

A Novel Ideal Contrast Visual Secret Sharing Scheme with Reversing

Haibo Zhang

¹College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang, 150001, China

²Wuhan Digital Engineering Institute, Wuhan, Hubei, 430074, China

Email: zhanghb412@yahoo.com.cn

Xiaofei Wang and Youpeng Huang

¹College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang, 150001, China

²Wuhan Digital Engineering Institute, Wuhan, Hubei, 430074, China

Abstract—In visual secret sharing (VSS) schemes, a secret image can be visually revealed from overlapping shadow images without additional computations. However, the contrast of reconstructed image is much lost. Employing reversing operation to reverse black and white pixels as well as increasing encoding runs is an effective way to improve the contrast. A novel VSS scheme with reversing is presented in this paper. It achieves really ideal contrast within only $\lceil m/h \rceil$ encoding runs (where m and h are the number of the total columns and the number of the whole-white columns in the basis matrix to encode white pixels, respectively) and no pixel expansion occurs. It encodes the secret image block by block. A block consists of m pixels, which means that m pixels together join into each encoding step. It is suitable for all access structures and can be applied to encrypt black-white, gray-scale and chromatic images. The experimental results, analyses and comparisons show that the proposed scheme is optimal among those schemes with reversing in encoding runs, pixel expansion, complexity, system capacity and encoding efficiency.

Index Terms—Visual secret sharing (VSS), reversing, ideal contrast

I. INTRODUCTION

In 1994, Naor and Shamir [1] first showed a novel secret sharing scheme called visual cryptography which differs exceedingly from the traditional cryptography. It divides a black-white image into n shares that are also called shadows. Among those shares, any k ($\leq n$) or shares more than k are stacked and then a discernable image appears; otherwise any shares less than k together can reveal nothing about the original secret.

The advantages of this visual secret sharing (VSS) scheme are very clear in that those complex computations needed in traditional cryptography are redundant and the decryption even doesn't need any knowledge of cryptography or any help with computer, it only depends on the human visual system. Today we are accustomed to referring the Naor-Shamir scheme as the traditional VSS scheme. After its appearance, many related researches and some extended VSS schemes have come forth.

Among the concerned problems in VSS schemes, how to enhance the contrast of the reconstructed image stands a remarkable position [2, 3, 4, and 5]. For our visual system, the higher the contrast is, the clearer the stacked image is. Recently, an effective measure to enhance the contrast is emerging. The main idea of this way is to employ the reversing operation of most copy machines and to increase the encoding runs [6, 7, 8, and 9].

By revering operation, Viet and Kurosawa [6] first designed a VSS scheme based on the traditional VSS scheme. But the reconstructed image by this scheme can only obtain an almost ideal contrast. To get a really ideal contrast, it must employ the traditional VSS scheme for infinite runs. However, the more the runs are, the more the shadows are. Therefore, how to cut down the encoding runs in such schemes is a very important issue. Afterwards, Cimato et al. [7] presented another scheme with reversing that cuts the number of required runs down to m (the number of all columns of the basis matrix, also named pixel expansion). Yang et al. [8, 9] introduced shift operation as a supplementary to further cut the number of runs down to $(m - h + 1)$ where $m > h > 0$. (h is the number of the whole-white columns in the basis matrix to encode white pixels and means the whiteness of the white secret pixel in the reconstructed image.)

However, except for Cimato et al's scheme [7], the other schemes with reversing have pixel expansion m . This means that the size of each share is m times as that of the original image and results in that more storage, more transmission bandwidth and delay for the shares need to be consumed. Therefore, our proposed scheme will be non-expanded.

In addition, all the above-mentioned schemes encode the secret image pixel by pixel. That is, there is only one pixel joining each encoding process. Therefore, the encoding efficiency is inevitably low in those VSS schemes with reversing. To improve such situation, we will introduce a new encoding method which encodes the secret image block by block. A block is composed of m pixels and it means that m pixels together join into each

encoding step. So the encoding efficiency of this new method will be higher than the usual one.

Thirdly, the number of required encoding runs is one of the important parameters in those schemes with reversing. It is directly related with the whole performance of the system implementation. The least number of runs for current related works is $(m - h + 1)$; whereas, it still needs to be largely improved in practical applications. This paper also will show a contribution to such aspect.

In one word, this paper will present a novel scheme with reversing, which encodes the secret image block by block without pixel expansion and can achieve really ideal contrast within only $\lceil m/h \rceil$ runs.

The rest of this paper is organized as follows. Firstly, section 2 introduces the model of the traditional VSS scheme and reviews the previous works about the ideal contrast schemes with reversing. Subsequently, section 3 describes the proposed scheme in detail and explains the security and applicability of this scheme. At the same time, some experimental results and comparisons are shown in section 4 and 5, respectively. Finally, section 6 concludes our works and points out the direction of our future works.

II. RELATED WORKS

In this section, we first introduce the model of VSS as a preliminary knowledge. Based on this model, some schemes with reversing have been presented. They usually repeat the distribution in the VSS model for more runs and employ reversing operation during the reconstruction. Next, we review those well-known schemes with such facilities and show some simple remarks on them.

A. The Model of VSS

It is usually assumed that the secret image is composed of a collection of black and white pixels. The model of VSS consists of two phases as follows.

- *Distribution*

At this phase, the secret image is encoded pixel by pixel into n shadows and then distributed to n participants. Generally, a pixel of the original image is encoded into m black and white sub pixels of each shadow. Those sub pixels are printed in close proximity to each other, so that the human visual system averages their individual black/white contributions and a gray level forms. Usually two basis matrices, M_0 and M_1 , are required to encode the secret image. They are both $n \times m$ Boolean matrix $M = [a_{ij}]$ where $a_{ij} = 1$ if and only if the j -th sub pixel in the i -th shadow is black, otherwise $a_{ij} = 0$. When encoding a white (resp. black) pixel in the secret image, the dealer randomly permutes all the columns of M_0 (resp. M_1), and then chooses the i -th row of the permuted matrix to fill into the corresponding positions of the i -th shadow. After all pixels in the secret image are encoded, n shadows are formed. Obviously, each shadow has the size m times as that of the original image. Therefore, we call the parameter m pixel expansion.

- *Reconstruction*

At this phase, any k ($\leq n$) or shadows more than k are stacked, and then a secret image with gray level is reconstructed. The gray level is proportional to the Hamming weight of the ORed m -vector \mathbf{V} , which is usually denoted as $H(\mathbf{V})$. This gray level is interpreted by the visual system of the users as black or as white according to certain rule of contrast. Generally, in the reconstructed image, if $H(\mathbf{V}) \geq (m - l)$, the gray level is interpreted by our visual system as black, and $H(\mathbf{V}) \leq (m - h)$ as white, where $m > h > l \geq 0$ [5] and l is the number of the whole-white columns in M_1 and means the whiteness of the black secret pixel in the reconstructed image. Especially, if $l = 0$ in a VSS scheme, a black secret pixel is totally reconstructed by m black sub pixels, so we call such scheme perfect black VSS (PBVSS) scheme; otherwise we call it non-perfect black VSS (NPBVSS) scheme. Here, we introduce two notations: p_0 and p_1 denoting the whiteness rate of the white and black secret pixel in the reconstructed image, respectively. Therefore, there are $p_0 = h/m$ and $p_1 = l/m$; it is easily to know that there is $p_1 = 0$ in the PBVSS scheme.

From the model of VSS, we know without difficulty that there is a very poor contrast in the reconstructed image. The essential reason is that a pixel in the original image becomes m pixels with a gray level in the reconstructed image.

B. Viet-Kurosawa Scheme

Employing the reversing operation of copy machines, Viet and Kurosawa proposed a new scheme based on a traditional (k, n) VSS scheme to achieve an almost ideal contrast [6]. At the distribution of this scheme, a (k, n) -PBVSS scheme is independently performed for r times. Each participant gets a shadow at each run and finally each participant gets r shadows. At reconstruction, for each run any k or shadows more than k are stacked, and then a secret image T_i ($1 \leq i \leq r$) with gray level is reconstructed from the foundational (k, n) -PBVSS scheme. Subsequently, reverse each T_i , stack them, and then reverse the stacked image too. Finally, the last rebuilt image is $\overline{\overline{T_1 + T_2 + \dots + T_r}}$. After the *reversing-stacking-reversing* process, namely NOT-OR-NOT operations, the contrast is improved largely [6].

Let P_0 and P_1 denote the average whiteness rate of the white and black secret pixel after reconstruction, respectively. If $P_0 = 1$ and $P_1 = 0$ for a VSS scheme, we call it an ideal contrast VSS Scheme.

Obviously there is $P_1 = 0$ for Viet-Kurosawa scheme because this scheme is based on a PBVSS scheme. The value of P_0 after finishing r runs in Viet-Kurosawa scheme can be deduced as follows: $P_0 = 1 - (1 - p_0)^r = 1 - (1 - h/m)^r$ [6]. Because there are $0 < p_0 < 1$ in the foundational PBVSS scheme for each run, to achieve an ideal contrast (i.e., also $P_0 = 1$), the value of r needs to be infinite.

It is evident that for Viet-Kurosawa scheme, the more the runs are, the more the contrast is improved. So each participant needs to hold more shadows to achieve higher resolution of the reconstructed image. As a result, Viet-

Kurosawa Scheme is only an almost ideal contrast VSS scheme in practice. At the same time, it inherits the pixel expansion m and the pixel by pixel encoding method from the traditional VSS scheme.

C. Cimato et al's Scheme

Also by reversing operation, Cimato et al. presented a really ideal contrast VSS scheme based on (k, n) -PBVSS scheme [7]. In this scheme, an ideal contrast, namely $P_0 = 1$ and $P_1 = 0$, can be achieved within m runs. At distribution, when encoding a white (resp. black) pixel in the secret image, the dealer randomly permutes all the columns of M_0 (resp. M_1), and then picks out the j -th sub pixel in the i -th row of the permuted matrix to fill into the corresponding position of the i -th shadow. After the value of j goes from 1 to m , m runs are finished. Finally, each participant obtains m shadows. On the other hand, the reconstruction of this scheme is similar to that of Viet-Kurosawa Scheme. After the reversing-stacking-reversing process, the last rebuilt image is $\overline{T_1 + T_2 + \dots + T_m}$ with a really ideal contrast [7], i.e., $P_0 = 1$ and $P_1 = 0$.

From the encoding process of Cimato et al's scheme, we know that a secret pixel is represented by only one pixel in each shadow, that is, the size of each shadow is not expanded. However, this scheme also encodes the secret image pixel by pixel.

D. Yang et al's Scheme

Yang et al. showed a new scheme based on a traditional (k, n) -PBVSS scheme to achieve a really ideal contrast within $(m - h + 1)$ runs [8, 9]. Besides reversing, shift operation is also employed in this scheme. At distribution, a (k, n) -PBVSS scheme is performed in the first run. In the succeeding $(m - h)$ runs, every shadow produced by the last run is cyclically shifted right one sub pixel in every m sub pixels corresponding to a secret pixel and then another shadow forms. Then each participant gets a shadow at each run. Finally, each participant gets $(m - h + 1)$ shadows. Similarly, the reconstruction of this scheme is the same to that of Viet-Kurosawa scheme and finally the last rebuilt image is $\overline{T_1 + T_2 + \dots + T_{m-h+1}}$ with a really ideal contrast [8, 9], i.e. $P_0 = 1$ and $P_1 = 0$.

The main benefit of Yang et al's scheme is that the number of required encoding runs is only $(m - h + 1)$. However, this scheme still encodes the secret image pixel by pixel; additionally there is a pixel expansion m in each shadow.

III. PROPOSED SCHEME

In this section, a novel scheme based on PBVSS scheme is proposed. This scheme only employs reversing operation and achieves the really ideal contrast, i.e. $P_0 = 1$ and $P_1 = 0$, within only $\lceil m/h \rceil$ runs. The required encoding runs are quite less than what all the above-mentioned schemes need. The other advantages of this novel scheme are as follows: there is no pixel expansion and it encodes the secret image block by block. An encoding block consists of m white or black pixels. That

is, it is m pixels instead of one pixel in the secret image that are simultaneously joined into every encoding steps. So the encoding efficiency is promoted largely. The idea of encoding block by block is also called multi-pixel encoding method by Hou and Tu in [10, 11]. Similar to the traditional VSS scheme, the proposed scheme also includes two necessary phases: distribution and reconstruction. Here is the general description in detail.

A. Distribution

For the simplicity and clearness, the distribution of our proposed scheme shows the encoding procedures for white pixels and black pixels, respectively. When encoding a secret image, if the encoder meets a white or black pixel block during scanning, it invokes the responding block encoding procedure as follows.

- *Block encoding for white pixels*

Let A denote the set including the sequence-numbers of all columns of M_0 with h whiteness, i.e. $A = \{1, 2, \dots, m\}$, and H_0 denote the set including the sequence-numbers of all the whole-white (whole-zero) columns of M_0 for PBVSS scheme. Then let $H_1 = A - H_0$ representing the set including the sequence-numbers of columns with one or more black pixels (i.e., one or more "1"s). Firstly, there are $H_0 = \emptyset$ and $H_1 = A$. Note that some changes occur for the two sets H_0 and H_1 only when encoding the white pixels. In other words, during the following encoding procedure, the black pixel encoding has nothing to do with them.

When encoding a white pixel block, the dealer randomly permutes all the columns of M_0 and takes down the positions of the m continuous white pixels in the secret image as l_1, l_2, \dots, l_m . Notice that there maybe some intervals in the position numbers. If this occurs, it means that the intervals are opposite pixels and need to stay at the next block encoding. Then pick out the i -th row of the permuted matrix M_0 , denoted by $M_{0,1}$, to fill into the corresponding positions indicated by l_1, l_2, \dots, l_m of the i -th shadow. This is the first run. Now we describe the detail encoding steps for the rest runs as follows.

When the first run finishes, it is determined that $H_0 = \{i_1, i_2, \dots, i_h\}$ where $1 \leq i_1, i_2, \dots, i_h \leq m$ and $H_1 = A - H_0$. Subsequently, repeat the following step till $H_1 = \emptyset$ or $H_0 = A$:

Randomly pick out h elements, denoted by j_1, j_2, \dots, j_h , from H_1 and then exchange these chosen h columns with those h whole-white columns, i.e., i_1, i_2, \dots, i_h , within $M_{0,1}$. For example, a quite simple way is to exchange column i_1 with column j_1 , column i_2 with column j_2 and so on. So a new M_0 forms; we denote it as $M_{0,u}$ where $2 \leq u \leq \lceil m/h \rceil$. Then pick out the i -th row of $M_{0,u}$ to fill into the corresponding positions indicated by l_1, l_2, \dots, l_m of the i -th shadow for the u -th run. At the end of this run, remove j_1, j_2, \dots, j_h from H_1 and join them into H_0 .

Note that it is possible that there maybe less than h elements left in H_1 at the last run. However, it is easy to know that the above step will still work well in this case. Finally, $\lceil m/h \rceil$ runs are required to finish encoding a white pixel block.

- *Block encoding for black pixels*

For the black pixels in the secret image, it is quite simple: the encoding process for each run can be similarly implemented as what the traditional VSS scheme does. However, here we also adopt block by block encoding method and a block also consists of m continuous black pixels. For example, if the positions of the m continuous black pixels in the secret image are q_1, q_2, \dots, q_m , the dealer will pick out the i -th row of the permuted matrix M_1 to fill into the corresponding positions indicated by q_1, q_2, \dots, q_m of the i -th shadow. For each run, the matrix M_1 can be independently permuted. Obviously, it also needs to perform $\lceil m/h \rceil$ encoding runs for black pixels as what the white pixel encoding needs.

Up to now, we have finished the encoding for a block that consists of m whole white or whole black pixels. Repeat the block encoding process and hence the secret image is totally encoded. Finally each participant gets only $\lceil m/h \rceil$ shadows with the same size of the original image.

B. Reconstruction

This phase is same to the reconstruction of the above-mentioned schemes with reversing. Finally, the last rebuilt image is $\overline{T_1 + T_2 + \dots + T_{\lceil m/h \rceil}}$ with really ideal contrast, i.e., $P_0 = 1$ and $P_1 = 0$.

C. Example

To well understand the block encoding process, here take an example. Because this scheme is also based on a PBVSS scheme, there is $l = 0$ and every black pixel in the secret image is certainly rebuilt into a black one. The principle and some examples of the encoding and decoding for black pixels can be easily found in [1, 6, 7, 8, and 9] and omitted here. Now, we pay more attentions to the demonstration of the encoding and decoding for a white pixel block.

Suppose $m=5, h=2$ and the m white pixel sequence is 19, 20, 22, 25, and 26 in the secret image. Then the number of required runs is 3. For the first run, the dealer permutes M_0 and hence $M_{0,1}$ is produced; then he picks out the i -th row of $M_{0,1}$ to fill into the positions indicated by 19, 20, 22, 25, and 26 of the i -th shadow for the first run. Further suppose $M_{0,1}$ is shown in (1) and hence there are $H_0 = \{1, 3\}$ and $H_1 = \{2, 4, 5\}$. For the second run, if the dealer pick out 2 and 4 from H_1 , he should exchange the column 1 with column 2 and column 3 with column 4 within $M_{0,1}$, respectively. Then a new basis matrix, i.e. $M_{0,2}$, is formed as shown in (2). The dealer picks out the i -th row of $M_{0,2}$ to fill into the positions indicated by 19, 20, 22, 25, and 26 of the i -th shadow. Now there are $H_0 = \{1, 3, 2, 4\}$ and $H_1 = \{5\}$. For the third run, the dealer exchanges the column 1 with column 5 for $M_{0,1}$ and $M_{0,3}$ is formed as shown in (3); then he finishes the similar filling-in operations. Finally, there are $H_0 = \{1, 2, 3, 4, 5\}$ and $H_1 = \emptyset$.

$$M_{0,1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{1}$$

$$M_{0,2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \tag{2}$$

$$M_{0,3} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{3}$$

As to the pixels at the positions indicated by 21, 23, and 24 of the secret image, they must be black pixels and they will take part in the succeeding block encoding process.

Subsequently, let's learn the reconstruction process. First, we remember that the original "image" consists of $m (= 5)$ continuous white pixels at different locations. If we ignore the pixels' location information, we can denote the original "image" by a vector $S = (0, 0, 0, 0, 0)$ where "0" means white pixel. For the first run, those legal shadows are stacked and an "image" T_1 with m pixels is revealed in the following form: $T_1 = (0, x, 0, x, x)$ where "x" means either "1" or "0", which also can be obtained from (1). Similarly, the second and the third "image" are $T_2 = (x, 0, x, 0, x)$ and $T_3 = (x, x, 0, x, 0)$, respectively. After reversing operations are imposed on T_1, T_2 and T_3 , we get that $\overline{T_1} = (1, x, 1, x, x), \overline{T_2} = (x, 1, x, 1, x)$ and $\overline{T_3} = (x, x, 1, x, 1)$, respectively. Then another stacking operation further leads to that $\overline{T_1 + T_2 + T_3} = (1, 1, 1, 1, 1)$. Finally, a last reversing operation gives us the final rebuilt "image": $T = \overline{\overline{T_1 + T_2 + T_3}} = (0, 0, 0, 0, 0)$ that is absolutely same to the original "image" S .

D. Security

The following theorem shows that the proposed scheme has sufficient security.

Theorem 1. The security of the proposed scheme is equivalent to that of the traditional Naor-Shamir scheme.

Proof. From the model of VSS introduced in section 2, we learn that in the traditional Naor-Shamir scheme [1], when encoding a white (resp. black) pixel in the secret image, the dealer randomly permutes the columns of M_0 (resp. M_1). In the proposed scheme, for black pixel encoding, the same thing is done for each encoding run and hence the security of encoding for black pixels is equivalent to that of the traditional Naor-Shamir scheme.

Now let's review the encoding for white pixels. When encoding, for the first run the dealer also randomly permutes all the columns of M_0 , which means that the first encoding run is adequately secure, too. For the other

encoding runs, all the $M_{0,u}$ ($2 \leq u \leq \lceil m/h \rceil$) used to encode white pixels for different runs come from $M_{0,1}$ of which some columns are exchanged. So it is easy to know that the security of all the $M_{0,u}$ s are equivalent to the security of $M_{0,1}$. In fact, the basis matrix $M_{0,1}$ is a result from a random column-permutation of M_0 and hence the security of $M_{0,1}$ is also equivalent to that of the traditional Naor-Shamir scheme. Therefore, we can learn that the security of encoding for white pixels is equivalent to that of the traditional Naor-Shamir scheme, too.

The proof is completed.

E. Applicability

The proposed scheme has a broad applicability. It can be applied to all access structures as long as they are suitable for a PBVSS situation. For example, both a threshold structure such as (k, n) and (n, n) threshold structure and a general access structure [12] can be well implemented by the proposed scheme. The reason is that this problem only has something to do with the chosen basis matrices during the implementation and the proposed scheme pays no attention to the construction of basis matrices.

On the other hand, by introducing half-toning technology [13, 14], a gray-scale or a chromatic image can be transferred into a binary image whose bit-planes have only two states: "0" means *empty* and "1" means *non-empty*. Therefore, the proposed scheme also can work well for gray-scale and chromatic images to perfectly improve their contrast.

IV. EXPERIMENTAL RESULTS

In this section, we take a binary secret image shown in Fig. 1 for an instance. Suppose the chosen basis matrices are as follows.

$$M_0 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad (4)$$

$$M_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \quad (5)$$

It is easy to know that the foundational scheme is a $(4, 4)$ -PBVSS scheme with parameters $m = 6$, $h = 3$ and $l = 0$. Fig. 2 shows the experimental results of some typical schemes including Viet-Kurosawa scheme, Cimato et al's scheme, Yang et al's scheme and the proposed scheme.



Figure 1. A binary secret image (125×125 pixels)

It is evident that the reconstructed images by both the proposed scheme and Cimato et al's scheme have no pixel expansion; others' pixel expansions are 6. Except for Viet-Kurosawa scheme, others achieve really ideal contrast within no more than 6 runs. For the same purpose, the proposed scheme uses only 2 runs.

V. ANALYSES AND COMPARISONS

Take account of all the mentioned schemes throughout the literature, we can find out that they vary in some different cases such as pixel expansion, required runs, complexity, encoding method and so on.

A. Contrast

From the discussions and experimental results in previous sections, it is easy to know that except for Viet-Kurosawa scheme, others achieve really ideal contrast, namely $P_0 = 1$ and $P_1 = 0$, within at most m runs. It is doomed that Viet-Kurosawa scheme is an almost ideal contrast scheme in practice, which results from the fact that it requires infinite encoding runs to achieve really ideal contrast. In fact, the reason for this situation is that all the encoding runs are independent and hence there are no relationships among them.

Security and contrast are the two foundational parameters in VSS schemes [1]. Because the proposed scheme and the others throughout the literature are all based on the traditional VSS scheme, they also satisfy the conditions for security and contrast given by Naor and Shamir in [1].

B. Number of Runs

To get really ideal contrast, it is clear that the number of required runs for the proposed scheme is the least among all the above-mentioned schemes. To achieve the same purpose, the order from low to high for the number of required runs by the schemes is: the proposed scheme, Yang et al's scheme, Cimato et al's scheme and Viet-Kurosawa scheme.

The number of encoding runs is an important parameter for the VSS schemes with reversing. It is largely related to the complexity, the store capacity and the transmission bandwidth for the shares, etc. For example, for a (k, n) threshold access structure, if the encoding runs are cut down by x , it will directly lead to that the stacking and reversing operations are reduced by at least $(x * k - 1)$ and x respectively as well as to that the total shares are reduced by $(x * n)$. So the complexity, the required store capacity and bandwidth are largely cut down by the proposed scheme compared to other schemes with reversing.

C. Complexity

For most VSS schemes with reversing, the complexity mainly includes the stacking and reversing operations, namely OR and NOT operations, respectively. It is not difficult to know that for all schemes with reversing, the complexity is approximately proportional to the number of encoding runs. Furthermore, we can deduce without difficulty that if the number of encoding runs is w , the number of reversing operations is $(w + 1)$; the lower and

upper bounds for stacking operations are $(w * k - 1)$ and $(w * n - 1)$ respectively in a (k, n) threshold access structure.

D. Number of Shadows

This parameter reflects the total capacity of a VSS system. For the schemes with reversing, each participant obtains one shadow for each encoding run. So the total

number of all shadows for such VSS system is the product of the number of encoding runs and the number of participants. It is easy to know that the proposed scheme has the least system capacity for the same size of participants. Generally speaking, lower system capacity has more advantages in system security, management, distribution and so on.

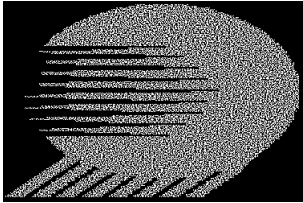

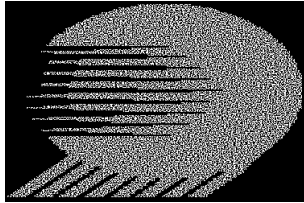

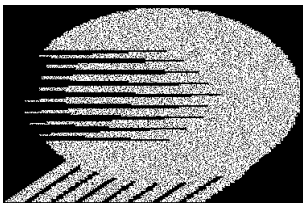

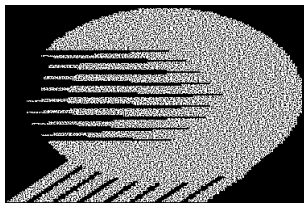

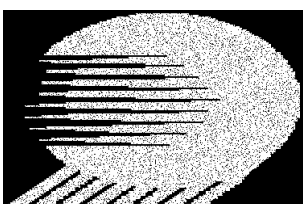

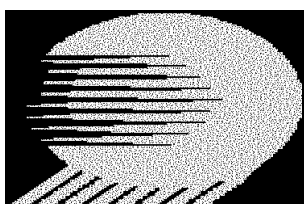

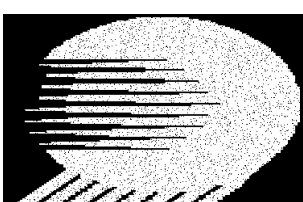



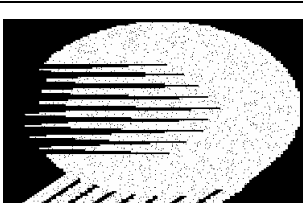



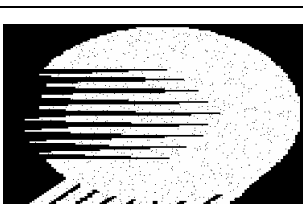



	Viet-Kurosawa scheme	Cimato et al's scheme	Yang et al's scheme	The proposed scheme
1 st run				
2 nd run				
3 rd run				
4 th run				
5 th run				
6 th run				
size	375×250 pixels	125×125 pixels	375×250 pixels	125×125 pixels

Figure 2. Experimental results of different schemes with reversing

E. Pixel Expansion

This is a common parameter for the VSS schemes with or without reversing. The pixel expansion for the traditional VSS scheme is m , which means that a pixel in the secret image becomes m sub pixels in every shadow. Among all the above-mentioned schemes with reversing, the proposed scheme and Cimato et al's scheme have no expansion. In other words, all the shadows produced by both schemes have the same size as that of the original image. But the other schemes have the pixel expansion m . It is clear that if an expansion exists in shadows, more storage, more transmission bandwidth and delay will be consumed. On account of that more runs are inevitably required in such schemes with reversing, this problem should deserve more attentions.

On the other hand, another direct result from the pixel expansion in a VSS scheme is that all the shadows and the final revealed secret image are expanded and even distorted. Even though there is a really ideal contrast in the final reconstructed image from an expansive VSS scheme with reversing, the decoded secret image is largely different from its original one and we only can recognize it by our smart visual system.

F. Encoding Method and Efficiency

The proposed scheme encodes the original image block by block. A block consists of m pixels that join in each encoding step simultaneously. Therefore, the encoding efficiency of the proposed scheme is higher than that of the other schemes throughout the literature. Currently all

the known schemes with reversing encode an image only pixel by pixel.

Conclusively, most parameters such as complexity, number of total shadows, storage and bandwidth are (approximately) proportional to the number of encoding runs. So it is very important to decrease the number of encoding runs for those schemes with reversing. In addition, the pixel expansion influences the storage and transmission bandwidth as well as the appearance of the shadows. The encoding efficiency is also an aspect that increasingly attracts more attentions. From all the above mentions, we can conclude without difficulty that the proposed scheme is optimal among those schemes with reversing. Some more accurate analysis results based on a (k, n) -PBVSS scheme are concluded and shown in Tab. 1.

VI. CONCLUSION

Researches on the ideal contrast schemes are very significant in practice by reason of that a VSS scheme with ideal contrast is very suitable for sharing secrete images including useful information of only white, only black or both. In this paper, we present a scheme with reversing based on a PBVSS scheme. It achieves really ideal contrast within only $\lceil m/h \rceil$ runs and encodes the secret image block by block without pixel expansion. It is suitable for any access structure and also can be applied to encrypt gray-scale and chromatic images. How to design a really ideal contrast VSS scheme based on NPBVSS scheme within the runs as less as possible is a challenge in our future work.

TABLE I. COMPARISON OF DIFFERENT SCHEMES BASED ON (k, n) -PBVSS SCHEME WITH REVERSING

		Viet-Kurosawa scheme	Cimato et al's scheme	Yang et al's scheme	The proposed scheme
Pixel expansion		m	1	m	1
Appearance of shadows		distorted	normal	distorted	normal
Encoding method		pixel by pixel	pixel by pixel	pixel by pixel	block by block
Number of pixels to encode for each step		1	1	1	m
Encoding efficiency		low	low	low	high
Number of required runs		r	m	$m-h+1$	$\lceil m/h \rceil$
Contrast		almost ideal (really ideal when $r \rightarrow \infty$)	really ideal	really ideal	really ideal
OR operations	at least	$r*k-1$	$m*k-1$	$(m-h+1)*k-1$	$\lceil m/h \rceil *k-1$
	at most	$r*n-1$	$m*n-1$	$(m-h+1)*n-1$	$\lceil m/h \rceil *n-1$
NOT operations		$r+1$	$m+1$	$m-h+2$	$\lceil m/h \rceil +1$
Number of total shadows		$r*n$	$m*n$	$(m-h+1)*n$	$\lceil m/h \rceil *n$
Storage required by each participant ^a		$r*m$	m	$(m-h+1)*m$	$\lceil m/h \rceil$
Bandwidth required by each participant ^a		$r*m$	m	$(m-h+1)*m$	$\lceil m/h \rceil$
System capacity ^a		$r*m*n$	$m*n$	$(m-h+1)*m*n$	$\lceil m/h \rceil *n$

a. The values are shown here using the Multiple of that of the original secret image.

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology-Eurocrypt'94*, pp. 1–12, 1995.
- [2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Computer Science*, vol. 250, no. 1–2, pp. 143–161, 2001.
- [3] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *Journal of Cryptology*, vol. 12, no. 4, pp. 261–289, 1999.
- [4] C. Kuhlmann and H. U. Simon, "Construction of visual secret sharing schemes with almost optimal contrast," *Symposium on Discrete Algorithms*, pp. 263–272, 2000.
- [5] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes and Cryptography*, vol. 25, no. 1, pp. 15–61, 2002.
- [6] D. Q. Viet and K. Kurosawa, "Almost ideal contrast visual cryptography with reversing," *Proceeding of Topics in Cryptology – CT-RSA2004 (LNCS 2964)*, pp. 353–365, 2004.
- [7] S. Cimato, A. De Santis, A. L. Ferrara, and B. Masucci, "Ideal contrast visual cryptography schemes with reversing," *Information Processing Letters*, vol. 93, no. 4, pp. 199–206, 2005.
- [8] C. N. Yang, C. C. Wang, and T. S. Chen, "Real perfect contrast visual secret sharing schemes with reversing," *Lecture Note in Computer Science*, vol. 3989, pp. 433–447, 2006.
- [9] C. N. Yang, C. C. Wang, and T. S. Chen, "Visual cryptography schemes with reversing," *The Computer Journal*, vol. 51, no. 6, pp. 710–722, 2008.
- [10] Y. C. Hou and S. F. Tu, "Visual cryptography techniques for color images without pixel expansion," *Journal of Information, Technology and Society*, no. 1, pp. 95–110, 2004.
- [11] Y. C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," *Journal of Research and Practice in Information Technology*, vol. 37, no. 2, pp. 179–191, 2005.
- [12] F. Yi, D. S. Wang, P. Luo, L. S. Huang, and Y. Q. Dai, "Multi secret image color visual cryptography schemes for general access structures," *Progress in Natural Science*, vol. 16, no. 4, pp. 431–436, 2006.
- [13] M. Mese and P. P. Vaidyanathan, "Recent advances in digital halftoning and inverse halftoning methods," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 6, pp. 790–805, 2002.
- [14] H. B. Zhang, X. F. Wang, W. H. Cao, and Y. P. Huang, "Visual cryptography for general access structure using pixel-block aware encoding," *Journal of Computers*, vol. 3, no. 12, pp. 68–75, 2008.