Real Perfect Contrast Visual Secret Sharing Schemes with Reversing

Ching-Nung Yang, Chung-Chun Wang, and Tse-Shih Chen

Department of Computer Science and Information Engineering,
National Dong Hwa University
#1, Sec. 2, Da Hsueh Rd., Hualien, Taiwan
cnyang@mail.ndhu.edu.tw

Abstract. The visual secret sharing (VSS for short) scheme is a secret image sharing scheme. A secret image is visually revealed from overlapping shadow images without additional computations. However, the contrast of reconstructed image is much lost. By means of the reversing operation (reverse black and white), Viet and Kurosawa used the traditional VSS scheme to design a VSS scheme which the secret image is almost perfectly reconstructed. Two drawbacks of the Viet-Kurosawa scheme are: (1) one can only reconstruct an almost ideal-contrast image but not an ideal-contrast image (2) the used traditional VSS scheme must be a perfect black scheme. This paper shows a real perfect contrast VSS scheme such that black and white pixels are all perfectly reconstructed within finite runs, no matter what type (perfect black or non-perfect black) of the traditional VSS scheme is.

Keywords: Visual secret sharing scheme, secret sharing scheme, ideal contrast.

1 Introduction

Naor-Shamir (k, n) VSS scheme [1] is to share the secret image into n shadow images (shadows) by dividing a pixel in the secret image to m black(B)/white(W) sub pixels in each shadow. When decrypting, any k out of n participants can reconstruct the secret image by stacking their shadows. In the reconstructed image, the 'm–h'B'h'W and 'm–l'B'l'W sub pixels are used to represent the white and black secret pixels, respectively, where h and l are the whiteness of the white and black secret pixel and $m > h > l \geq 0$. For a perfect black VSS (PBVSS) scheme (l=0), the black pixel is perfectly reconstructed but the white pixel is not. For the specific h and l, Eisen and Stinson [2] had found the minimum m to achieve the better contrast. However, since $m > h > 0$, 'm–h'B'h'W is impossibly changed into 'm'W anyway and thus we cannot reconstruct an ideal-contrast image, i.e., all black and white pixels are perfectly reconstructed.

Consider another totally different approach to improve the contrast, by more runs of stacking shadows and reversing operation (a non-cryptographic operation), Viet and Kurosawa used the PBVSS scheme to design an almost ideal VSS scheme [3]. Note that, in fact, many copy machines have the reversing operation that the black (white) color is changed into the white (black) color. For the Viet-Kurosawa scheme,

J. Zhou, M. Yung, and F. Bao (Eds.): ACNS 2006, LNCS 3989, pp. 433–447, 2006.

'm'B sub pixels are reconstructed for the black secret pixel and 'm'W sub pixels are reconstructed for almost all white secret pixels. The more runs the more 'm'W sub pixels for the white secret pixels. However, the ideal whiteness cannot be achieved even for large number of runs. So we call the Viet-Kurosawa scheme an almost contrast VSS scheme. Afterwards, Cimato et al. [4] achieved the ideal-contrast image within m finite runs. In this paper, a cyclic shift operation of sub pixels in the shadow image is used to design a real perfect contrast VSS (RPCVSS) with an ideal-contrast image when finishing $(m-h+1)$ finite runs. Moreover, for even m and $h=m/2$ the number of runs is reduced to two. Besides, the shift operation can also be applied to design a RPCVSS scheme based on the non-perfect black VSS (NPBVSS) scheme with odd '$h-l$'.

The rest of this paper is organized as follows. Section 2 reviews the previous works. In Section 3 we describe the proposed RPCVSS schemes based on the PBVSS and NPBVSS schemes, respectively. Experimental results, discussion and comparison are given in Section 4, and we draw our conclusion in Section 5.

2 Previous Works

2.1 Naor-Shamir VSS Scheme

Suppose that B_1 and B_0 are the black and white n×m basis Boolean matrices $\mathcal{A}= [a_{ij}]$, where $a_{ij} = 1$ if and only if the jth sub pixel in the ith shadow is black, otherwise $a_{ij}=0$ for the (k, n) VSS with the pixel expansion m. C_1 and C_0 are their corresponding black and white sets including all matrices obtained by permuting the columns of B_1 and B_0. The dealer randomly chooses one row of the matrix in the set C_1 (resp. C_0) to a relative shadow for sharing a black (resp. white) pixel. The chosen matrix defines the gray level of the m sub pixels in the reconstructed image.

When any k or more shadows are stacked, we view a reconstructed image whose black sub pixels are represented by the Boolean 'OR' of the corresponding rows in $\mathcal{A}$. The gray level of this reconstructed image is proportional to the Hamming weight of the ORed m-vector V. If $H(V) \geq (m-l)$, this gray level is interpreted by the user's visual system as black, and if $H(V) \leq (m-h)$, the result is interpreted as white. For example, in a (2, 2) VSS scheme, let black and white matrices be $B_1=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, $B_0=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$ and then their corresponding sets are $C_1=\left\{\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right\}$, $C_0=\left\{\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}\right\}$. For sharing a black secret pixel in the recovered image, the dealer may randomly choose the first matrix or second matrix in the black set C_1. Suppose choosing the first matrix $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, we then use 1W1B in the first shadow and 1B1W in the second shadow. The stacked result of the black secret pixel is 2B, but otherwise it is observed that the stacked result of white secret pixel is 1B1W or 1W1B. Therefore, we can view the recovered secret due to the different contrast, while we cannot get any information from any one shadow because every pixel is represented as 1B1W or 1W1B sub pixels in shadows.

Formal contrast and security conditions for (k, n) VSS schemes are shown below [1]:

(1) Contrast condition:
For any r ($\geq k$) shadows, $s_{i_1},\ldots,s_{i_r}$, the ORed V of rows $i_1, i_2, \ldots, i_r$ of matrices in C_1 (resp. C_0) satisfies $H(V) \geq (m-l)$ (resp. $H(V) \leq (m-h)$).
(2) Security condition:
For any r ($<k$) shadows, $s_{i_1},\ldots,s_{i_r}$, the two collections of $r\times m$ matrices obtained by restricting each $n\times m$ matrices in C_1 and C_0 to rows $i_1, i_2, \ldots, i_r$ are not visual in the sense that they contain the same matrices with the same frequencies.

For l=0, we call a VSS scheme the PBVSS scheme because the black secret pixel is all reconstructed by m black sub pixels; otherwise we call it the NPBVSS scheme. In this paper, we use (k, n, h, l, m)-VSS scheme to denote a (k, n) VSS scheme with the whiteness h, l and the pixel expansion m. Example 1 shows (k, n, h, l, m)-PBVSS and (k, n, h, l, m)-NPBVSS schemes, respectively.

Example 1. For a (2, 2, 1, 0, 2)-PBVSS scheme with the black and white matrices $B_1=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ and $B_0=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$, the black secret pixel is represented as 2B sub pixels and the white pixel is 1B1W sub pixels in the reconstructed image. For a (2, 3, 2, 1, 3)-NPBVSS with $B_1=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$ and $B_0=\begin{bmatrix}1 & 0 & 0\\ 1 & 0 & 0\\ 1 & 0 & 0\end{bmatrix}$, the black secret pixel is 2B1W sub pixels and the white secret pixel is 1B2W sub pixels in the reconstructed image. Table 1 shows the diagrammatic representation for the stacked results of (2, 2, 1, 0, 2)-PBVSS scheme and the (2, 3, 2, 1, 3)-NPBVSS scheme. The whiteness percentage P_W means the whiteness percentage in all the white (or black) secret pixels for a reconstructed image. □

Table 1. The (2, 2, 1, 0, 2)-PBVSS scheme and the (2, 3, 2, 1, 3)-NPBVSS scheme

(k, n, h, l, m)-VSS schemes	Secret pixel	Probability	Reconstructed pixel	Whiteness percentage P_W
(2, 2, 1, 0, 2)-PBVSS scheme	□	1/2	□■	50%
		1/2	■□	
	■	1/2	■■	0%
		1/2	■■	
(2, 3, 2, 1, 3)-NPBVSS scheme	□	1/3	□□■	67%
		1/3	□■□	
		1/3	■□□	
	■	1/3	■■□	33%
		1/3	■□■	
		1/3	□■■	

2.2 Almost Ideal VSS Scheme: The Viet-Kurosawa Scheme

By using the reversing operation of copy machines, Viet-Kurosawa scheme shows a novel idea to achieve the perfect reconstruction of white pixel by using a (k, n)-PBVSS scheme [3]. The sharing phase includes two steps: (1) distribution (2) reconstruction. A brief description for the Viet-Kurosawa scheme is shown as follow.

Distribution phase
Perform a (k, n)-PBVSS scheme R times independently. These n shadows, $s_1^i,\ldots,s_n^i$, are used for the ith run, $i\in[1, R]$. Finally, Participant j gets R shadows $s_j^1,\ldots,s_j^R$.

Reconstruction phase
For ith run, we first reconstruct the image T_i by stacking any k ore more shadows, $T_i = s_{i_1}^i+\ldots+s_{i_r}^i$, $i\in[1, R]$. Note that each T_i is a reconstructed image of the PBVSS scheme. To improve the contrast we perform the following operations: reverse the reconstructed image in each round and then stack them; finally reverse the stacked image again. The reconstructed image of the ith run is $\overline{\overline{T}_1+\overline{T}_2+\ldots+\overline{T}_i}$; for example, the final run is $\overline{\overline{T}_1+\overline{T}_2+\ldots+\overline{T}_R}$.

Doing more runs, the whiteness of the white secret pixel is increased. Table 2 shows a (2, 2, 1, 0, 2)-PBVSS scheme with reversing for two runs. The whiteness percentage of the white secret pixel is increased from 50% to 75 % and the whiteness percentage of the black secret pixel is still 0 %. The average P_W of the white secret pixel when finishing R runs is $\left(1-(1-h/m)^R\right)$ [3]. To achieve the percentage $\left(1-(1-h/m)^R\right)\approx 100\%$ (ideal contrast), the R value needs to be infinite. So there is a loss of resolution for the Viet-Kurosawa scheme within finite runs. Also, for the higher resolution, a participant needs to store more shadows.

Table 2. An almost ideal contrast VSS scheme based on (2, 2, 1, 0, 2)-PBVSS scheme for two runs

Secret Pixel	Probability	T_1	T_2	$U=\overline{T}_1+\overline{T}_2$	$\overline{U}$	Whiteness percentage P_W
□	1/4	□■	□■	■□	□■	75%
	1/4	■□	■□	□■	■□	
	1/4	■□	□■	■■	□□	
	1/4	□■	■□	■■	□□	
■	1	■■	■■	□□	■■	0%

2.3 Ideal VSS Scheme: Cimato et al's Scheme

Cimato et al. [4] used reversing operation to propose an ideal contrast VSS scheme based on (n, k, h, l, m)-PBVSS scheme which the whiteness percentage of the white secret pixel P_W=100% (ideal contrast) can be achieved within m finite runs. Meantime the shadow size is not expanded. The sharing process is described below.

Distribution phase
When sharing a black (resp. white) pixel, the dealer randomly chooses one matrix form C_1 (resp. C_0) and delivers a pixel p_i, where (p_1, …, p_m) is located in ith row of matrix, to the s_j^i shadow for participant j. Finally, participant j gets m shadows $s_j^1,\ldots,s_j^m$ for m runs. Note that a secret pixel is represented by a pixel in the shadow, and hence the shadow size is same to the original image.

Reconstruction phase
For ith run, we first reconstruct the image α_i by stacking any k ore more shadows, $\alpha_i = s_{i_1}^i + \ldots + s_{i_r}^i$, $i\in[1, m]$. Using reversing and stacking to get $\beta = \overline{\alpha_1} + \overline{\alpha_2} + \ldots + \overline{\alpha_i}$, the reconstructed image is then obtained by reversing again, i.e, $\overline{\beta}$.

Table 3 shows the whiteness percentage of the white secret pixel can be improved to 100% within two runs. It is evident that the whiteness percentage of the black secret pixel is still 0% because we use the PBVSS scheme. So it is a really ideal contrast VSS scheme when finishing m runs.

Table 3. The ideal contrast VSS scheme based on (2, 2, 1, 0, 2)-PBVSS scheme for two runs

Secret Pixel	Probability	α_1	α_2	$\beta = \overline{\alpha_1} + \overline{\alpha_2}$	$\overline{\beta}$	Whiteness percentage P_W
□	1/2	□	■	■	□	100%
	1/2	■	□	■	□	
■	1	■	■	□	■	0%

3 The Proposed RPCVSS Schemes

In this section, two RPVCC schemes based on PBVSS scheme and one RPVCC scheme based on NPBVSS scheme are proposed. All schemes achieve the real perfect contrast, i.e., the whiteness percentage of white and black secret pixels are 100% and 0%, respectively, within finite runs.

3.1 RPCVSS Scheme Based on Perfect Black VSS Scheme

For the description of the construction, we first define a matrix operation $\Gamma(\cdot)$ that cyclically shifts right one sub pixel in every m sub pixels (for a secret pixel) in the shadow image.

Let the shadow image s be represented as a matrix $[s_{ijk}]$ as follows, where s_{ijk} means the secret pixel s_{ij} in the (W×H)-pixel secret image replaced by m sub pixels $(s_{ij1}, s_{ij2}, \ldots, s_{ijm})$, where $i\in[1, H]$, $j\in[1, W]$, $k\in[1, m]$. Then the matrix operation $\Gamma\left([s_{ijk}]\right) = [\gamma(s_{ijk})]$, where $\gamma(s_{ij1}, s_{ij2}, \ldots, s_{ijm}) = (s_{ijm}, s_{ij1}, \ldots, s_{ijm-1})$.

Method A:
Distribution phase
Perform a (n, k, h, l=0, m)-PBVSS scheme to generate n shadows, $s_1^1,\ldots,s_n^1$ to n participants, for the first run. For ith run, Participant j gets the shadows $s_j^i=\Gamma(s_j^{i-1})$, $i\in[2,(m-h+1)]$. Finally a participant has (m–h+1) shadows.

Reconstruction phase
Same to the Viet-Kurosawa scheme.

Theorem 1. The whiteness percentages P_W for the white and black secret pixels of the RPCVSS scheme based on Method A are 100% and 0%, respectively, when finishing (m–h+1) runs.

Proof. here are 'm–h'B'h'W sub pixels for the white secret pixel. The maximum interval between two "0" is (m–h) an thus when shifting right one bit (m–h) times, there is at least a white sub pixel in a same position in a white secret pixel block for these T_i images, i=∈[1, (m–h+1)]. Reversing and stacking will result in all black sub pixels and finally reverse again to get the pure white color. It is evident that the whiteness percentage of the black secret pixel is P_W=0% because we use the PBVSS scheme and other shadows are obtained from the shadows in the first run by shifting operation. The proof is completed. □

For even m and h=m/2, the number of runs can be substantially reduced to two. From observation of the proof for Theorem 1, it is evident that if only assure a same position of at least a white sub pixel, we can reconstruct the ideal-contrast image using the same decoding way.

Method B:
Distribution phase
Perform a (n, k, h=m/2, 0, m: even)-PBVSS scheme to generate n shadows, $s_1^1,\ldots,s_n^1$ to n participants, for the first run. For the second run, Participant j gets the shadows $s_j^2=\overline{s_j^1}$, $j\in[1,\ n]$. Finally a participant has only two shadows.

Reconstruction phase
Same to the Viet-Kurosawa scheme.

Theorem 2. The whiteness percentages P_W for the white and black secret pixels of the RPCVSS scheme based on Method B are 100% and 0%, respectively, when finishing two runs.

Proof. Because the two shadows for these two runs are complemented, the sub pixel in a in a white secret pixel block for T_1 and T_2 are mutually complemented. So, reversing and stacking will result in all black sub pixels in the white secret pixel and finally reverse again to get the pure white color. Same as the poof in Theorem 1, the whiteness percentage of the black secret pixel is P_W=0%. The proof is completed. □

Using the (2, 2, 1, 0, 2)-PBVSS scheme, we can design a RPCVSS scheme (Method A) with two runs (since (*m*–*h*+1)= 2). Table 4 shows that our RPCVSS scheme has the whiteness percentage of the white (resp. black) secret pixel P_W=100% (resp. 0%) when finishing two runs.

Table 4. The RPCVSS scheme based on (2, 2, 1, 0, 2)-PBVSS scheme for two runs

Secret Pixel	Probability	T_1	T_2	$U=\overline{T_1}+\overline{T_2}$	$\overline{U}$	Percentage of whiteness P_W
□	1/2	■□	□■	■■	□□	100%
	1/2	□■	■□	■■	□□	
■	1	■■	■■	□□	■■	0%

3.2 RPCVSS Scheme Based on Non-perfect Black VSS Scheme

Both the almost ideal VSS scheme and the ideal VSS scheme [3, 4] are based on PBVSS scheme. The shift operation used in Section 3.1 can also be used to design a RPCVSS scheme based on the NPBVSS scheme. However, the difference of whiteness '*h*–*l*' needs to be odd number and the exclusive or (XOR) operation is required for decoding.

Generally, copy machines support reversing operation (i.e. NOT) and OR can be done by stacking shadows. By Boolean reduction, the XOR(⊕) operation can be reduced as $A\oplus B=\overline{(A+\overline{B})}+\overline{(\overline{A}+B)}$. Thus XOR operation can be implemented by four NOTs and three ORs.

Method C:
Distribution phase

Perform a (*n*, *k*, *h*, *l*≠0, *m*)-NPBVSS scheme, where '*h*–*l*' is odd number, to generate *n* shadows, $s_1^1,\ldots,s_n^1$, for the first run. For *i*th run, Participant *j* gets the shadows $s_j^i=\Gamma(s_j^{i-1})$, $i\in[2,\ m]$. Finally a participant has *m* shadows.

Reconstruction phase

Reconstruct T_i image for *i*-th run, *i*∈[1, *m*]. Use XOR operation to reconstruct $U'=T_1\oplus\ldots\oplus T_m$. If '*m*–*h*' is even (i.e., '*m*–*l*' is odd) then the reconstructed image is U'; otherwise the reconstructed image is $\overline{U'}$.

Theorem 3. The whiteness percentages P_W for the whie and black secret pixels of the RPCVSS scheme based on Method C are 100% and 0%, respectively, when finishing *m* runs.

Proof. There are '*m*–*h*'B'*h*'W (resp. '*m*–*l*'B'*l*'W) sub pixels for the white (resp. black) secret pixel. When shifting right one bit *m* times, there is *m*–*h* (resp. *m*–*l*) black sub pixels for the white (resp. black) secret pixels in U'. Suppose '*m*–*h*' is even (resp. odd), then XORing will result in all white sub pixels for the white pixels in U' (resp. $\overline{U'}$). Thus, P_W for the white secret pixel is 100%. On the other hand, even (resp. odd) '*m–h*' means odd (resp. even) '*m–l*' since '*h–l*' is odd. It is evident that XORing operation will result in all black sub pixels for the black pixels in U' (resp. $\overline{U'}$), i.e., P_W for the black secret pixel is 0%. The proof is completed. □

Example 2. Using a (2, 3, 2, 1, 3)-NPBVSS with $B_1=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$ and $B_0=\begin{bmatrix}1&0&0\\1&0&0\\1&0&0\end{bmatrix}$ to design our RPCVSS scheme (Method C), we show the patterns of black and white pixels for these three runs.

Suppose three sub pixels for the white secret pixel in the 1st-run shadow s_1^1 is (010) for Participant #1, where 1 and 0 denote black and white colors, so Participant #2 and Participant #3 also have the pattern (010) on s_2^1 and s_3^1. Then the patterns of sub pixels for other shadows s_1^2, s_1^3, s_2^2, s_2^3, s_3^2 and s_3^3 are determined from the following.

$$\text{The patter in } s_i^2 \text{ is } \gamma(\text{the pattern in } s_i^1)=\gamma(010)=(001),\ i\text{=1, 2, 3;}$$
$$\text{the patter in } s_i^3 \text{ is } \gamma(\text{the pattern in } s_i^2)=\gamma(001)=(100),\ i\text{=1, 2, 3.}$$

Suppose three sub pixels for the black secret pixel in the 1st-run shadow s_1^1 is also (010) for Participant #1, so Participant #2 and Participant #3 have the patterns (100) and (001) on s_2^1 and s_3^1, respectively. Then the patterns of sub pixels for other shadows s_1^2, s_1^3, s_2^2, s_2^3, s_3^2 and s_3^3 are determined from the following.

$$\text{The patter in } s_1^2 \text{ is } \gamma(\text{the pattern in } s_1^1)=\gamma(010)=(001);$$
$$\text{the patter in } s_1^3 \text{ is } \gamma(\text{the pattern in } s_1^2)=\gamma(001)=(100);$$
$$\text{the patter in } s_2^2 \text{ is } \gamma(\text{the pattern in } s_2^1)=\gamma(100)=(010);$$
$$\text{the patter in } s_2^3 \text{ is } \gamma(\text{the pattern in } s_2^2)=\gamma(010)=(001);$$
$$\text{the patter in } s_3^2 \text{ is } \gamma(\text{the pattern in } s_3^1)=\gamma(001)=(100);$$
$$\text{the patter in } s_3^3 \text{ is } \gamma(\text{the pattern in } s_3^2)=\gamma(100)=(010).$$

Table 5 shows that our RPCVSS scheme has the whiteness percentages of the white and black secret pixels are P_W=100% and 0%, respectively, when finishing three runs. We successfully implement a real perfect contrast VSS scheme from a NPBVSS scheme. □

Note that as the Method C uses the XOR operation. For obtaining the ideal-contrast secret image it can not be implemented just by superimposing the shadows but need using XOR operations among shadows, i.e., $U'=T_1\oplus\ldots\oplus T_m$. As the above description, one XOR can be implemented by 4 NOTs and 3 ORs. For example, to get $T_1\oplus T_2$, one needs to first superimpose separately (T_1 and $\overline{T_2}$) and ($\overline{T_1}$ and T_2). Then will have to process (T_1 and $\overline{T_2}$) (resp. $\overline{T_1}$ and T_2) to get ($\overline{T_1+\overline{T_2}}$) (resp.

$\overline{T_1 + T_2}$) and then superimpose them. So, although it does not follow the traditional VSS scheme where just superimposes shadows and no additional computation is required, it still can be implemented using the copy machine with reversing function to achieve the XORed result step by step according the above procedure. Even if we do not have the copy machine with reversing function, like the Viet-Kurosawa scheme, Method C can reconstruct the secret image by stacking the shadows directly in the same way as the traditional VSS scheme. The reason is that for the same round our shadows are just obtained from the first shadow by cyclically shifting right a creation position.

Table 5. The RPCVSS scheme based on (2, 3, 2, 1, 3)-NPBVSS scheme for three runs

Secret Pixel	Probability	T_1	T_2	T_3	$U' = T_1 \oplus T_2 \oplus T_3$	$\bar{U}'$	Whiteness percentage P_W
□	1/3	■□□	□■□	□□■	■■■	□□□	100%
	1/3	□■□	□□■	■□□	■■■	□□□	
	1/3	□□■	■□□	□■□	■■■	□□□	
■	1/3	■■□	□■■	■□■	□□□	■■■	0%
	1/3	■□■	■■□	□■■	□□□	■■■	
	1/3	□■■	■□■	■■□	□□□	■■■	

4 Experimental Results and Comparison

We show experimental results of the (2, 2, 1, 0, 2)-PBVSS scheme, the (2, 2, 2, 0, 4)-PBVSS scheme and the (2, 3, 2, 1, 3)-NPBVSS scheme among the Viet-Kurosawa scheme [3], Cimato et al's scheme [4] and our proposed RPCVSS schemes. The first twos show the case of different *h*, and the third shows the case of NPBVSS scheme. Also, discussion and comparison for these schemes are given.

4.1 Experimental Results

Fig. 1 is the original secret image (a school badge of National Dong Hwa University). Fig. 2 (a) is our RPCVSS scheme, Fig. 2(b) is the almost ideal contrast scheme (the Viet-Kurosawa scheme) and Fig. 2(c) is the ideal contrast scheme (Cimato et al's scheme) based on the (2, 2, 1, 0, 2)-PBVSS scheme. For viewing convenience, we

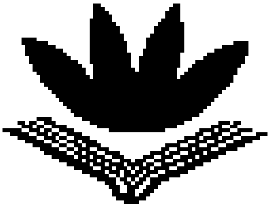


Fig. 1. The original secret image

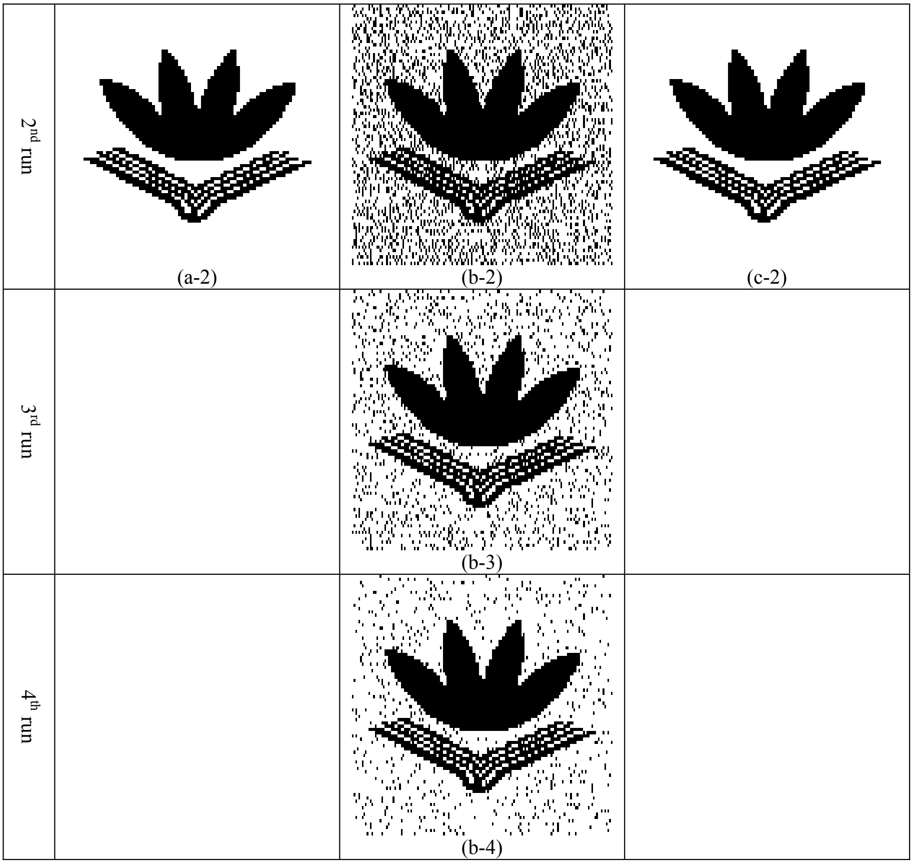


Fig. 2. Different schemes based on the (2, 2, 1, 0, 2)-PBVSS scheme (a) the proposed RPCVSS scheme (Method A) (b) the Viet-Kurosawa scheme (c) Cimato et al's scheme

arrange the reconstructed images to the same original image size without expansion. From Fig. 2(b), the reconstructed images by the Viet-Kurosawa scheme of 1, 2, 3, 4-run, it is shown that the whiteness of the white secret pixel is increased gradually. There are still noise-like random dots on the reconstructed image in Fig. 2(b-4). On the contrary, Figs. 2(a) and (c) show that the proposed scheme (Method A) and Cimato et al's scheme achieve 100% whiteness of the white secret pixel within two runs. The pixel expansion of our RPCVSS scheme is 2; however there is no pixel expansion for Cimato et al's scheme because it uses the construction nature of the probabilistic VSS schemes [5, 6].

When using (2, 2, 2, 0, 4)-PBVSS scheme, do the same experiment like Fig. 2. The results are given in Fig.3. Our scheme (Method B) still achieves 100% whiteness of the white secret pixel within two runs. According Cimato et al's construction in [4], they prepared four shadows for each participant but, in fact, only three runs are required to achieve 100% whiteness. This is due to the using of 2B2W for a white

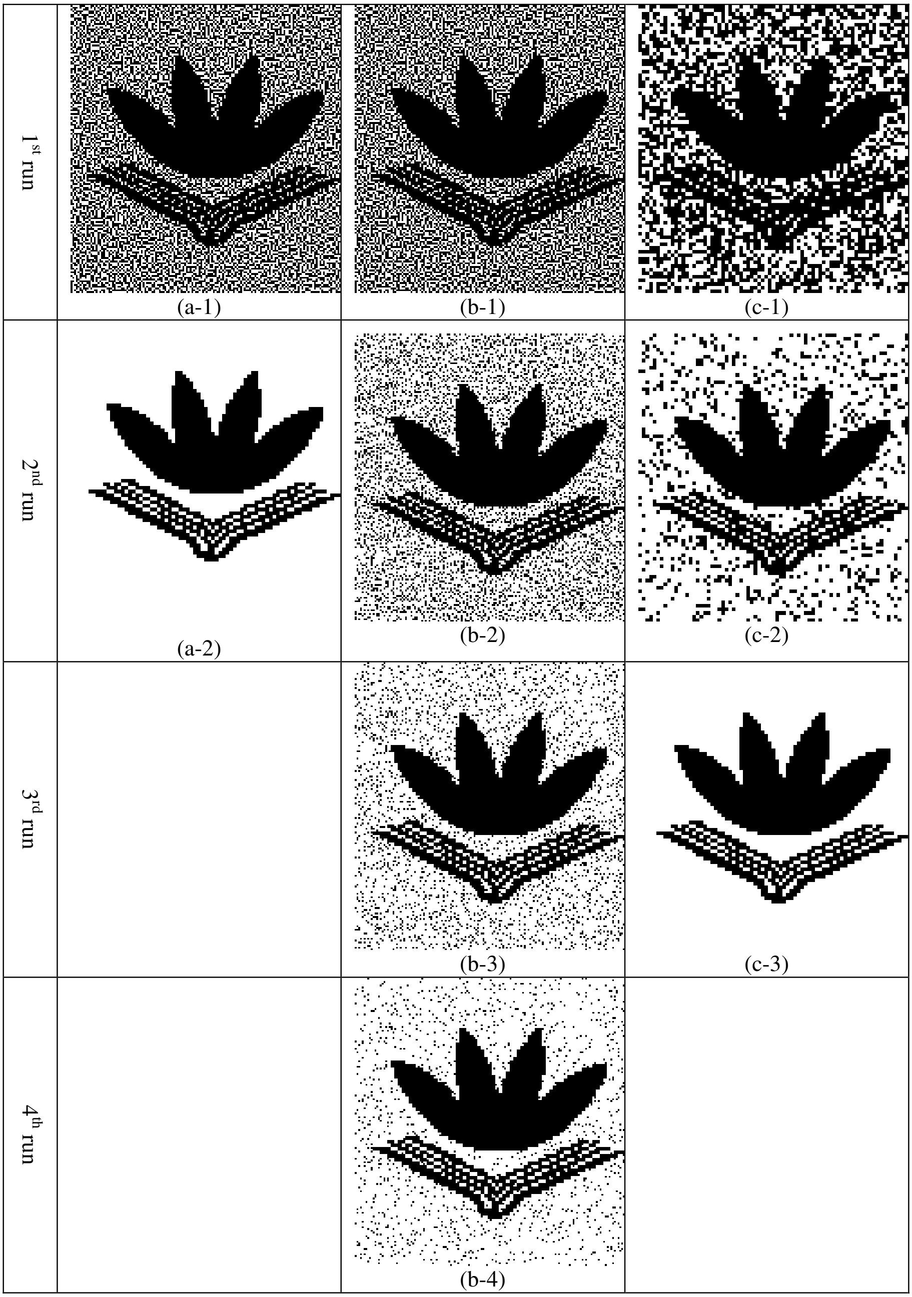
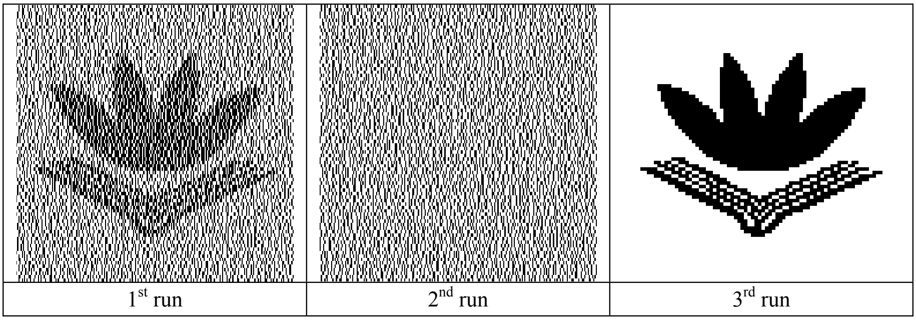


Fig. 3. Different schemes based on the (2, 2, 2, 0, 4)-PBVSS scheme (a) the proposed RPCVSS scheme (Method B) (b) the Viet-Kurosawa scheme (c) Cimato et al's scheme

secret pixel and there is at least one white sub pixel in a same position when finishing three runs. Thus, the number of runs for Cimato et al's scheme should be modified to (m−h+1). In Fig. 4, we show a RPCVSS scheme based on the (2, 3, 2, 1, 2)-NPBVSS scheme (Method C). We have the perfect whiteness of the white secret pixel and perfect blackness of the black secret pixel when finishing three runs. However, we see nothing in other runs except the first and last runs due to the XOR operation.



1st run

2nd run

3rd run

Fig. 4. The RPCVSS scheme based on the (2, 3, 2, 1, 2)-NPBVSS scheme (Method C)

4.2 Discussion and Comparison

In this section, we discuss about the security, compatibility, complexity and contrast for the R-run VSS schemes. Besides, the comparison is given for three schemes: the RPCVSS schemes, the almost ideal contrast scheme and the ideal contrast scheme.

Security: For the R-run (k, n) VSS schemes, as examples, the participants store more than one shadow for improving the contrast of the reconstructed image, e.g., the dealer needs to prepare $n\times R$ shadows, s_j^i , $i\in[1, R]$ and $j\in[1, n]$. Considering security, the first concern is that one should not get any secret information from his own shadows, $s_j^1,\ldots,s_j^R$. The Viet-Kurosawa scheme performs the VSS scheme R times independently. Cimato et al's scheme uses the concept of probabilistic scheme and delivers the elements in one row to the shadows of different runs.In the same position of m different shadows, the frequencies of black and white sub pixels are same and thus one cannot obtain any information from his own shadows. The proposed RPCVSS schemes only perform the shift operation on the first shadow to generate other shadows. Therefore, all three schemes satisfy the first security concern, i.e., there is no any mutual information among their own shadows.

The second concern is that whether stacking any k or more shadows of the different run from the different participants, the secret information should be kept secret or not. For this scenario, the leak of secret information does not affect the secrecy of secret sharing scheme. The reason is that when one discloses the shadow, in fact, he agrees to share the secret. So, at this time, if one can see the secret image it does not compromise the secrecy. Unlike the Viet-Kurosawa scheme performing the VSS scheme R times independently, Cimato et al's scheme and the RPCVSS schemes may have the secret image when stacking shadows of different runs. Considering these two schemes constructed from (2, 2, 1, 0, 2)-PBVSS scheme, our cyclic shift operation and Cimato et al's delivering elements of one row to different shadows are just right changing the black and white color in the stacking result. For example, for the RPCVSS scheme, when stacking the shadows of different runs the black and white matrices in the stacked result are $B_1' = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $B_0' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ which same to the white and black matrices $B_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ in a (2, 2, 1, 0, 2)-PBVSS scheme. Fig. 5 shows this situation. Both schemes are secure even though Figs. 5(a) and (b) reveal the secret.

Compatibility: Even if we do not have the copy machine with reversing operation, the Viet-Kurosawa scheme could reconstruct the image by stacking the shadows directly. We call the Viet-Kurosawa scheme fully compatible to the traditional VSS scheme. It is evident that the proposed RPCVSS schemes and Cimato et al's scheme also have the compatibility (see Fig. 2 ~ Fig. 4). However, in [4], another construction method based on binary secret sharing scheme and Boolean function method [7, 8] was proposed for reducing the number of shadows to $\lfloor \log(n-k+2) \rfloor + 1$ (lower bound). The scheme does not hold the compatibility. For example an ideal contrast (*k*, *k*) VSS scheme in [4] only needs one shadow and one run to achieve the ideal contrast by XORing these shadows but get nothing when stacking them directly. Although our Method C for NPBVSS scheme also uses XOR operation but we can reconstruct the image by direct stacking.

Complexity: Operations of stacking any *k* shadows equal (*k*–1) ORs. When finishing *R* runs of the Viet-Kurosawa scheme, we require *R* NOTs to reverse T_i and (*R*–1) ORs to stack them and finally a NOT to reverse the image. So, the total operations are $\left(R(k-1)+(R-1)\right)=(Rk-1)$ ORs, (*R*+1) NOTs. Instead of *R* by (*m*–*h*+1) and 2, the operations are $\left((m-h+1)k-1\right)$ ORs, (*m*–*h*+2) NOTs (Method A and Cimato et al's scheme), and (*mk*–1) ORs, 3 NOTs (Method B). For the RPCVSS scheme (Method

C) based on NPBVSS scheme, except the operations of stackind shadows, we require (*k*–1) XORs and one NOT when finishing *m* runs. So, the total operations are $\left(m(k-1)+3(m-1)\right)=(mk+2m-3)$ ORs and (4(*m*–1)+1)= (4*m*–3) NOTs. (Note: 1 XOR = 3 ORs + 4 NOTs).

Contrast: The Viet-Kurosawa scheme is an almost ideal contrast scheme but our proposed RPCVSS scheme and Cimato et al's scheme are really ideal contrast scheme. So the reconstructed images of the last two schemes are better than the first scheme. Actually, our scheme is the deterministic VSS scheme with the pixel expansion *m* and Cimato et al's scheme is the probabilistic VSS scheme with no pixel expansion. The disadvantage of the probabilistic VSS scheme is that details of the

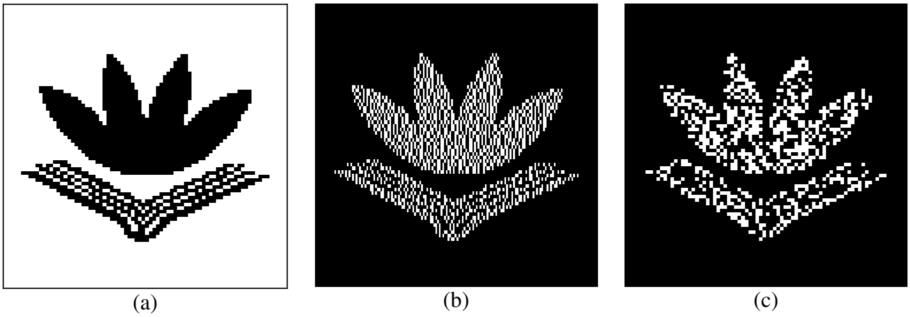


Fig. 5. Stacking $s_1^1 + s_2^2$ for the RPCVSS scheme and Cimato et al's scheme based on the (2, 2, 1, 0, 2)-PBVSS scheme (a) the original secret image: white background color (b) the RPCVSS scheme: black background color (c) Cimato et al's scheme: black background color

Table 6. Comparison of VSS schemes with reversing

		RPCVSS scheme			Viet-Kurosawa scheme	Cimato et al's scheme
		Method A	Method B	Method C		
Number of runs		$m–h$+1	2	m	R: 1→∞	$m–h$+1
Shadow expansion		m	m	m	m	1
Operation complexity	OR	($m–h$+1)k–1	2k–1	mk+2m–3	($m–h$+1)k–1	mk − 1
	NOT	$m–h$+2	3	4m–3	$m–h$+2	m+1
Compatibility		YES	YES	YES	YES	YES (or NO for XOR based scheme)
Available to NPBVSS scheme		NO	NO	YES	NO	NO
Contrast		The best among these three schemes			the random dots due to the almost ideal contrast	the loss of clarity due to th probabilistc nature

picture are not recognizable if they do not consist of enough pixels. When comparing these two schemes, our reconsructed image is better than Cimato et al's scheme. From the above description, our contrast is the best among these three schemes.

The comparison among the proposed RPCVSS schemes and the schemes in [3, 4] are summarized in Table 6. The RPCVSS schemes based on PBVSS scheme has less runs and operations than other two schemes and the RPCVSS scheme based on NPBVSS is the first R-run scheme available to the NPBVSS scheme.

5 Conclusion

We first use the cyclic shift operation of the sub pixels to design a real perfect contrast VSS scheme based on the PBVSS scheme with simple reversing operation within less finite runs. Using the same strategy and the XOR operation (also a no-cryptographic operation), we next propose the scheme based on the NPBVSS scheme. It will be interesting to further design the real perfect contrast scheme based on the NPBVSS scheme for even (h – l) by means of other simple operations.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” Advances in *Cryptology-EUROCRYPT’94*, pp.1-12, 1994.

[2] 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.

[3] D.Q. Viet and K. Kurosawa, “Almost ideal contrast visual cryptography with reversing,” in Proceeding of Topics in Cryptology─CT-RSA2004. *Lecture note in Computer Science*, vol. 2964, pp. 353-365, 2004.

[4] S. Cimato, A. De Santis, A.L. Ferrara and B. Masucci, “Ideal contrast visual cryptography schemes with reversing,” *Information Processing Letters*, vol. 93, issue 4, pp. 199-206, 2005.

[5] C.N. Yang, “New Visual Secret Sharing Schemes Using Probabilistic Method,” *Pattern Recognition Letters*, vol. 25, issue 4, pp. 481-494, 2004.

[6] R. Ito, H. Kuwakado and H. Tanaka, “Image size invariant visual cryptography,” *IEICE Trans. Fundamentals*, vol. E82-A, no. 10, pp. 2172-2177, Oct. 1999.

[7] A. De Bonis and A. De Santis, “Randomness in secret sharing and visual cryptography schemes,” *Theoretical Computer Science*, vol. 314, issue 3, pp. 351-374, 2004.

[8] P. Tuyls, H.D.L. Hollmann, J.H. Van Lint and L. Tolhuizen, “XOR-based Visual Cryptography Schemes,” *Designs, Codes and Cryptography*, vol. 37, pp. 169-186, 2005.