Guo et al.'s scheme [20], since schemes in [13] and [20] have good features in VSS, such as  $(k, n)$  threshold, no pixel expansion and so on.

Fang and Lin [8] realized a PVSS through expanding every secret pixel into a  $2 \times 2$  block. However, it has pixel expansion and cross-interference of secret information on shares, which will lead to more storage space and severe security problem. While our method has no pixel expansion and cross-interference. The visual quality of Fang and Lin's method is less than 50 %, while ours is  $\frac{t-1}{n}$  in a  $(2, n)$  PVSS which will be more than 50 % when all the  $n$  shadow images are collected.

Hou et al. [7] utilized image block to design two  $(2, n)$  PVSS, which have progressive and partial quality for the recovered secret images when more shadows are available. Unfortunately, the method fails to support  $(k, n)$  threshold, while ours is a general  $k$  out of  $n$  mechanism. The visual quality of Hou et al.'s  $(2, n)$  PVSS method is also less than 50 % when stacking all the  $n$  shadow images, which is less than ours.

Hou and Quan [11] proposed a  $(2, n)$  PVSS with unexpanded shares by designing two basic sharing matrices. In Hou and Quan's scheme, the possibility of either black or white pixels to appear as black pixels on the shares is equal to  $1/n$ . Although when more shares are stacking, clearer secret will be gained, Hou and Quan's scheme fails to support  $(k, n)$  threshold, which will restrict the application range. The proposed scheme is an improved method of Hou and Quan's scheme, which has no pixel expansion with a general  $k$  out of  $n$  mechanism. From Theorem 1, when  $k=2$ , the contrast of the proposed scheme is  $\frac{t-1}{n}$ , which is the same as Hou and Quan's scheme.

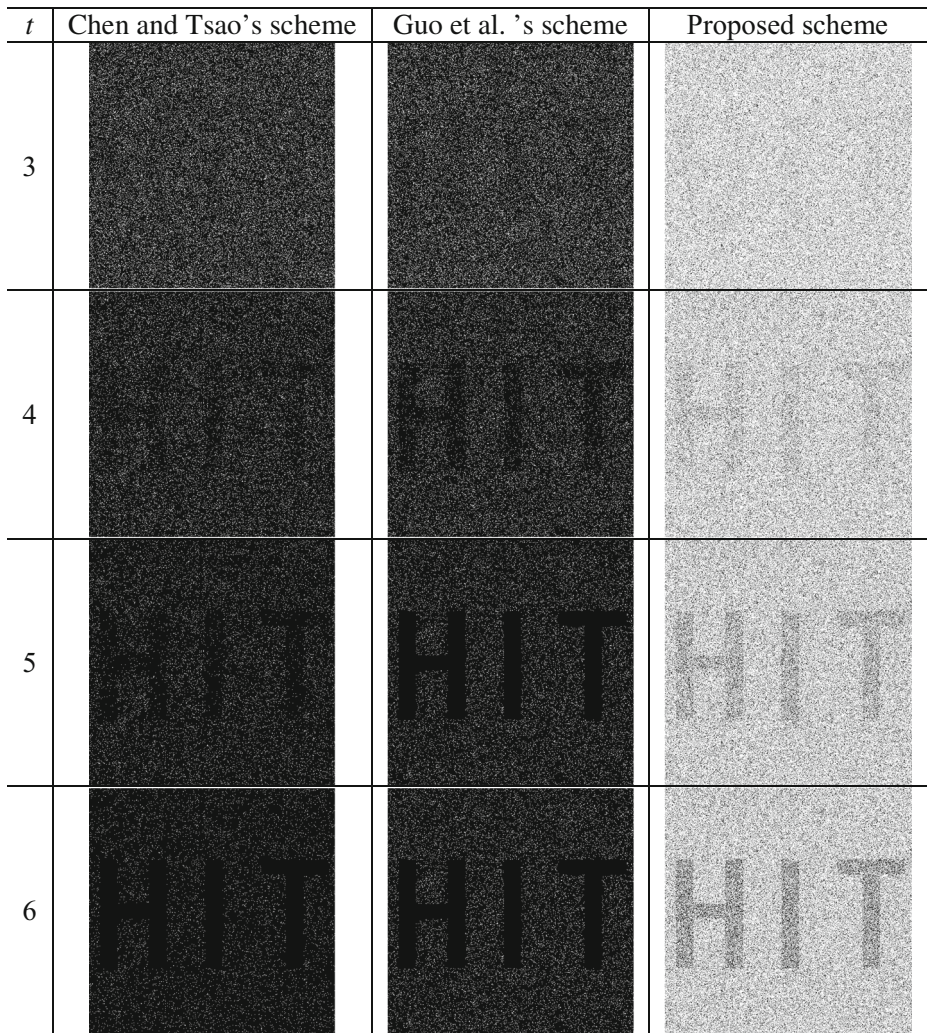
Theoretical contrast of Hou and Quan's  $(2, n)$  ( $2 \leq n \leq 5$ ) scheme is shown in Table 3. By comparing Table 2 and Table 3, we can see that the progressive visual quality of the proposed scheme and Hou and Quan's  $(2, n)$  can be achieved. In addition, the experimental results of the proposed  $(2, n)$  are overall the same as Hou and Quan's scheme. Hence, the contrast of the proposed scheme is the same as Hou and Quan's  $(2, n)$  PVSS. However, Hou and Quan's scheme is only for case  $(2, n)$ , while the proposed scheme is for case  $(k, n)$ .

Figure 8 indicates the comparison between the proposed scheme and schemes in [13] and [20] for case  $(3, 6)$ . By all appearances, the proposed scheme has competitive visual quality compared with the other two methods.

Table 4 shows the functionality comparison between the proposed scheme and other schemes. From Table 4, we can see that the proposed scheme has good properties than other competitive schemes. Compared with Hou and Quan's scheme [11], the proposed scheme is a general  $k$  out of  $n$  PVSS.

**Table 3** Theoretical contrast of Hou and Quan's  $(2, n)$  scheme

$(2, n)$	$t=2$	$t=3$	$t=4$	$t=5$
$(2, 2)$	0.5			
$(2, 3)$	0.25	0.666667		
$(2, 4)$	0.166667	0.4	0.75	
$(2, 5)$	0.125	0.285714	0.5	0.8



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

**Table 4** Properties comparison with relative schemes

Scheme	Progressive	$(k,n)$ threshold	Recovering measure	No pixel expansion
Ref. [2]	×	√	Boolean	√
Ref. [4]	×	√	Stacking	×
Ref. [13]	√	√	Stacking	√
Ref. [19]	×	√	Stacking	√
Ref. [11]	√	$(2, n)$	Stacking	√
Proposed scheme	√	$(k, n)$	Stacking	√

## 5.4 Significance of the proposed scheme

In order to highlight the merits of the proposed scheme, further discussions are examined as follows.

### 5.4.1 $(k, n)$ threshold

Thanks to the Hou and Quan's PVSS, the proposed scheme is  $(k, n)$  threshold: share the secret image among  $n$  shadow images and need at least  $k$  shares to recover the secret image. The merit could be loss-tolerant and control access for a wider application.

### 5.4.2 No pixel expansion

Thanks to the extension from Hou and Quan's scheme, the skillful design makes no pixel expansion occurred in the proposed scheme, which could reduce the storage and transmission bandwidth.

### 5.4.3 Extension for grayscale/color images

Thanks to halftone technologies and color model, the proposed scheme can be extended for grayscale/color images.

## 6 Conclusion

An efficient general threshold progressive visual secret sharing, threshold PVSS, construction method from  $(2, n)$  PVSS with unexpanded shares is proposed in this paper, which could be loss tolerant and access control for a wider application. The secret image can be recovered by human visual system with no cryptographic computation and pixel expansion. We have performed several experimental results and analysis to evaluate the security and efficiency of the proposed construction method. Based on the proposed construction method, a new threshold PVSS scheme is constructed. Comparisons with previous approaches suggest that the constructed PVSS scheme has several merits and outperforms relative approaches. 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.

**Acknowledgement** The authors would like to thank the anonymous reviewers for their valuable discussions and comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61100187, 61301099, 61361166006).

## References

1. Chen S-K (2009) Friendly progressive visual secret sharing using generalized random grids. *Optical Eng* 48(11):117001-1–117001-7
2. Chen T-H, Tsao K-H (2011) Threshold visual secret sharing by random grids. *J Syst Software* 84:1197–1208
3. Chen T-H et al (2013) Quality-adaptive visual secret sharing by random grids. *J Syst Softw* 86(5):1267–1274



4. Fang W-P, Lin J-C (2006) Progressive viewing and sharing of sensitive images. *Pattern Recog Image Analysis* 16(4):632–636
5. Guo T, Liu F, Wu CK (2013) Threshold visual secret sharing by random grids with improved contrast. *J Syst Software* 86(8):2094–2109
6. Hou Y-C (2003) Visual cryptography for color images. *Pattern Recogn* 36(7):1619–1629
7. Hou Y-C, Quan Z-Y (2011) Progressive visual cryptography with unexpanded shares. *IEEE Trans on Circ and Sys for Video Tech* 21(11):1760–1764
8. Hou Y-C, Quan Z-Y, Tsai C-F (2013) Block-based progressive visual secret sharing. *Inf Sci* 233:290–304
9. Jin D, Yan W-Q, Mohan S (2005) Kankanhalli, Progressive color visual cryptography. *SPIE J Electron Imaging* 14(3)
10. Naor, Moni, and Adi Shamir (1995) Visual cryptography, in *Advances in Cryptography, Eurocrypt'94*, pp. 1–12
11. Shyu SJ (2007) Image encryption by random grids. *Patt Recog* 40.3:1014–1031
12. Shyu SJ (2009) Image encryption by multiple random grids. *Patt Recog* 42:1582–1596
13. Wang Z, Arce GR, Di G (2009) Crescenzo. Halftone visual cryptography via error diffusion *IEEE Trans Inf Forensics Security* 4(3):383–396
14. Wang D, Zhanga L, Ma N, Li X (2007) Two secret sharing schemes based on Boolean operations [J]. *Pattern Recogn* 40(10):2776–2785
15. Weir J, Yan WQ (2010) A comprehensive study of visual cryptography, *Transactions on DHMS V. LNCS* 6010:70–105
16. Wu X (2013) Wei Sun, Random grid-based visual secret sharing with abilities of OR and XOR decryptions. *J Vis Commun Image R* 24:48–62
17. Wu X, Sun W (2013) Improving the visual quality of random grid-based visual secret sharing. *Signal Process* 93(5):977–995
18. Yan X, Shen W, Abd El-Latif AA, Niu X (2014) A novel perceptual secret sharing scheme. *Trans Data Hiding Multimedia Secur IX Lect Notes Comp Sci* 8363:68–90
19. Yan X, Wang S, El-Latif AAA et al. (2013) Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery[J]. *Multimedia Tools and Applications* :1–22
20. Yang C-N (2004) New visual secret sharing schemes using probabilistic method [J]. *Pattern Recogn Lett* 25(4):481–494



**Xuehu Yan** was born in China, in Feb 1984, received the B.Sc. degree with honor rank in Science in Information & Calculate Science from Harbin Institute of Technology, China in 2006, M.Sc. degree in Computational Mathematics in 2008, and doctoral degree in Computer Science and Technology in 2015 from Harbin Institute of Technology. He now is a teacher at Electronic Engineering Institute, Hefei, P. R. China. His areas of interests are cryptography, multimedia security, secret image sharing and biometrics.



**Shen Wang** received the B.S. and M.E. degrees in electrical engineering and information technology from TU-Dresden, Germany, in 2001 and 2007, respectively, and the Ph.D degree in computer science from Harbin Institute of Technology, China, in 2012. Currently, he is a lecturer in the Department of Computer Science, Harbin Institute of Technology. His research interests include image disguise, digital forensics and quantum information processing etc.



**Xiamu Niu** was born in China, in May 1961, received the B.S. degree and M.S. degree in Communication and Electronic Engineering from Harbin Institute of Technology (HIT), Harbin, P. R. China in 1982 and 1989 respectively, and received the Ph.D degree in Instrument Science and Technology in 2000. He was an invited scientist and staff member in Department of Security Technology for Graphics and Communication System, Fraunhofer Institute for Computer Graphics, Germany, from 2000 to 2002. He was awarded the Excellent Ph.D Dissertation of China in 2002. He now is the Professor (doctoral advisor) and Superintendent of Information Countermeasure Technique Institute HIT, Director of Information Security Technique Research Center, HIT-ShenZhen. He is SPIE member, ACM member, IEEE member, and the advanced CIE member. He has published 3 works and more than 150 papers were cited by SCI and EI. His current research fields include computer information security, hiding communication, cryptography, digital watermarking, signal processing and image processing etc.