Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 16(5): 5750–5764.
DOI: 10.3934/mbe.2019287
Received: 25 January 2019
Accepted: 29 May 2019
Published: 20 June 2019

Research article

Weighted visual secret sharing with multiple decryptions and lossless recovery

Feng Liu, Xuehu Yan*, Lintao Liu, Yuliang Lu and Longdan Tan

National University of Defense Technology, Hefei 230037, China

* **Correspondence:** Email: publictiger@126.com.

Abstract: Traditional visual secret sharing (VSS) encodes the original secret image into n shares, and each share is of equal importance. However, in some scenarios, we need to make a difference between the participants according to the levels of their importance. Therefore, the capability of each share to recover the original secret image will be different. In this paper, we proposed a weighted (k, n)-threshold random grid VSS(RG-VSS) with multiple decrytions and lossless recovery. When we get k or more shares for decryption, we will recover different levels of the original image because of the different weights of the shares. More importantly, the secret information can be recovered by OR and XOR operations in our scheme. When we get all the n shares and using the XOR operation to recover the image, we can recover the secret information losslessly. The experimental results and analyses show that our scheme outperforms the related schemes.

Keywords: visual secret sharing; random grid; weighted; multiple decryptions; lossless recovery

1. Introduction

With the rapid development of information security technology [1–6], visual secret sharing (VSS) technology has also developed rapidly. Traditional visual secret sharing [7, 8] encodes the secret information into different shares, then distributes the shares to the participants. And we can stack the shares to decode the secret of VSS. The decryption does not need any cryptographic knowledge on computational devices.

In 1995, Naor and Shamir [7] first proposed the threshold-based VSS [8–15] to encode the secret images. In their scheme, a binary secret image is encoded into n noise-like shadow images, and each shadow image is also called a share. And each share is distributed to one of the participants. Only when any k or more participants stack their shares together can recover the secret information visually. However, when less than k participants will not decode any information. Then some researchers have applied VSS to many different fields such as authentication [16], information hiding,

digital watermarking [17] and so on [18]. The advantage of VSS by [7] is simple recovery, because the decryption is only based on stacking without any cryptographic computation and computational devices. But, the scheme also has some disadvantage of pixel expansion, codebook design.

Some researchers proposed different VSS approaches to solve the problem of pixel expansion. Such as, Ito, et al. [19] selected a column from codebook with equally likely possibility and proposed the probabilistic VSS. Later Yang, et al. [10] presented the different thresholds probabilistic VSS. Soon Cimato, et al. [11] further proposed the generalization probabilistic VSS.

Random grid (RG) is a kind of image encoding method proposed by Kafri and Keren [20]. Their scheme could produce two noise-like shares by randomly selecting the pixel values. The method successfully solved the two problems of the conventional VSS scheme: The pixel expansion problem and codebook design. So the method got people's attention. But, the RG-VSS could only realize a $(2, 2)$-threshold. Soon, many scholars proposed their schemes to extend the work of Kafri and Keren's scheme. And they have developed the (n, n)-threshold and (k, n)-threshold RG-VSS. However, in RG-VSS, when we use OR-based VSS (OVSS), the background of the recovery image will become darker. When we use RG XOR-based VSS (XVSS) [12, 21] can improve the visual quality of the recovery image, so as to solve the problem of darker background caused by RG-based OVSS [22]. However, only when we have the lightweight device that can perform XOR operation, we can use the device to recover the image through XVSS. Generally speaking, RG-VSS with multiple decryptions [22, 23] can realize OVSS and XVSS, which can be applied in wider applications.

In traditional VSS, the secret images can be recovered by a certain number of shares. Moreover, each share has the same capability to recover the secret images, and does not differ.

Hou, et al. [24] implemented a $(2, n)$-threshold VSS with different priority weights that has no pixel expansion. Their scheme assigned different priority weights to the shares according to the importance of the participants. Hence, each share will have their own priority, which means that we can reveal different amount of secret information when stacking different shares with the same number of shares. In such a way, when we get the shares with higher weights, we can get more messages of the secret image, and in a similar way, when we get the shares with lower weights, we will get less messages of the secret image. Although, the scheme presented by Hou, et al. implemented the different priority of the shares, the shares with different weights have the different average light transmission, which means that the shadow images of different weights will be different in color visually. So we can easily know which share is important. Yang, et al. [25] presented improved scheme of Hou, et al. 's scheme. In their scheme, each share has the same average light transmission, so the shares can't be distinguished visually. However, the scheme needs a codebook to generate the shares. Fan, et al. [26] proposed a priority RG-VSS for threshold access structures, in which the shares have the same average light transmission and do not need the codebook.

Unfortunately all the schemes above can not losslessly recover the secret image with multiple decryptions. In our previous work [9], we have realized RG-VSS with the abilities of or and xor lossless recovery. In [9], the shares have the same weight which means the share images have the same importance. However, in some applications we need to give different participants different levels of importance. This need us to give different share images with different weights and this is just the work of this paper.

The contribution of our proposed scheme is as follow. In this paper, we propose a weighted (k, n) RG-VSS. And our approach has two advantages. First, our scheme has two kinds of decryption

capabilities, which means we can use both OVSS and XVSS to recover the secret images. So it can be applied in wider applications. Second, our scheme is able to recover the secret images losslessly with XVSS. Therefore, our approach has the features of multiple decryptions and lossless recovery.

In our proposed scheme, a binary original image is generated into n shares, and each share has its own weight according to the level of the importance. First, we assign the weight according to the corresponding probability, and randomly select k positions from the n positions of the n shares. Second, we use the (k, k)-threshold RG-VSS to get the k pixel values to fill in the positions we selected previously. Third, the remaining $(n - k)$ positions will be assigned white (0) value [27]. In such a way, we get all the n pixel values on the corresponding positions in the n shares according to the weight of each share. And our scheme has the following features: We can recover the secret image by stacking. Meanwhile, if we have a lightweight device with XOR operation, we can recover the secret image losslessly when we get all the n shares. In addition to this, our scheme does not need codebook design and have no pixel expansion due to RG. And the effectiveness of our scheme will be given by experimental results and analyses.

The rest of the paper is organized as follows. In section 2 , we will introduce the basic concepts for our proposed scheme. In Section 3, we will propose our scheme in more details. In section 4, we will analyse the performance of our proposed scheme. In section 5 , we will provide experimental results. Finally, in section 6 , we will conclude this paper.

2. Preliminaries

In order to understand our method more conveniently. First, some definitions about our proposed scheme will be introduced. Also the notations used in our paper will be given in Table 1.

Table 1. Notations used in the paper.

Notations	Descriptions
0(resp. 1)	A white(resp. black) pixel
$\otimes$	Stacking (OR) operation
$\oplus$	Boolean XOR operation
S	The binary secret image
$SC_1, SC_2, \cdots SC_n$	Shadow images generated by VSS schemes
t	Number of collecting shares in the recovery phase
$SC_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}$	Stacked (XOR-ed) result by shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}$
$\alpha_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}$	Contrast of the revealed secret image from shares $SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}$ by stacking (XOR) recovery
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
$Prob$ (x)	the probability when any event x occurs

In our proposed scheme, we employ the random pixels to generate the shares, therefore the definitions used in our paper related to RG-based VSS will be presented as follows:

Definition 1 (Average light transmission)**.** *For each pixel s in the binary image S, which size is $M \times N$, the light transmission of each transparent (resp. opaque) pixel is defined as $T(s) = 1$ (resp. $T(s) = 0$). So, the average light transmission of S can be defined as*

$$T(S) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(S(i, j))}{M \times N} \tag{2.1}$$

Definition 2 (Contrast)**.** *The contrast is used to evaluated to the visual quality of the reconstructed image S' corresponding to the original image S . And the contrast is defined as follows:*

$$\alpha = \frac{T\left(S'\left[S\left(0\right)\right]\right) - T\left(S'\left[S\left(1\right)\right]\right)}{1 + T\left(S'\left[S\left(1\right)\right]\right)} \tag{2.2}$$

We can use the contrast to evaluate the visual quality of the recovered image. So the value of contrast is large, the reconstructed image will have better quality for human eyes to recognize.

Definition 3 (Visually recognizable)**.** *The reconstructed image S' can be recognized as the corresponding original image S, if $\alpha > 0$ when S' is reconstructed from the shares.*

Definition 4 (Security)**.** *When S' is reconstructed from the shares, we can identify the scheme proposed is secure if $\alpha = 0$, because it means that we can recognize no information of S through S' [7].*

The generation and reconstruction phases of the original $(2, 2)$ RG-based VSS can be described as follow:

Step 1: Randomly generate the SC_1.

Step 2: Compute the SC_2 as in Eq (2.3).

Reconstruction: $S' = SC_1 \otimes SC_2$ as in Eq (2.4). If the selected pixel $s = S(i, j)$ of S is 1, the reconstruction result $SC_1 \otimes SC_2 = 1$ will always be black. If the selected pixel is 0, the reconstruction result $SC_1 \otimes SC_2 = SC_1(i, j) \otimes SC_1(i, j)$ will have half chance to be white or black since the pixels of SC_1 are generated randomly.

$$SC_2(i, j) = \begin{cases} SC_1(i, j) & if\ S(i, j) = 0 \\ \overline{SC_1(i, j)} & if\ S(i, j) = 1 \end{cases} \tag{2.3}$$

$$\begin{aligned} S'(i, j) =& SC_1(i, j) \otimes SC_2(i, j) \\ =& \begin{cases} SC_1(i, j) \otimes SC_1(i, j) & if\ S_1(i, j) = 0 \\ SC_1(i, j) \otimes \overline{SC_1(i, j)} = 1 & if\ S_1(i, j) = 1 \end{cases} \end{aligned} \tag{2.4}$$

We can derive that Eq (2.3) is equal to $sc_2 = sc_1 \oplus s$ or $s = sc_1 \oplus sc_2$. Because 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 it can be extended to $s = sc_1 \oplus sc_2 \oplus \cdots \oplus sc_k$. In a word, we will apply the XOR operation in the reconstruction. And when we get all the n shares together, we even can recover the original secret image losslessly.

3. The proposed scheme

In this section, we will propose a weighed (k, n) -threshold scheme, which has the abilities of multiple decryptions and lossless recovery. In the scheme, the secret image will be shared into n different weighted shares. And the important participants can have the shares of priority weight so that they will have more information. When we stack $t \geq k$ shares, the information in the secret image will be recovered with different weights, according to the priority weights and the number of the shares. Therefore, the shares being stacked with higher weights can recover more information of the original image. Conversely, the shares being stacked with lower weights will reveal less information

of the original image. And the secret image recovery of our proposed scheme can also be XOR, so the scheme has the abilities of multiple decryptions. When we using XOR operation to recover the secret image with all the shares, we even can recover the secret image losslessly.

We can know the share construction of our proposed scheme in Figure 1. And the scheme will be introduced as follows:

The proposed (k, n)-threshold weighted scheme will generate n shares with the size of $M \times N$. When we get t shares ($t \geq k$), the binary original image S can be reconstructed. Before we encode the pixels, we should initialize the priority weight of each share w_i, $i = 1, 2, \ldots, n-1, n$, and $\sum_{i=1}^{n} w_i = 1$. The weight w_i corresponding to each share is defined related to the level of importance of the participant. And the shares with higher weight will recover more information. The weight value of each share w_i has no impact on the implement of our scheme. Successively, we should encode the pixel $s(i, j)$ in the secret image. First, we use the (k, k)-threshold RG-VSS to generate k pixel values b_i, $i = 1, 2, \ldots, k-1, k$. The (k, k)-threshold algorithmic steps are described in Algorithm 1.

Algorithm 1: (k, k) RG-based VSS

Input: A $M \times N$ binary secret image S, the threshold parameters (k, k)
Output: k shadow images $SC_1, SC_2, \cdots SC_k$

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: Random generate k bits $b_1, b_2, \cdots b_k$
Step 3: If $S(i, j) = b_1 \oplus b_2 \oplus \cdots \oplus b_k$, then retain the bits. Else randomly reverse one bit.
Step 4: Randomly rearrange the final k bits $b_1, b_2, \cdots, b_k$ to $SC_1(i, j), SC_2(i, j), \cdots, SC_k(i, j)$.
Step 5: Output the k shadow images $SC_1, SC_2, \cdots SC_k$.

The possibility of each pixel's value distribution in the n shares is according to the priority weight. First, we set the probability intervals according to the weights, and the sum of probability intervals is 1. Then we use random number to generate a random value for an interval of [0, 1]. The random number falling within which interval means that the position of the pixel is selected. Repeat the operation until we select k positions of the n shares. The share with higher weight will be selected more times, so it will have more valid values.

In general, the share with higher priority weight is more likely to reconstruct the original image. On the contrary, the share with lower priority weight is less likely to recover the original image. Therefore, a set of pixels p_i, $i = 1, 2, \ldots, k$, is selected according to the w_i. And the unselected $(n - k)$ can be assigned as 0 values. Finally, the values on the positions according to the original image of n shares are generated. So the (k, n)-threshold weighted algorithmic steps are described in Algorithm 2.

We can use OR and XOR operation to recover the secret image in our proposed scheme. In other word, our proposed scheme has the abilities of multiple decryptions. And we even can losslessly recover the original image using the XOR operation device when we get all the shares.

4. Performance analyses

In this section, we will theoretically analyze the performances of the security and the visual quality of our proposed scheme. When we apply stacking or XOR decryption by Theorem 1, we would prove that our proposed scheme is a valid (k, n)-threshold weighted RG-VSS. And in order to prove the theorem 1, some Lemmas will be given.

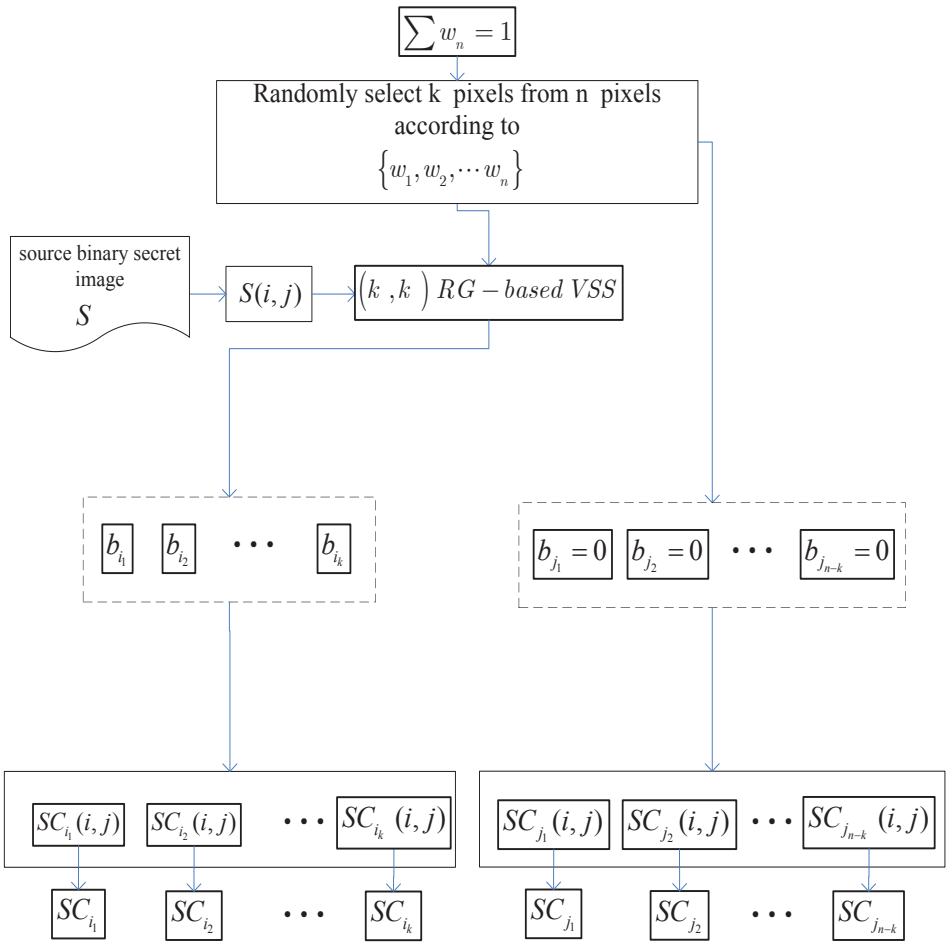


Figure 1. Shares generation architecture of the proposed scheme.

Algorithm 2: (k, n) weighted VSS with multiple decryptions and lossless recovery

Input: A $M \times N$ binary secret image S, the threshold parameters (k, n), and the weighted values $W = \{w_1, w_2, \cdots w_n\}$.

Output: n shadow images $SC_1, SC_2, \cdots SC_n$

Step 1: Gain its basis W sections according to its weighted values. For each position $(i, j) \in \{(i, j)|1 \leq i \leq M, 1 \leq j \leq N\}$, repeat Steps 2–4

Step 2: From $\{1, 2, \cdots n\}$, select one set $w = \{w_1, w_2, \cdots w_k\} \in W$ according to their weights, and the last $n - k$ number of all the n participants is denoted as $\{j_1, j_2, \cdots j_{n-k}\} = \{1, 2, \cdots, n\} \backslash \{i_1, i_2, \cdots i_k\}$.

Step 3: For the input secret bit $s = S(i, j)$ and $\{i_1, i_2, \cdots i_k\}$, compute $b_{i_1}, b_{i_2} \cdots, b_{i_k}$ using (k, k) RG-based VSS in Algorithm 1 and orderly arrange them to $SC_{i_1}(i, j), SC_{i_2}(i, j) \cdots, SC_{i_k}(i, j)$.

Step 4: Set all the last $n - k$ bits, i. e., $b_{j_1}, b_{j_2} \cdots, b_{j_{n-k}}$, to be 0, and arrange them to $SC_{j_1}(i, j), SC_{j_2}(i, j) \cdots, SC_{j_{n-k}}(i, j)$ directly.

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

In order to without losing of generality about the following analysis in this section, we will assume that $b_1, b_2, \cdots b_{k-1}, b_k$ are generated according to the pixel $s = S(i, j)$ of the original image and the $b_1, b_2, \cdots b_{k-1}, b_k$ bits are respectively arranged to $sc_1, sc_2, \cdots, sc_k$ by Step 3, the other bits $(b_{k+1}, b_{k+2}, \cdots b_n)$ will be assigned 0 by Step 4.

Lemma 1. $s = sc_1 \oplus sc_2 \oplus \cdots \oplus sc_k$.

Proof. Obviously, we can derive Eq (4.1) from Eq (2.3).

$$sc_2 = sc_1 \oplus s \quad \Rightarrow \quad s = sc_1 \oplus sc_2 \tag{4.1}$$

Because if $s = 0 \Rightarrow sc_2 = sc_1 \oplus 0 \Rightarrow sc_2 = sc_1$, or if $s = 1 \Rightarrow sc_2 = sc_1 \oplus 1 \Rightarrow sc_2 = \overline{sc_1}$. And, sc_1 and sc_2 are both random, so, $T(sc_1) = T(sc_2) = 1/2$. In the same way, the approach can be extended to

$$s = sc_1 \oplus sc_2 \oplus \cdots \oplus sc_k \tag{4.2}$$

Besides, $Prob\,(b_i = 0) = 1/2$ since b_i is randomly generated, where $i = 1, 2, \ldots, k-1, k$. So it is easy to get $T(sc_1) = T(sc_2) \cdots = T(sc_k) = 1/2$.

□

Lemma 2. *Each share generated from the* (k, n)*-threshold scheme will not reveal any clue about the original image:* $T\,(SC_i\,[S\,(0)]) = T\,(SC_i\,[S\,(1)])$*, where* $i = 1, 2, \ldots, n-1, n$.

Proof. According to Lemma 1 and Step 4, we can know that the generated pixel b_j, where $j = k+1, k+2, \ldots, n$, is independent of the original pixel $S(i, j)$. Therefore, $Prob\left(b_j = 0\right) = 1$ is obtained.

Obviously we can get $T\,(SC_i\,[S\,(0)]) = T\,(SC_i\,[S\,(1)])$ by Definition 1. So, we prove the Lemma.

□

Lemma 3. *In our proposed scheme,*

If $s = 0$, $T\,(b_{\{\otimes 1,2,\cdots k-1,k\}}) = T\,(b_{\{\otimes 1,2,\cdots k-2,k-1\}}) = (1/2)^{k-1}$.

If $s = 1$, $T\,(b_{\{\otimes 1,2,\cdots k-1,k\}}) = 0$.

Proof. According to Lemma 1, we can know that the bits $b_1, b_2, \cdots b_{k-1}$ are independent from each other and the original image s. But b_k is dependent on $b_1 \oplus b_2 \oplus \cdots b_{k-1}$ and the original image s.

Therefore,

$$\begin{aligned} T\,(b_{\{\otimes 1,2,\cdots k-2,k-1\}}[0]) &= (1/2)^{k-1}, \\ T\,(b_{\{\otimes 1,2,\cdots k-2,k-1\}}[1]) &= (1/2)^{k-1} \end{aligned} \tag{4.3}$$

So if $s = 0$, we can prove Eq (4.4).

$$T\,(b_{\{\otimes 1,2,\cdots k-1,k\}}) = T\,(b_{\{\otimes 1,2,\cdots k-2,k-1\}}) = (1/2)^{k-1} \tag{4.4}$$

Because if the bit $b_k = 0$, then
$b_{\{\otimes 1,2,\cdots k-1,k\}}[0] = b_{\{\otimes 1,2,\cdots k-2,k-1\}}[0]$ sets up.

Else if $b_k = 1$, then b_k is the same as one of $b_1, b_2, \cdots b_{k-1}$. If not, it means that every bit of $b_1, b_2, \cdots b_{k-1}$ is complementary to $b_k \Rightarrow b_1 = b_2 \cdots = b_{k-1} = 0 \Rightarrow s = 0 \oplus 0 \cdots \oplus 0 \oplus 1 = 1,\ k \in 2Z^+ - 1$ in conflict with $s = 0$.

Therefore, b_k is the same as one of $b_1, b_2, \cdots b_{k-1}$. Because of commutative law of OR($\otimes$) operation, $b \otimes b = b$ for any bit b , then we can get
$b_{\{\otimes 1,2,\cdots k-1,k\}}[0] = b_{\{\otimes 1,2,\cdots k-2,k-1\}}[0]$.

Hence, if $s = 0 \Rightarrow b_{\{\otimes 1,2,\cdots k-1,k\}}[0] = b_{\{\otimes 1,2,\cdots k-2,k-1\}}[0]$. In consequence, Eq (4.4) is set up.

Similarly, if $s = 1$, we can prove that at least one of $b_1, b_2, \cdots b_k$ is the same as 1. If not, every bit of $b_1, b_2, \cdots b_k$ is the same as $0 \Rightarrow b_1 = b_2 \cdots = b_k = 0 \Rightarrow s = 0 \oplus 0 \cdots \oplus 0 \oplus 0 = 0$ in conflict with $s = 1$. In consequence, at least one of $b_1, b_2, \cdots b_k$ is the same as 1, so that $b_{\{\otimes 1,2,\cdots k-1,k\}} = 1$.

Hence, we can get

$$T\left(b_{\{\otimes 1,2,\cdots k-1,k\}}\right) = 0 \tag{4.5}$$

□

Lemma 4. *The stacking (XOR-ed) operation result by any $t < k$ pixels will not reveal the secret: $T\left(b_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}[(0)]\right) = T\left(b_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}[(1)]\right)$, while by any $t \geq k$ pixels will reveal the secret: $T\left(b_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}[(0)]\right) > T\left(b_{\{\otimes(\oplus),i_1,i_2,\cdots i_t\}}[(1)]\right)$.*

Proof. Let us assume that the t pixels $b_{q_1}, b_{q_2}, \cdots b_{q_t}$ is a subset of $b_1, b_2, \cdots b_{n-1}, b_n$, so we can consider $t = t_1 + t_2$. the t_1 pixels $b_{q_1}, b_{q_2}, \cdots b_{q_{t_1}}$ are from $b_1, b_2, \cdots b_{k-1}, b_k$ introduced by Step 3, and the t_2 pixels $b_{q_{t_1+1}}, b_{q_{t_1+2}}, \cdots b_{q_{t_1+t_2}}$ are picked up from $b_{k+1}, b_{k+2}, \cdots b_n$ generated by Step 4.

Because $b_{k+1} = 0, b_{k+2} = 0, \cdots b_n = 0$, so $b_{\{\otimes(\oplus),q_1,q_2,\cdots q_t\}} = b_{\{\otimes(\oplus),q_1,q_2,\cdots q_{t_1}\}}$.

When $t < k$, it means $t_1 < k$ and $t_2 = 0$. According to Lemma 1, $T(b_1) = T(b_2) \cdots T(b_k) = 1/2$. As a result, $T(b_{\{\otimes(\oplus),q_1,q_2,\cdots q_t\}}) = T(b_{\{\otimes(\oplus),q_1,q_2,\cdots q_{t_1}\}})$ no matter $s = 0$ or $s = 1$, the secret cannot be revealed.

When $t \geq k$, we should consider two cases : Case 1: $t_1 < k$ and case 2: $t_1 = k$.

For case 1, we can get
$T(b_{\{\otimes(\oplus),q_1,q_2,\cdots q_t\}}) = T(b_{\{\otimes(\oplus),q_1,q_2,\cdots q_{t_1}\}})$ no matter $s = 1$ or $s = 0$.

For case 2, according to Lemma 3, $T\left(b_{\{\otimes 1,2,\cdots k-1,k\}}[0]\right) > T\left(b_{\{\otimes 1,2,\cdots k-1,k\}}[1]\right) = 0$.

Besides, by Lemma 1, we can get $b_{\{\oplus 1,2,\cdots k-1,k\}}[0] = 0$ and $b_{\{\oplus 1,2,\cdots k-1,k\}}[1] = 1$. So $T\left(b_{\{\oplus 1,2,\cdots k-1,k\}}[0]\right) = 1 > T\left(b_{\{\oplus 1,2,\cdots k-1,k\}}[1]\right) = 0$.

In a word, when $t \geq k$ we can get $T\left(b_{\{\otimes(\oplus)1,2,\cdots k-1,k\}}[0]\right) > T\left(b_{\{\otimes(\oplus)1,2,\cdots k-1,k\}}[1]\right)$. □

Theorem 1. *For the (k, n)-threshold weighted RG-VSS, the proposed scheme in the paper is a valid construction. Because it satisfies the following conditions:*

1) For each share reveals no information about the original image: $T\left(SC_i[S(0)]\right) = T\left(SC_i[S(1)]\right)$, where $i = 1, 2, \ldots, n-1, n$

2) For the stacking (XOR-ed) operation result by shares $t < k$ cannot reveal the secret: $T\left(SC_{\{\otimes(\oplus),j_1,j_2,\cdots j_q\}}[S(0)]\right) = T\left(SC_{\{\otimes(\oplus),j_1,j_2,\cdots j_q\}}[S(1)]\right)$.

3) The stacking (XOR-ed) operation result by shares $t \geq k$ visually discloses the secret: $T\left(SC_{\{\otimes(\oplus),i_1,i_2,\cdots i_q\}}[S(0)]\right) > T\left(SC_{\{\otimes(\oplus),i_1,i_2,\cdots i_q\}}[S(1)]\right)$.

Proof. According to Lemma 2, the first condition above is satisfied. According to Lemma 4, the second and third conditions above are satisfied.

□

5. Experimental results and analyses

In this section, we will present the experimental results and the analyses to show the effectiveness of our proposed scheme. In the experiments, the original binary secret image is showed in Figure 2a. And all the size of images is 512×512. The secret image is the standard image of Lena whose pixel values are distributed uniformly and the size of the image has no impact on this experiment. The size of 512×512 is the normal size in our experiments. As the compared schemes also use the same size images, which is convenient for comparison. For convenience to compare with other schemes, we set the threshold of our scheme is $(2, 4)$, and the weight of each share is $w = \{0.1, 0.2, 0.3, 0.4\}$.

5.1. Experimental results

The experimental results of our proposed scheme for $(2, 4)$-threshold weighted RG-VSS are presented in Figures 2 and 3, where the basis $w = \{0.1, 0.2, 0.3, 0.4\}$ is applied in Figure 2 by OR decryption and Figure 3 by XOR decryption.

In Figure 2 with the basis $w = \{0.1, 0.2, 0.3, 0.4\}$, the original binary secret image and the generated shares are all shown in Figure 2a–e, respectively. We can see that the generated shares are all noise-like, and the shares with lower weight in the basis w have more white(0) pixels than others.

When we employ the OR decryption, the results by any two or more shares are shown in Figure 2f–p. And the results clearly show that the visual quality of recovered image using the same number of the shares is different. The shares with higher weight will recover more information, and better visual quality will be shown when we get more shares. But the visual quality is dependent on the sum of the weights. For example, Figure 2l is obtained by stacking share 1, share 2 and share 3, with the weight of 0. 6. However, its visual quality is not good as Figure 2k, which is stacked by share 3 and share 4 with the weight of 0. 7.

When we employ the XOR decryption, the recovery secret images with any two or more together are shown in Figure 3f–p, the results is similar to the OR decryption results. Besides, we can see that the image visual quality is better than OR decryption. And we even can lossless recover the secret image when we collect all the shares together.

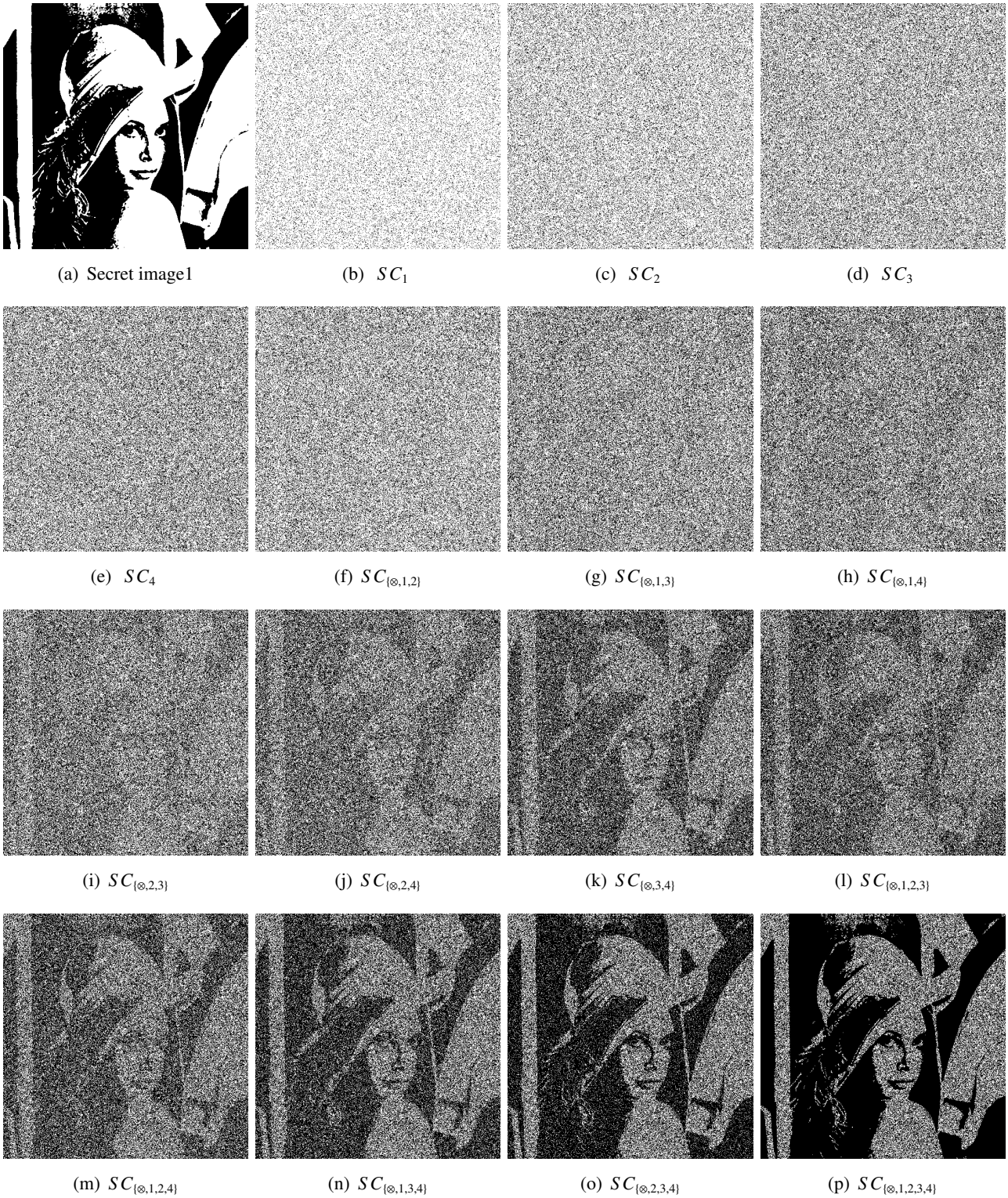
We can get the conclusions according to the results above:

1. Each share can not reveal any information of the secret image.
2. The visual quality of the reconstructed secret image is progressive when more shares are selected.
3. The weighted RG-VSS with multiple decryptions and lossless recovery is realized in our scheme.

5.2. Comparisons with related schemes

5.2.1. Contrast comparison

Table 2 shows the comparison of contrast between our proposed scheme and the related schemes with the basis $w = \{0.1, 0.2, 0.3, 0.4\}$ of $(2, 4)$-threshold. As the schemes presented by Hou, et al. [24] and Yang, et al. [25] are both the $(2, n)$-threshold VSS schemes, and the schmemes presented by Fan, et al. [26] and ourself are both the (k, n)-threshold VSS schemes. Therefore, in our experiment, we set the parameters of the threshold of (k, n) to be $(2, 4)$, as shown in Table 2.



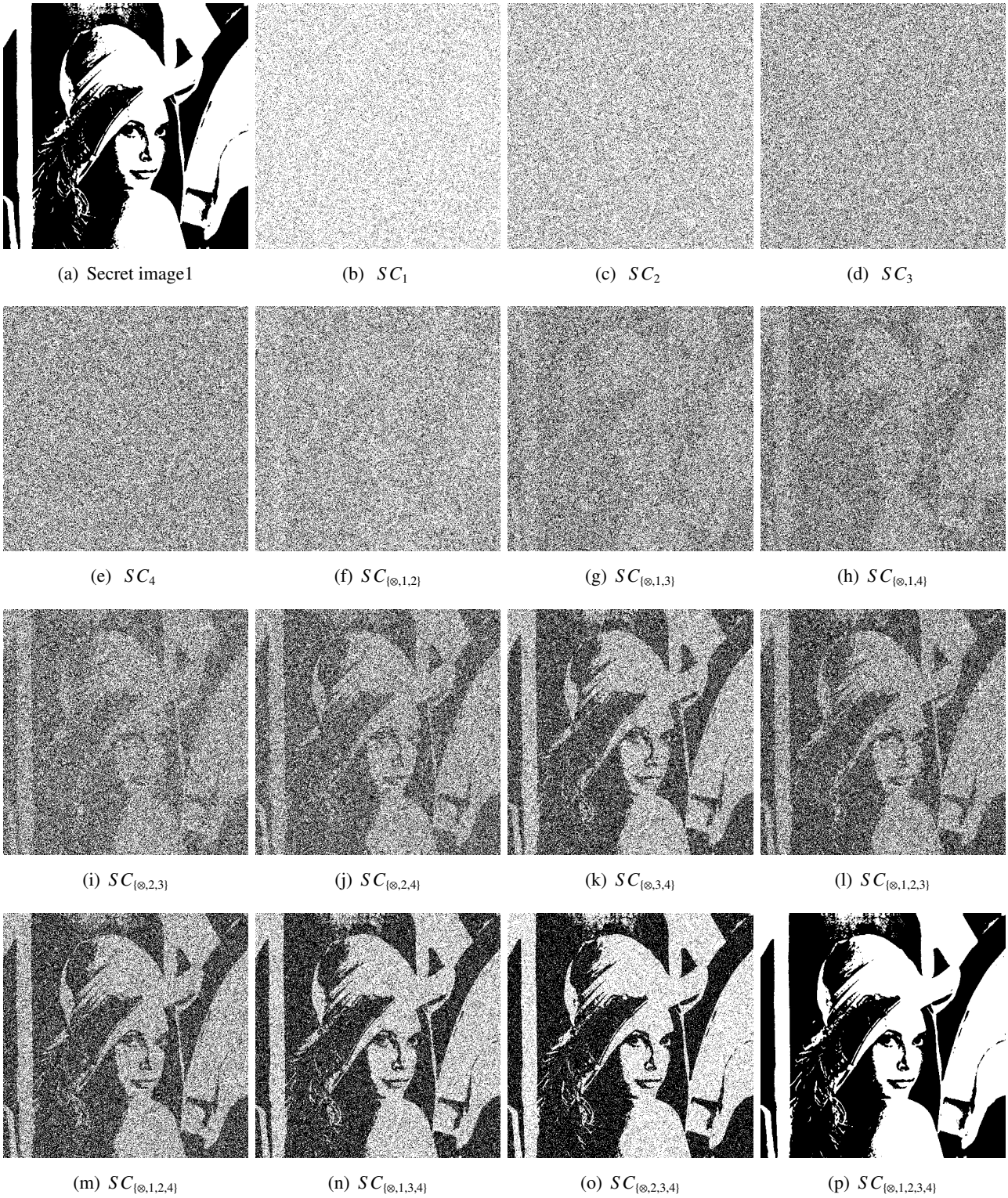
(a) Secret image1 (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $SC_{\{\otimes,1,2\}}$ (g) $SC_{\{\otimes,1,3\}}$ (h) $SC_{\{\otimes,1,4\}}$

(i) $SC_{\{\otimes,2,3\}}$ (j) $SC_{\{\otimes,2,4\}}$ (k) $SC_{\{\otimes,3,4\}}$ (l) $SC_{\{\otimes,1,2,3\}}$

(m) $SC_{\{\otimes,1,2,4\}}$ (n) $SC_{\{\otimes,1,3,4\}}$ (o) $SC_{\{\otimes,2,3,4\}}$ (p) $SC_{\{\otimes,1,2,3,4\}}$

Figure 2. Experimental result of our proposed scheme for $w = \{0.1, 0.2, 0.3, 0.4\}$ with OR decryption.



(a) Secret image1 (b) SC_1 (c) SC_2 (d) SC_3

(e) SC_4 (f) $SC_{\{\otimes,1,2\}}$ (g) $SC_{\{\otimes,1,3\}}$ (h) $SC_{\{\otimes,1,4\}}$

(i) $SC_{\{\otimes,2,3\}}$ (j) $SC_{\{\otimes,2,4\}}$ (k) $SC_{\{\otimes,3,4\}}$ (l) $SC_{\{\otimes,1,2,3\}}$

(m) $SC_{\{\otimes,1,2,4\}}$ (n) $SC_{\{\otimes,1,3,4\}}$ (o) $SC_{\{\otimes,2,3,4\}}$ (p) $SC_{\{\otimes,1,2,3,4\}}$

Figure 3. Experimental result of our proposed scheme for $w = \{0.1, 0.2, 0.3, 0.4\}$ with XOR decryption.

Based on Table 2, we can get the following conclusions:

1. The contrast of our proposed scheme is similar to others for OVSS.
2. Our scheme has two decryptions with OR and XOR.
3. If we get n shares, the recovery of our proposed scheme can be lossless for XVSS.

Table 2. Contrast comparison between our scheme and the related schemes with basis $w = \{0.1, 0.2, 0.3, 0.4\}$.

Number of shares	Our OR	Our XOR	Hou, et al. [24]	Yang, et al. [25]	Fan, et al. [26]
{1, 2}	0.0152	0.0289	0.0327	0.1096	0.1105
{1, 3}	0.0237	0.0478	0.0723	0.1531	0.1526
{1, 4}	0.0348	0.0478	0.1105	0.1985	0.1993
{2, 3}	0.0566	0.1107	0.1115	0.1986	0.1981
{2, 4}	0.0829	0.1647	0.1526	0.2491	0.2486
{3, 4}	0.1381	0.2777	0.2022	0.3045	0.3021
{1, 2, 3}	0.1056	0.2089	0.2496	0.2485	0.2488
{1, 2, 4}	0.1499	0.2995	0.3018	0.3040	0.3038
{1, 3, 4}	0.2276	0.4574	0.3654	0.3642	0.3623
{2, 3, 4}	0.3444	0.6875	0.4296	0.4278	0.4263
{1, 2, 3, 4}	0.5003	1.0	0.6665	0.4996	0.4988

5.2.2. Feature comparison

Table 3 shows the main features and the comparison of our proposed scheme with the related schemes. There are many indicators used to evaluate secret image sharing scheme. In this paper, only relevant features to the research branch of weighted secret image sharing are selected to evaluate the algorithm. The features shown in Table 3 are the main features that can reflect the pros and cons of the related schemes. The schemes of (k, n)-threshold are more scalable than other schemes of $(2, n)$-threshold. Also, the schemes with two decryptions of OR and XOR are more widely used than other schemes. Obviously, the schemes with no pixel expansion consume less storage space than other schemes. Similarly, the codebook design is complex. And in the schemes with lossless ability, the secret information can be losslessly recovered. The last weighted feature presents whether the share images of each scheme have different weights.

From Table 3, we can know that our proposed scheme has some advantages than the competitive schemes, such as: Multiple decryptions(OVSS and XVSS), lossless recovery and so on.

6. Conclusion

In this paper, we proposed a (k, n) weighted RG-VSS scheme with multiple decryptions and lossless recovery. Our scheme shares the secret image into n shares with the same size of the original image and has no pixel expansion. And our scheme also does not need a codebook to assist generating the shares. Besides, in our scheme, each share has its own weight according to the level of importance

of the participants who are holding them. When we get k or more shares stacked for decryption, we will recover different levels of messages from the original image because of the different weights of the stacked shares. Generally speaking, the decryption with higher weight shares can get more information about the original image, and the decryption with lower weight shares will get less information on the original image. In our scheme, the secret image can be recovered by OR and XOR operations. If we have a lightweight device with the ability to calculate XOR. When we get all the n shares using the XOR operation to recover the image, we can recover the secret image losslessly. And the experimental results and analyses reveal that our scheme outperforms the related schemes. However, we can see that our scheme has the limitation that the shares with different weights will have different average light transmission. So the next work of our scheme is to solve the problem that the shares don't have the same average light transmission.

Table 3. Feature comparison with relative schemes.

Scheme	Threshold	Recovering measure	No pixel expansion	No codebook design	Lossless	weighted
Shamir, et al. [7]	(k,n)	OR	√	√	×	×
Wu, et al. [28]	(k,n)	OR	√	√	×	×
Yan, et al. [27]	(k,n)	OR/XOR	√	√	√	×
Hou, et al. [24]	$(2,n)$	OR	√	×	×	√
Yang, et al. [10]	$(2,n)$	OR	√	×	×	√
Fan, et al. [26]	(k,n)	OR	√	√	×	√
Our	(k,n)	OR/XOR	√	√	√	√

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491) and National University of Defense Technology Foundation. The authors would like to thank the anonymous reviewers for their valuable discussions and comments.

Conflict of interest

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

1. Z.M. Yaseen, S.O. Sulaiman, R.C. Deo, et al., An enhanced extreme learning machine model for river flow forecasting: State-of-the-art, practical applications in water resource engineering area and future research direction, *J. Hydrology*, **569** (2019), 387–408.
2. A. Baghban, A. Jalali, M. Shafiee, et al., Developing an anfis-based swarm concept model for estimating the relative viscosity of nanofluids, *Eng. Appl. Comput. Fluid Mech.*, **13** (2019), 26–39.
3. C. Chuntian and K.W. Chau, Three-person multi-objective conflict decision in reservoir flood control, *Euro. J. Operational Res.*, **142** (2002), 625–631.

4. S. Samadianfard, A. Majnooni-Heris, S.N. Qasem, et al., Daily global solar radiation modeling using data-driven techniques and empirical equations in a semi-arid climate, *Eng. Appl. Comput. Fluid Mech.*, **13** (2019) 142–157.
5. C. Wu and K. Chau, Rainfall-runoff modeling using artificial neural network coupled with singular spectrum analysis, *J. Hydrology*, **399** (2011), 394–409.
6. R. Moazenzadeh, B. Mohammadi, S. Shamshirband, et al., Coupling a firefly algorithm with support vector regression to predict evaporation in northern iran, *Eng. Appl. Comput. Fluid Mech.*, **12** (2018), 584–597.
7. M. Naora and A. Shamir, Visual cryptography, *Advances in Cryptology-EUROCRYPT'94*, Italy: Springer, (1994), 1–12.
8. J. Weir and W. Yan, A comprehensive study of visual cryptography, *In: Transactions on DHMS V, LNCS 6010*, Berlin: Springer, (2010), 70–105.
9. X. Yan, S. Wang, A.A.A. El-Latif, et al., Visual secret sharing based on random grids with abilities of and xor lossless recovery, *Mult. Tools Appl.*, **74** (2015), 3231–3252.
10. C.N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognit. Lett.*, **25** (2004), 481–494.
11. S. Cimato, R. De Prisco and A. De Santis, Probabilistic visual cryptography schemes, *Comp. J.*, **49** (2006), 97–107.
12. D. Wang, L. Zhang, N. Ma, et al., Two secret sharing schemes based on boolean operations, *Pattern Recognit.*, **40** (2007), 2776–2785.
13. Z. Wang, G.R. Arce and G. Di Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Security*, **4** (2009), 383–396.
14. P. Li, P.J. Ma, X.H. Su, et al., Improvements of a two-in-one image secret sharing scheme based on gray mixing model, *J. Visual Commun. Image Representation*, **23** (2012), 441–453.
15. X. Yan, S. Wang, A.A.A. El-Latif, et al., Random grids-based visual secret sharing with improved visual quality via error diffusion, *Mult. Tools Appl.*, **74** (2015), 9279–9296.
16. S. J. Horng, S. F. Tzeng, Y. Pan, et al., b-specs+: Batch verification for secure pseudonymous authentication in vanet, *IEEE Trans. Inform. Forensics Security* **8** (2013), 1860–1875.
17. H. Ayad and M. Khalil, Qam-dwt-svd based watermarking scheme for medical images, *Int. J. Interactive Mult. Artificial Intelligence*, **5** (2018), 81–89.
18. F. Lopez, L. Valentn and I. Sarra, Detecting image brush editing using the discarded coefficients and intentions, *Int. J. Interactive Mult. Artificial Intelligence InPress*, 2018.
19. R. Ito, H. Kuwakado and H. Tanaka, Image size invariant visual cryptography, *IEICE Trans. Fundamentals Electronics, Commun. Comp. Sci.*, **82** (1999), 2172–2177.
20. O. Kafri and E. Keren, Encryption of pictures and shapes by random grids, *Optics Letters*, **12** (1987), 377–379.
21. P. Tuyls, H.D. Hollmann, J.H. Van Lint, et al., Xor-based visual cryptography schemes, *Designs Codes Cryptography*, **37** (2005), 169–186.

22. X. Wu and W. Sun, Random grid-based visual secret sharing with abilities of or and xor decryptions, *J. Visual Commun. Image Representation*, **24** (2013), 48–62.

23. X. Yan, S. Wang, X. Niu, et al., Random grid-based visual secret sharing with multiple decryptions, *J. Visual Comm. Image Representation*, **26** (2015), 94–104.

24. Y.C. Hou, Z.Y. Quan and C.F. Tsai, A privilege-based visual secret sharing model, *J. Visual Comm. Image Representation*, **33** (2015), 385–367.

25. C.N. Yang, J.K. Liao and D.S. Wang, New privilege-based visual cryptography with arbitrary privilege levels, *J. Visual Comm. Image Representation* **42** (2017), 121–131.

26. T.Y. Fan and H.C. Chao, Random-grid based progressive visual secret sharing scheme with adaptive priority, *Digital Signal Process.*, **68** (2017), 69–80.

27. X.H. Yan and Y.L. Lu, Progressive visual secret sharing for general access structure with multiple decryptions, *Mult. Tools Appl.*, **77** (2017), 1–20.

28. X. Wu, T. Liu and W. Sun, Improving the visual quality of random grid-based visual secret sharing via error diffusion, *J. Visual Comm. Image Representation*, **24** (2013), 552–566.

AIMS Press