Secure Progressive Visual Secret Sharing

Tai-Yuan Tu, Chih-Hung Wang and Tzung-Her Chen*

Department of Computer Science and Information Engineering, National Chiayi University

ABSTRACT

With visual secret sharing (VSS) in mind, to claim security guarantee of VSS is meaningful only when each single share image reveals no information about the secret image. Fang and Lin proposed a progressive visual secret sharing scheme, which claimed the secret image emerges gradually with the increasing number of stacking shares. However, their scheme fails to conceal secret information on any single share. As a result, a secret image is visually recognizable on each single share such that it is not a secure progressive visual secret sharing scheme. In order to overcome the above-mentioned problem and, simultaneously, achieve securely progressive property, a new progressive visual secret sharing method is proposed in this paper by redesigning basis matrices satisfying the security requirement for encoding the secret image. The experimental results illustrate that any single share looks noisy such that proposed visual secret sharing scheme is secure and progressive.

Keywords: progressive, visual secret sharing, visual cryptography, pixel expansion

安全漸進視覺秘密分享

涂泰源　王智弘　陳宗和*

國立嘉義大學資訊工程研究所

摘　　要

視覺密碼分享技術(VSS)惟有在任一單張分想影像(share)不顯露原始祕密影像訊息的情況下才有其意義與價值，Fang and Lin 所提出的漸進式視覺秘密分享技術中聲稱隨著堆疊的 share 數量增加，秘密影像將愈清楚明顯地逐漸浮現，然而，在他們的方法中，在任一單張分享影像並無法隱藏秘密資訊，以至於任一單張分享影像會顯露出原始秘密影項的訊息。因此，其所提的方法並不是一個安全的漸進式視覺秘密分享技術，為了解決前述的缺點同時達成安全漸進特性，本論文重新設計符合安全條件需求的 basis matrix 來編碼秘密影像，實驗結果也證明任一單張 share 是非常 noisy 沒有祕密影像顯示出來的現象，且當堆疊的 share 數量增加時影像也逐漸清晰浮現。

關鍵詞：漸進，視覺秘密分享，視覺密碼學，像素擴增

文稿收件日期 107.02.17;文稿修正後接受日期 107.11.01; *通訊作者

Manuscript received February 17, 2018; revised November 1, 2018; * Corresponding author

I. Introduction

In 1979, Shamir [1] first proposed the (k,n) secret sharing (SS) in which the main concept is to share a secret by a polynomial style. To achieve (k,n) SS, the secret is a constant term in a $(k\text{-}1)$ -degree polynomial and encoded into *n* shares, and decoded by Lagrange's interpolation. In 2002, Thien and Lin [2] proposed the first *k*-out-of-*n* polynomial-based secret image sharing (SIS) scheme to reconstruct secret images without any distortion by the Lagrange interpolation technique. In such a way, a certain of extensions to polynomial-based SIS have been presented to meet various applications such as authentication [3], remedy abilities [4], progressive secret image recovery [5], essentiality [6], etc.

However, since polynomial-based SIS schemes that apply Lagrange interpolation in the decoding phase may suffer intensive computation, some SIS schemes adopt bit-wise Boolean-based operations to benefit from comparatively low and cost-effective overhead. Inspired by that Wang et al. firstly proposed an exclusive-OR-based SIS (BSIS) scheme [7], Chen and Wu [8] proposed their Boolean-based multiple secret image sharing (BMSIS) scheme, in which *n* secret images are encoded into *n*+1 shares. Chen and Wu [9] proposed the improved scheme of Chen and Wu's scheme [8] which is improved by encoding *n* secret images into only *n* share images. In 2016, Chen et al. [10] and Yang et al. [11] pointed out that Chen and Wu [9] potentially suffers a threshold security problem such that it is possible to reveal partial information in case of decoding two consecutive shares.

Visual secret sharing (VSS) [12,13,14,15] is a secret sharing scheme for image data, utilizing the human visual system to decrypt the secret image by superimposing encrypted images without any computation and knowledge of cryptography. It was first proposed by Naor and Shamir [12] in 1995. Besides they also developed the constructions of visual cryptographic solutions for the general *k* out of *n* secret sharing problem, so-called (*k*,*n*) visual secret sharing (VSS). In (*k*,*n*) VSS scheme, an input image is transformed into *n* shares with noise-like appearance $S_1,S_2,\ldots,S_n$. Each noisy share conceals the information and ensures the unintelligibility of the secret. These shares can be printed on *n* transparent slides and then distributed to *n* participants. The secret image can be recovered if any *k* or more shares are stacked, but no information about the secret image can be revealed if less than *k* shares are stacked. To the end of sharing multiple secret images, more and more visual multiple secret sharing (VMSS) schemes have drawn attention recently, such as rotating shares at different degrees [16,17,18].

Taking encoding into account, the encoding way of VSS is mainly classified into visual-cryptography-based (VC-based) [12,13,15] and random-grid-based (RG-based) [14,19,20,21,22]. The features of VC-based VSS scheme can be summarized: 1) For each (*k*,*n*) case, it needs a tailor-made codebook for encoding, and 2) The size of generated share images is larger than the original secret image. Comparing with VC-based VSS, the feature of RG-based VSS is also considered: 1) It only needs to design an encoding algorithm, and the algorithm can be applied in each (*k*,*n*). 2) The size of share images and the reconstructed secret image keeps the same as the original secret image. The first threshold RG-based VSS was proposed by Kafri and Keren [19] in 1987 and enhanced [20,22] in 2007 and 2009. It is worthwhile to note that the VC-based VSS benefits from the high visual quality of disclosed secret images compared with RG-based VSS.

On the other hand, while taking decoding into account, it is interesting to combine the main properties of the polynomial-based SIS and the VSS to form a new two-in-one two-decoding-option scheme [23,24,25,26]. When the encoded share images are collected, the participants can decode them by combining these two schemes' properties, utilizing the VSS property to visually recognize the secret immediately by human visual system (HVS) and the polynomial-based SIS property to disclose the secret perfectly with a decoding device.

With the security of VC-based VSS, in 2006 Horng et al. [27] pioneer in pointing out

the (*k*,*n*) VC-based VSS potentially suffering the cheating of malicious participants aiming at mislead insider and honest participants by means of generating a fake share to cheat honest participants to accept the revealed fake secret information. Since then, a series of cheating prevention schemes [27,28,29,30,31,32,33] have been designed. Unfortunately, threshold RG-based VSS [20] was pointed out that it suffers from cheating problem [34] in 2012. In case of (2,*n*) (or (*k*,*n*)) RG-based VSS [20], at least 2 (or *k*) malicious participants can generate fake share images with a cheating message to cheat the rest participants.

Conventional (*k*,*n*)-threshold (VSS) is an all-or-nothing scheme. That is, when any *k* or more shares are superimposed, the secret image is revealed. No information about the secret image can be revealed if less than *k* shares are stacked. This type of sharing policy reveals either the entire image or nothing. In daily life, however, not all confidential data are secret. Some progressive visual secret sharing (PVSS) schemes [35,36,37,38,39,40,41] are proposed in the previous literature. The major difference between conventional and progressive VSS is the way of revealing secret image. In conventional (*k*,*n*)- threshold VSS, we could only construct an image of single resolution so long as *k* or more shares are stacked, while in progressive VSS, the amount of information about secret image is released by means of the number of shares collected. The more shares stacked, the clearer secret image is. In other words, we not only reveal the information about secret image by stacking the threshold number of shares together, but also utilize the other shares to enhance resolution of the reconstructed image.

Fang and Lin [35] proposed a PVSS scheme that not only builds the reconstructed image by stacking threshold number of shares together, but also utilizes the other shares to gradually enhance the resolution of the reconstructed image. For the progressive property, the revealed secret image will have better contrast and be clearer when more shares are stacked progressively. The scenario [35] is described. Assume that each VIP teammate of a company team has more than one shares while the other teammates only have one share. That is, the members of teammates of a company team are weighted. Upon viewing of the secret image, the very simple stacking action is done such that a benefit inherited from traditional visual cryptography is obtained. The potential application is given simultaneously. As not everything top secret, a teammate is not always to be selling good quality pictures or blueprints on the black market, but cooperates and discusses to hence improve the commerce-valued design shown on the blueprints.

However, their design would reveal the information about the secret image on each share and result in serious security problem that each share can obviously reveal information of the secret image.

Since security is always one of the main concerns for a new cryptosystem, the cryptanalysis to Fang and Lin's scheme is a must. With VSS in mind, to claim security guarantee of VSS is meaningful only when each single share image reveals no information about the secret image. The key weak design mentioned above will be shown by means of conducting some counter examples. In order to overcome the afore-mentioned problem, this paper proposes a new secure progressive visual secret sharing method by redesigning basis matrices that satisfy both contrast and security conditions. Thus, the superiority, such as the progressive disclosure of the original secret in Fang and Lin's scheme is kept. The experimental results show that the proposed scheme not only satisfies security requirement but is progressive.

The rest of this paper is organized as follows. In Section 2, Fang and Lin's progressive visual secret sharing scheme is briefly reviewed. In Section 3, the detail of the proposed scheme is described. Section 4 presents the experimental results. Section 5 gives the discussions and Section 6 makes a concluding remark.

II. Review of Fang and Lin's scheme

This section briefly reviews Fang and Lin's progressive VSS method and points out the weakness of their design in which a share potentially reveals the secret.

2.1 Fang and Lin's scheme

Fang and Lin's progressive VSS scheme encompasses the following phases.

(1) Size expansion

Firstly, in order to derive the expanded version of a secret image, each pixel is expanded to a 2 × 2 block. When each secret pixel is expanded into a 2 x 2 sub-pixel block, the following properties should be satisfied. If the secret pixel is black, all four elements of the 2 x 2 sub-pixel block in the expanded image are set to black; otherwise, two elements of the 2 x 2 sub-pixel block of the expanded image are randomly chosen, to be black and the other two white. After the procedure, an expanded secret image is generated. The size of expanded image is four times as that of original secret image.

(2) Share generation

Subsequently, while distributing into *n* shares, *n* shares with the same size of as the expanded image are generated. All elements of each share are initially set to white. For each black element of the expanded image, one or two shares are randomly selected from *n* shares, in which the corresponding elements in the chosen ones are painted black. Meanwhile the corresponding elements of the unchosen shares are kept white. While distributing the black elements to *n* shares, if a share has received two black elements in a 2 x 2 sub-pixel block, the share has to be ruled out from *n* shares of receiving current black element. It means that there are at most two black elements in a 2x2 sub-pixel block on a share.

(3) Slight modification

If a share image has obtained two black elements in the 2 × 2 block being processed, that share image is kicked out from the candidate set {1, 2, …, *n*} of receiving the current black element. The further modification to avoid guessing may be made, especially if the value of *n* is less than 4. Since each black block of (a block expanded from a black pixel of the original secret) has four black elements, and if there are only two or three share images, at least one share will obtain two black elements in the block being discussed. The participant with a share might therefore guess that each 2 × 2 of his share image having two black elements probably correspond to a black pixel. In such a way, a minor compensation modification is made. The readers may refer to Fang and Lin's scheme for details.

2.2 Security Analysis

Conventional (k,n) threshold VSS scheme can be designed using two basis $n\times m$ Boolean matrices B^0 and B^1 with elements "1" and "0" denoting black and white pixels, respectively. When encoding a white (resp. black) secret pixel, the dealer randomly chooses one row of the matrix in the white color set C^0 (resp. C^1), which includes all matrices obtained by permuting the columns in B^0 (resp. B^1) to a relative share. The chosen matrix defines the color of the secret pixel. Let the notation $OR(B^i \mid r), i = 0,1$ denote the "OR"-ed vector of any r rows in B^i, and $H(\cdot)$ is the Hamming weight function. The basis matrices for the conventional (k,n) threshold VSS scheme satisfy the following two conditions:

$H(OR(B^1 \mid r)) \geq (m-l)$ and $H(OR(B^0 \mid r)) \leq (m-h)$ for $r \geq k$,where $0 \leq l < h \leq m$ and h and l are the whiteness of white and black secret pixels.

$H(OR(B^1 \mid r)) = H(OR(B^0 \mid r))$, for $r \leq (k-1)$.

The first condition is related to the contrast of the reconstructed image, which shows that secret image can be visually revealed due to the different contrast of black and white colors. The contrast is $\alpha = \frac{(h-l)}{m}$. The second condition is related to the security of the scheme. It guarantees that any set of less than k shares stacked has no information on the shared image.

Assume the basis matrices B^0 and B^1 are constructed in Fang and Lin's scheme. "1" stands for a black pixel and "0" for a white pixel in both basis matrices B^0 and B^1 . Matrices B^0 and B^1 are used to encode a white pixel and a black pixel of the original secret image, respectively.

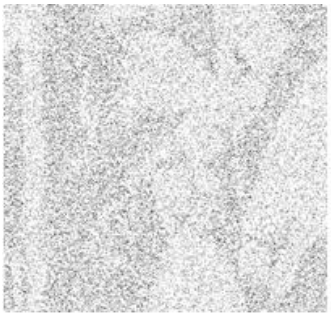
$$B^0=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\1&1&0&0\end{bmatrix}\quad B^1=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&1&1\\1&0&1&0\\1&0&0&1\\0&1&1&0\\0&1&0&1\\1&1&0&0\end{bmatrix}$$

Observing these two matrices, we find B^0 and B^1 are not the same size of matrices with the same frequencies. The appearance probability of 0,1 and 2 black pixels for a 2x2 sub-pixel block of a white pixel of the original secret image is 1/4, 2/4, and 1/4 respectively. On the other hand, the appearance probability of 0, 1, and 2 black pixels for a 2x2 sub-pixel block of a black pixel of the original secret image is 1/11, 4 /11, and 6/11, respectively. Table 1 gives the probability of all combinations of encoding basis matrices B^0 and B^1 for encoding white and black pixels in original image on a share respectively. The appearance probability of the row with 2 black sub-pixels in matrix B^1 is much more than the appearance probability of the same one in matrix B^0. This implies that a black block will be darker than a white one on each share.

The security condition will lead to creation of non-complete noise-like shares. In other words, each single share will reveal the information of the secret image. Fang and Lin's experimental results are shown in Fig. 1. To overcome the disadvantage, a secure and progressive VSS scheme will be proposed in the next session.

Table 1 The combinations of encoding basis matrices B^0 and B^1 on a single share

B^0	B^1	probability	α (contrast)	reveal
(0,0,0,0)	(0,0,0,0)	$\frac{1}{44}$	0	N
	(1,0,0,0)、(0,1,0,0)、(0,0,1,0)、(0,0,0,1)	$\frac{4}{44}$	0.25	Y
	(0,0,1,1)、(1,0,1,0)、(1,0,0,1)、(0,1,1,0)、(0,1,0,1)、(1,1,0,0)	$\frac{6}{44}$	0.5	Y
(1,0,0,0) (0,1,0,0)	(0,0,0,0)	$\frac{2}{44}$	0.25	Y
	(1,0,0,0)、(0,1,0,0) (0,0,1,0)、(0,0,0,1)	$\frac{8}{44}$	0	N
	(0,0,1,1)、(1,0,1,0)、(1,0,0,1)、(0,1,1,0)、(0,1,0,1)、(1,1,0,0)	$\frac{12}{44}$	0.25	Y
(1,1,0,0)	(0,0,0,0)	$\frac{1}{44}$	-0.5	Y
	(1,0,0,0)、(0,1,0,0) (0,0,1,0)、(0,0,0,1)	$\frac{4}{44}$	-0.25	Y
	(0,0,1,1)、(1,0,1,0)、(1,0,0,1)、(0,1,1,0)、(0,1,0,1)、(1,1,0,0)	$\frac{6}{44}$	0	N


share 1($\alpha = 0.25$)


(b) share 2($\alpha = 0.25$)


(c) share 3($\alpha = 0.25$)


(d) share 4($\alpha = 0.25$)


(e) share 5($\alpha = 0.25$))

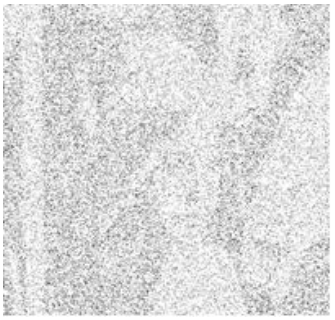

(f) share 6($\alpha = 0.25$)

Fig. 1 Fang and Lin's experimental results: (a)-(f) are six shares (*n*=6)

III. The proposed method

To achieve the goals of being secure and progressive, the basis matrix construction satisfying security and contrast is designed for encoding a secret pixel. Three sets of basis matrices are constructed in this scheme. Each is applied to different numbers of shares. Each pixel of the original secret will be expanded into a 2 x 2 sub-pixel block of black and white pixels.

3.1 Matrices design

The basis matrices for encoding a pixel of the original image into two shares are

$$B_2^{\,0} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$$B_2^{\,1}(0) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$B_2^{\,1}(1) = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$B_2^{\,1}(2) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Here, C_2^0 ={all the matrices obtained by permuting the columns of B_2^0} and C_2^1 = {all the matrices obtained by permuting the columns of $B_2^1(i)$ where $i \in \{0,1,2\}$}.

The basis matrices for encoding a pixel of the original image into three shares are shown in Fig. 2.

$$B_3^0=\begin{bmatrix}1&1&0&0\\1&1&0&0\\1&1&0&0\end{bmatrix}\quad B_3^1(0)=\begin{bmatrix}1&1&0&0\\1&0&1&0\\1&0&0&1\end{bmatrix}\quad B_3^1(1)=\begin{bmatrix}1&1&0&0\\1&0&1&0\\0&1&0&1\end{bmatrix}\quad B_3^1(2)=\begin{bmatrix}1&1&0&0\\1&0&1&0\\0&0&1&1\end{bmatrix}$$

$$B_3^1(3)=\begin{bmatrix}1&1&0&0\\1&0&0&1\\0&1&1&0\end{bmatrix}\quad B_3^1(4)=\begin{bmatrix}1&1&0&0\\1&0&0&1\\0&0&1&1\end{bmatrix}\quad B_3^1(5)=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&1&0&1\end{bmatrix}$$

$$B_3^1(6)=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\end{bmatrix}\quad B_3^1(7)=\begin{bmatrix}1&1&0&0\\0&1&0&1\\0&0&1&1\end{bmatrix}\quad B_3^1(8)=\begin{bmatrix}1&0&1&0\\1&0&0&1\\0&1&1&0\end{bmatrix}$$

$$B_3^1(9)=\begin{bmatrix}1&0&1&0\\1&0&0&1\\0&1&0&1\end{bmatrix}\quad B_3^1(10)=\begin{bmatrix}1&0&1&0\\0&1&1&0\\0&1&0&1\end{bmatrix}\quad B_3^1(11)=\begin{bmatrix}1&0&1&0\\0&1&1&0\\0&0&1&1\end{bmatrix}$$

$$B_3^1(12)=\begin{bmatrix}1&0&1&0\\0&1&0&1\\0&0&1&1\end{bmatrix}\quad B_3^1(13)=\begin{bmatrix}1&0&0&1\\0&1&1&0\\0&1&0&1\end{bmatrix}\quad B_3^1(14)=\begin{bmatrix}1&0&0&1\\0&1&1&0\\0&0&1&1\end{bmatrix}$$

$$B_3^1(15)=\begin{bmatrix}1&0&0&1\\0&1&0&1\\0&0&1&1\end{bmatrix}$$

Fig. 2 The basis matrices for encoding a pixel of the original image into three shares

Here, C_3^0 ={all the matrices obtained by permuting the columns of B_3^0} and C_3^1 = {all the matrices obtained by permuting the columns of $B_3^1(i)$ where $i\in\{0,1,2,\ldots,15\}$}.

The basis matrices for encoding a pixel of the original image into n (n ≧ 4) shares are

$$B_4^0=\begin{bmatrix}1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0\end{bmatrix}\qquad B_4^1=\begin{bmatrix}1&1&0&0\\1&0&1&0\\1&0&0&1\\0&1&1&0\\0&1&0&1\\0&0&1&1\end{bmatrix}$$

Here, C_4^0 ={all the matrices obtained by permuting the columns of B_4^0} and C_4^1 = {all the matrices obtained by permuting the columns of B_4^1}.

Any single row in $B_n^m,(m=0,1,n=2,3,4)$ contains two black and two white sub-pixels, which makes a single share appear with a uniform contrast so as not to reveal the secret.

3.2 Algorithm

Let matrix $B_j^0, j=2,3,4$ represent the basis matrix for encoding a white pixel of the original image, and $B_j^1, j=2,3,4$ represent the basis matrix for encoding a black pixel of the original image. The collection of encoding matrices C_j^0 and C_j^1 for encoding white and black pixels, respectively, is all of the matrices obtained by permuting the columns of B_j^0 and B_j^1. To produce a 2x2 sub-pixel block of two black and two white pixels in each of *n* shares, the

encoding procedure of secret image is demonstrated as follows.

Step 1: input a halftone image *S*.

Step 2: examine the number *n* of shares that the image *S* will be encoded into; if *n*=2 the basis matrix $B_2^i, i = 0,1$ is chosen; if *n*=3 the basis matrix $B_3^i, i = 0,1$ is chosen; otherwise, the basis matrix $B_4^i, i = 0,1$ is chosen for all *n* (*n* $\geqq$ 4);

Step 3: fetch a pixel *p*, not processed yet, from *S* according to the scanning order, and proceeds one of the following sub-steps:

3.1) if *p* is white, randomly choose a matrix from the encoding matrices C_j^0 and use it to encode *p* on all *n* shares.

3.2) if *p* is black, randomly choose a matrix from the encoding matrices C_j^1 and randomly choose one share from {1,2,…,*n*} to encode *p*, if $n > 6$, randomly choose one row of the encoding matrices and use it to encode all remaining (*n*-6) un-chosen shares.

Step 4: repeat Step3 until all of the pixels in *S* are processed.

Step 5: output *n* shares.

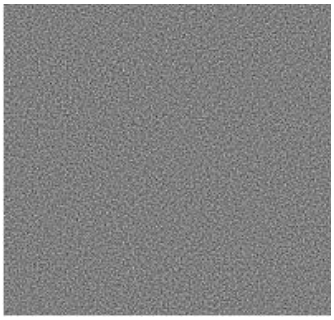
The decoding process is the same as that in conventional VSS. If the total number of shares is two, the expanded image is recovered while these two shares are stacked. The larger number of shares stacked, the clearer the reconstructed secret image becomes.

IV. Experimental results

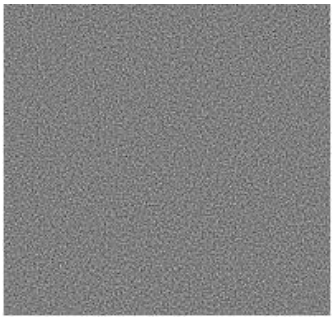
This section shows some experiments of the proposed scheme. The original secret image is a gray-level image of size 256 x 256 pixels as shown in Fig. 3a. Since the halftone image is binary, it is well suited for visual cryptography. The gray-level image is transformed into a 256 x 256 halftone image (Fig. 3b). The number *n* of shares that will be created is set to 6. The result of encoding secret image is shown in Fig. 4. Note that all the generated shares look noise-like. The proposed improved scheme does solve the security problem in Fang and Lin's scheme. The results of stacking two, three, four, five and six are shown in Fig. 5 (a)-(e) respectively. Obviously, the proposed scheme achieves the goal of progressively secure reconstruction.

Fig. 3a Original secret

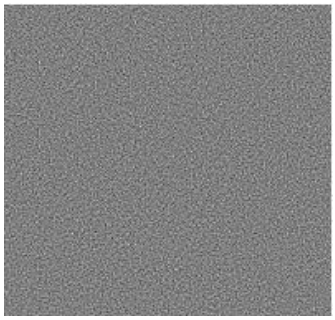
Fig. 3b Halftone secret



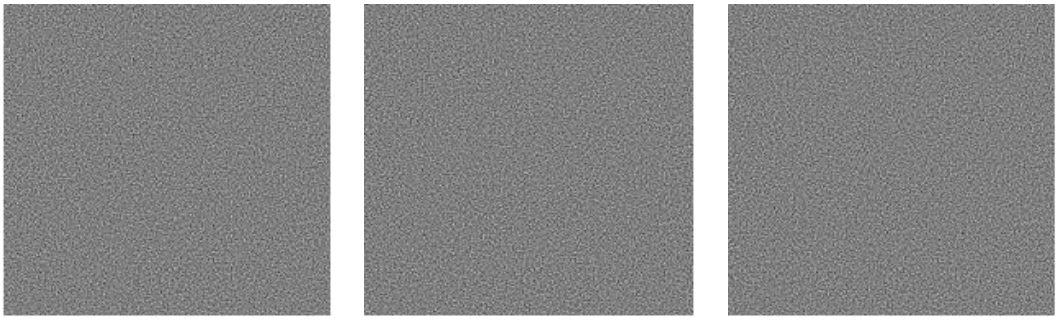
(a) share 1 ($\alpha = 0$)



(b) share 2 ($\alpha = 0$)



(c) share 3 ($\alpha = 0$)



(d) share 4 ($\alpha = 0$) (e) share 5 ($\alpha = 0$) (f) share 6 ($\alpha = 0$)

Fig. 4 the results of experiment: (a)-(f) are shares of encoded secret image (n=6)

(a) stacking two shares ($\alpha = 0.25$) (b) stacking three shares ($\alpha = 0.5$) (c) stacking four shares ($\alpha = 0.5$)

(d) stacking five shares ($\alpha = 0.5$) (e) stacking six shares ($\alpha = 0.5$)

Fig. 5 Progressively stacking (a)-(e): the results after stacking two, three, four, five, and six shares, respectively

V. Discussions

The main contribution in this paper consists of the following three points.

Cryptanalysis: As is well known, prior to withstanding significant cryptanalysis, a new cryptosystem is not considered secure. Hence, the cryptanalysis to Fang and Lin's scheme is a must. And, with secret sharing in mind, to claim security guarantee is meaningful only when each single share reveals no information about the secret. Fang and Lin's scheme is demonstrated to fail to conceal secret information on any single share. As a result, a secret image is visually recognizable on each single share such that it is not a secure progressive visual secret sharing scheme.

Superiority-inherited: Fang and Lin proposed the progressive VSS scheme, in which the secret image emerges gradually with the increasing number of stacking shares. Thus, in the proposed scheme, the superiority, i.e., the progressive disclosure of the original secret in

Fang and Lin's scheme, is kept.

Security-enhancement: The new progressive visual secret sharing method is demonstrated by redesigning basis matrices satisfying the security requirement for encoding the secret image. The experimental results tell the story that any single share looks noise-like and the disclosed secret is in a progressive way.

Inspecting the basis matrix construction of Fang and Lin's method, we illustrate that the probability of the row with two "1"s in matrix B^1 is much more than the probability of the row with two "1"s in matrix B^0. As a result, the outline of secret image is visually recognizable on each single share, causing the security problem in which each share reveals information about the secret image. In order to enhance the security, we redesign three sets of secure basis matrices, where any single row contains two "1"s and two "0"s, which makes a single share appear with a uniform contrast so as not to reveal the secret.

Carry on the demonstration of security analyses and superiority, it's worthwhile to highlight the difference and advantages of the proposed scheme compared with the related work by the description in Table 2.

Table 2. Comparison between the related schemes and the proposed schemes

	method	expansion	Security	Progressive
[12]	VC	Yes	Yes	No
[14]	RG	No	Yes	No
[35]	PVSS	No	No	Yes
Proposed	PVSS	No	Yes	Yes

Thus, the proposed scheme achieves the essential requirement of security and is a secure progressive VSS scheme.

VI. Conclusion

Visual secret sharing (VSS) is a secret sharing scheme for image data, utilizing the human visual system to decrypt the secret image by superimposing encrypted images without any computation and knowledge of cryptography. The essential requirement of a secret sharing method is to meet the security, i.e. each single share must not reveal any information about the secret image. Although Fang and Lin's scheme has been shown the superiority in terms of the progressive disclosure of the original secret, it potentially suffers from the security problem such that a share image can even reveal some information about the secret. Except for demonstrating the potential security weakness, by redesigning basis matrices to satisfy the security requirement for encoding the secret image, the proposed scheme achieves the requirement of security and is a completely progressive VSS scheme.

References

[1] Shamir, A., "How to share a secret," Communications of the ACM, Vol. 22, Issue 11, pp. 612-613, 1979.

[2] Thien, C. C., Lin, J. C., "Secret image sharing," Computers & Graphics, Vol. 26, No. 5, pp. 765-770, 2002.

[3] Ulutas, G., Ulutas, M., Nabiyev, V., "Secret image sharing scheme with adaptive authentication strength," Pattern Recognition Letters, Vol. 34, Issue 3, pp. 283-291, 2013.

[4] Chang, C. C., Chen, Y. H., Wang, H. C., " Meaningful secret sharing technique with authentication and remedy abilities," Information Sciences, Vol. 181, Issue 14, pp. 3073-3084, 2011.

[5] Guo, C., Chang, C. C., Qin, C., "A hierarchical threshold secret image sharing," Pattern Recognition Letters, Vol. 33, Issue 1, pp. 83-91, 2012.

[6] Li, P., Yang, C.N., Wu, C.C., Kong, Q., and Ma, Y., "Essential secret image sharing scheme with different importance of shadows," Journal of Visual Communication and Image Representation, Vol. 24, pp. 1106-1114, 2013.

[7] Wang, D., Zhang, L., Ma, N., Li, X., "Two secret sharing schemes based on Boolean operations," Pattern Recognition, Vol. 40, No. 10, pp. 2776-2785, 2007.

[8] Chen, T. H., and Wu, C. S., "Efficient multi-secret image sharing based on Boolean operations," Signal Processing, Vol. 91, No. 1, pp. 90–97, 2011.

[9] Chen, C. C., and Wu, W. J., "A secure Boolean-based multi-secret image sharing scheme," Journal of Systems and Soft-ware, Vol. 92, pp. 107–114, 2014.
[10] Chen, C. C., Wu, W. J., and Chen, J. L., "Highly efficient and secure multi-secret image sharing scheme," Multimedia Tools and Applications, Vol. 75, Issue 12, pp. 7113-7128, 2016.
[11] Yang, C. N., Chen, C., H., and Cai, S. R., "Enhanced Boolean-based multi secret image sharing scheme," Journal of Systems and Software, Vol. 116, pp. 22-34, 2016.
[12] Naor, M., and Shamir, A., "Visual cryptography," in Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, Vol. 950, pp. 1-12, 1995.
[13] Zhou, Z., Arce, G. R, and Crescenzo, G. D., "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, Issue 8, pp. 2441-2453, 2006.
[14] Chen, T. H., and Tsao, K. H., "User-Friendly Random-Grid-Based Visual Secret Sharing," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, Issue 11, pp. 1693-703, 2011.
[15] Shyu, S. J., "XOR-based Visual Cryptographic Schemes with Monotonously Increasing and Flawless Reconstruction Properties," IEEE Transactions on Circuits and Systems for Video Technology, 2017.
[16] Wu, H. C., Chang, C. C., "Sharing visual multi-secrets using circle shares," Computer Standards & Interfaces, Vol. 28, Issue 1, pp. 123-135, 2005.
[17] Chen, J., Chen, T. S., Hsu, H. C., and Chen, H. W., "New visual cryptography system based on circular shadow image and fixed angle segmentation," Journal of Electronic Imaging, Vol. 14, Issue 3, pp. 0330181-0330185, 2005.
[18] Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., Chen, K., "Sharing multiple secrets in visual cryptography," Pattern Recognition, Vol. 40, Issue 12, pp. 3633–3651, 2007.
[19] Kafri, O., and Keren, E., "Encryption of pictures and shaped by random grids," Optics Letter, Vol. 12, Issue 6, pp. 377-379, 1987.
[20] Chen, T. H., and Tsao, K. H., "Visual secret sharing by random grids revisited," Pattern Recognition, Vol. 42, Issue 9, pp. 2203-2217, 2009.
[21] Chen, T. H., and Tsao, K. H., "Threshold visual secret sharing by random grids," Journal of Systems and Software, Vol. 84, Issue 7, pp. 1197-1208, 2011.
[22] Shyu, S. J., "Image encryption by random grids," Pattern Recognition, Vol. 40, Issue 3, pp. 1014 - 1031, 2007.
[23] Lin, S. J. Lin, C., "VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," Pattern Recognition, Vol. 40, Issue 12, pp. 3652 - 3666, 2007.
[24] Yang, C. N., and Ciou, C. B., "Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability," Image and Vision Computing, Vol. 28, Issue 12, pp. 1600 - 1610, 2010.
[25] Li, P., Ma, P. J., Su, X. H., and C. N. Yang, "Improvements of a two-in-one image secret sharing scheme based on gray mixing model," Journal of Visual Communication and Image Representation, Vol. 23, Issue 3, pp. 441 - 453, 2012.
[26] Chen, T. H., Lin, K. S., and Lin, C. H., "On the design of a two-decoding-option image secret sharing scheme," Multimedia Tools and Applications, 2018.
[27] Horng, G. B., Chen, T. H., and Tsai, D. S., "Cheating in Visual Cryptography," Designs, Codes and Cryptography, Vol. 38, Number 2, pp. 219-236, 2006.
[28] Prisco, R. D., and Santis, A.D., "Cheating Immune (2,n)-Threshold Visual Secret Sharing Scheme," Security and Cryptography for Networks, Lecture Notes in Computer Science, 4116, 2006.
[29] Tsai, D. S., Chen, T. H., and Horng, G., "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," Pattern Recognition, Vol. 40, Issue 8, pp. 2356-2366, 2007.
[30] Tsai, D. S., and Horng, G., "Cheating in Visual Cryptography Revisited," Proceedings of 17th Information Security Conference, pp. 769-771, 2007.
[31] Hu, C. M., and Tzeng, W. G., "Cheating Prevention in Visual Cryptography," IEEE

Transactions on Image Processing, Vol. 16, pp. 36-45, 2007.
[32] Chen, C. C., Chang, T. H., and Liu, L. J., "Preventing cheating in computational visual cryptography," Fundamental Information, Vol. 92, pp. 27-42, 2009.
[33] Lin, C. H., Wu, Y. T, Tsao, K. H., Lin, K. S., and Chen, T. H., "Multi-factor Cheating Prevention in Visual Secret Sharing by Hybrid Codebooks," Journal of Visual Communication and Image Representation, Vol. 25, pp. 1543–1557, 2014.
[34] Lee, Y. S., and Chen, T. H., "Insight into collusion attacks in random-grid-based visual secret sharing", Signal Processing, Vol. 92, No. 3, pp. 727-736, 2012.
[35] Fang, W. P., and Lin J. C., "Progressive viewing and sharing of sensitive images," Pattern Recognition and Image Analysis, Vol. 16, No. 4, pp. 638-642, 2006.
[36] Jin, D., Yan, W., and Kankanhalli, M. S., "Progressive color visual cryptography," Journal of Electronic Imaging, Vol.14, No. 3, pp. 033019-1 – 033019-13, 2005
[37] Hou, Y. C., Quan, Z. Y., Tsai, C. F., and Tseng, A.Y., "Block-based progressive visual Secret sharing," Information Sciences, Vol. 233, pp. 290-304, 2013.
[38] Y. C. Hou,, and Quan, Z. Y., "Progressive visual cryptography with unexpanded shares, "IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, pp. 1760-1764, 2011.
[39] Chen, G. , Wang, C., Yan, X. , and Li, P. , "Progressive visual secret sharing with multiple decryptions and unexpanded shares," Lecture Notes in Computer Science Vol. 9023, pp 376-386, 2015.
[40] Shivani, S., and Agarwal, S., "Novel basis matrix creation and preprocessing algorithms for friendly progressive visual secret sharing with space-efficient shares," Multimedia Tools and Applications, s11042-016-3484-1, pp. 1-34, 2016.
[41] Shivani, S., and Agarwal, S., "Progressive visual cryptography with unexpanded meaningful shares," ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 12, No.4, Article 50, 2016.