New Visual Secret Sharing Schemes With Non-Expansible Shadow Size Using Non-binary Sub Pixel

Ching-Nung Yang
Department of Computer Science & Information Engineering,
National Dong Hwa University,
1, Sec. 2, Da Hsueh Rd., Shou-Feng,
Hualien, Taiwan, Republic of China
TEL:886-3-8662500 Ext-22120
FAX: 886-3-8662781
E-mail: cnyang@mail.ndhu.edu.tw

Yun-Hsiang Liang and Wan-Hsiang Chou
Department of Computer Science & Information Engineering,
National Dong Hwa University,
1, Sec. 2, Da Hsueh Rd., Shou-Feng,
Hualien, Taiwan, Republic of China
TEL:886-3-8662500 Ext-22176
FAX: 886-3-8662781
E-mail: m8921011@mail.ndhu.edu.tw

Abstract

Visual secret sharing (VSS) scheme is a perfect secure method that protects a secret image by breaking it into shadow images (called shadows). Unlike other threshold schemes, VSS scheme can be easily decoded by the human visual system without the knowledge of cryptography and cryptographic computations. However, the size of shadow images (i.e., the number of columns of the black and white matrices in VSS scheme [1]), will be larger than the original image. Most recent papers about VSS schemes are dedicated to get a higher contrast or a smaller shadow size.

In this paper, the gray (non-binary) sub pixel in the proposed method is completely different from the black and white (binary) sub pixel in the conventional VSS scheme. The new definition of gray sub pixel lets the proposed VSS scheme have *non-expansible* shadow size. The term "*non-expansible*" means that the sizes of the shared secret and shadows are same.

Keywords: Secret sharing scheme, visual secret sharing scheme.

1 Introduction

The secret sharing scheme, or sometimes called threshold scheme, was first introduced by Blakley [9] and Shamir [10] independently in 1979. A threshold scheme is a method to protect a master key by breaking it to a set of participants and only qualified subsets of participants can retrieve the master key by combining their shadows. For a (k, n) threshold scheme, the master key is divided into to n different shadows, so that we can recover the master key by combining any $k(k \le n)$ shadows but k-1 or fewer shadows will get no information.

A new type of secret sharing scheme [1]-[8] called visual secret sharing (VSS) scheme, was first proposed by Naor and Shamir in 1994 [1]. The shared secret is an image (printed text, handwritten note, pictures, etc.) and the VSS scheme provides an unconditionally secure way to encode the shared secret into shadow images. The decoder is human

visual system so that we can easily recover the shared secret using the eyes of human being. For a (k, n) VSS scheme, k or more participants can get the shared secret by stacking their shadows (transparencies). In the previous construction methods for VSS schemes, we use several sub pixels in the shadow to represent a pixel in the original secret image, i.e., the size of shadow is larger than the original image. Here we define the *Pixel Expansion* = (the size of the shadow) / (the size of the secret image). For example the *Pixel Expansion* of Shamir's (2, 2), (2, n) and optimal (k, k) VSS schemes are 2, n, and 2^{k-1}.

In this paper, we will propose the new VSS schemes with non-expansible shadow size. That is the *Pixel Expansion* of our scheme is 1. Our method is to expand the binary level (only "black" and "white") of the sub pixel to non-binary level (gray level) instead of expanding their shadow size. This paper is organized as the following. In section 2, we will describe the conventional VSS scheme. In section 3, we propose our VSS schemes and also define the new contrast and security conditions. Section 4 gives the experimental results and our definition of the contrast. Section 5 concludes the paper.

2 The Basic VSS Scheme

As described in [1], in a (k, n) VSS scheme, the original image consists of a collection of black and white pixels. Each original pixel is divided into m black and white sub pixels in n shadows. VSS Scheme can be described by $n \times m$ Boolean matrix $S = [s_{ij}]$, where $s_{ij} = 1$ if and only if the jth sub pixel in the ith shadow is black, otherwise $s_{ij} = 0$. When shadows $i_1, i_2, \ldots i_r$, are stacked together in a way which properly aligns the sub pixels, we see a recovered image whose black sub pixels are represented by the Boolean "or" of rows $i_1, i_2, \ldots i_r$ in S. The gray level of this recovered image is proportional to the Hamming weight of the "or"ed m-vector $\vec{v}$. For the fixed threshold $1 \leqq d \leqq m$ and relative difference $\alpha > 0$, if $H(\vec{v}) \geqq d$, this gray level is interpreted by the user's visual system as black, and if $H(\vec{v}) \leqq d - \alpha m$, the result is interpreted as white.

DEFINITION 1. *A (k, n) VSS Scheme can be shown as two collections of $n \times m$ Boolean function matrices B_0 and B_1. When sharing a white (resp. black) pixel, the dealer randomly chooses one row of the Boolean matrix B_0 (resp. B_1) to a relative shadow. The chosen matrix defines the gray level of the m sub pixels in every one of the n shadows. A VSS Scheme is considered valid if the following conditions are met [1] :*

1. *For any S in B_0 (resp. B_1), the "or"ed $\vec{v}$ of any k of the n rows satisfies $H(\vec{v}) \leqq d - \alpha m$ (resp. $H(\vec{v}) \geqq d$).*
2. *For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of $q \times m$ matrices obtained by restricting each $n \times m$ matrices in B_i , $i \in \{0, 1\}$, to rows $i_1, i_2, \ldots, i_q$ are not visual in the sense that they contain the same matrices with the same frequencies.*

The first condition is called *contrast* and the second condition is called *security*. Due to the *security* condition, we cannot get any information about the shared secret if we do not have more than k shadows.

For the basic (2, 2) VSS scheme, we will stack two shadows to recover the shared secret, and "*black*" is 2B and "*white*" is 1B1W in the recovered image. We cannot get any information from any one shadow, because every pixel in the

shadow is represented as 1B1W.

3 The Proposed VSS Scheme with Non-Expansible Shadow Size

In this section, we use new definition of sub pixel to construct the VSS schemes. Instead of expanding the original pixel into *m* sub pixels, we expand the gray level of the sub pixel as a substitute. The new gray sub pixel is shown in Fig.1(a), where a sub pixel is a fixed gray level, and the operation between sub pixels is the "ADDITION". It means that a gray sub pixel "ADD" a gray sub pixel will cause a more gray sub pixel. The stacking operation for the conventional VSS scheme is "OR" shown in Fig.1(b). The major difference between two schemes is that our scheme uses non-binary operation and the conventional scheme uses Boolean operation.

As a replacement for using $n \times m$ Boolean matrix, we therefore define $n \times 1$ matrix $P = [p_i]$ where $p_i = 1$ iff the sub pixel in *i*th shadow is gray level, otherwise $p_i = 0$. When shadows $i_1, i_2, ..., i_r$ are stacked, we can represent it by "ADD" operation of rows $i_1, i_2, ..., i_r$ in *P*. The gray level of this combined sub pixel $G(\vec{v})$ is denoted by the "ADD"ed value of this *r*-tuple column vector $\vec{v}$, i.e., $G(\vec{v}) = i_1 + i_2 + ... + i_r$.

Next we use the DEFINITION 2 to show the formal required conditions of the proposed VSS scheme with non-expansible shadow size. As convenience, we herein use the abbreviation NEVSS (Non-Expansible VSS) scheme to denote our scheme.

DEFINITION 2. *A (k, n) NEVSS scheme can be shown as two collections C_0 and C_1 consisting of n_l and n_g $n \times 1$ matrices, respectively. When sharing a white (resp. black) pixel, the dealer first randomly chooses one column matrix in C_0 (resp. C_1), and then randomly selects one row of this column matrix to a relative shadow. The chosen matrix defines the gray level of one sub pixel in every one of the n shadows. A NEVSS Scheme is considered valid if the following conditions are met :*

1. *For these n_l (resp. n_g) matrices in C_0 (resp. C_1), the "ADD"ed value of any k-tuple column vector $\vec{v}$ satisfies $G(\vec{v}) \in l$ (resp. $G(\vec{v}) \in g$).*
2. *The two sets l and g satisfy that $|P_l - P_g|$ is great enough such that we can distinguish the "black" and "white", where P_l and P_g are the probabilities of the dominant color in the set l and g, respectively.*
3. *For any subset $\{i_1, i_2, .., i_q\}$ of $\{1, 2, .., n\}$ with $q < k$, the $G(\vec{v})$ in C_0 and C_1 are same with the same frequencies.*

The first two conditions are called *contrast* and the third condition is called *security*. Note that the two sets l and g are chosen to let us see the "*black*" and "*white*", and the dominant color means the color with the biggest contrast relative other colors in the set l and g. From the definition, C_0 and C_1 are $n \times 1$ matrices, so the *Pixel Expansion* is 1; however B_0 and B_1 are $n \times m$ matrices, and thus the *Pixel Expansion* is *m*.

3.1 A (2, 2) NEVSS Scheme

For the description of the construction, we first define the notation $m_{i,j}$ to represent the $n \times 1$ column matrices with the Hamming weight *i* of every column vector, and *j* denotes the matrices belong C_j where $j \in \{0, 1\}$. For example $n = 3$, $m_{2,0}$

are three 3×1 column matrices shown as $m_{2,0} = \{\begin{bmatrix}0\\1\\1\end{bmatrix}\begin{bmatrix}1\\0\\1\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}\}$ and $m_{2,0}$ belongs C_0.

Construction 1 : Let C_0 and C_1 be the two white and black collections of 2×1 matrices for a (2, 2) NEVSS scheme. Then, $C_0 = \{m_{0,0}, m_{2,0}\}$, and $C_1 = \{m_{1,1}\}$.

Theorem 1: The scheme from *Construction 1* is a (2, 2) NEVSS scheme with non-expansible shadow size.

Proof: Since the matrices $C_0 = \{m_{0,0}, m_{2,0}\} = \{\begin{bmatrix}0\\0\end{bmatrix}\ \begin{bmatrix}1\\1\end{bmatrix}\}$ and $C_1 = \{m_{1,1}\} = \{\begin{bmatrix}0\\1\end{bmatrix}\ \begin{bmatrix}1\\0\end{bmatrix}\}$, so $l = \{G(\begin{bmatrix}0\\0\end{bmatrix}), G(\begin{bmatrix}1\\1\end{bmatrix})\} = \{0, 2\}$ and $g = \{G(\begin{bmatrix}0\\1\end{bmatrix}), G(\begin{bmatrix}1\\0\end{bmatrix})\} = \{1, 1\}$ when stacking two shadows. The dominant color is "0" (white), because "0" is the biggest contrast among the colors "0", "1", and "2" in l and g. Now, P_l=1/2 P_g=0, the difference P_l-P_g=1/2, thus holds the second condition.

For a proof of the third condition "*security*", note that we randomly chooses one column matrix in C_0 and C_1, and then randomly selects one row of this column matrix to a relative shadow. So for each shadow every pixel will be "0"(white) or "1"(gray) half and half, and one cannot see any thing from the shadow. □

Example 1 : For a (2, 2) NEVSS scheme and $C_0 = \{m_{0,0}, m_{2,0}\}$, and $C_1 = \{m_{1,1}\}$. Fig. 2(a)~(d) are the shared secret, shadow 1, shadow 2, and the recovered image shadow 1 + shadow 2. We can observe that the shadow size is not expansible from the following figures, and the gray level "1" is used to represent "black" and gray level "0" and "2" are used to represent "white".

3.2 A (2, *n*) NEVSS Scheme

We now describe our 2-out-of-*n* NEVSS scheme based on the new gray sub pixel.

Construction 2 : Let C_0 and C_1 be the two white and black collections of *n*×1 column matrices for a (2, *n*) NEVSS scheme. Then, $C_0 = \{m_{0,0}, m_{n,0}\}$, and $C_1 = \{m_{n/2,\,1}\}$ for even *n* or $C_1 = \{m_{\lfloor n/2 \rfloor,\,1}, m_{\lfloor n/2 \rfloor+1,\,1}\}$ for odd *n*.

Theorem 2: The scheme from *Construction 2* is a (2, *n*) NEVSS scheme with non-expansible shadow size.

Proof: For even *n*, since the collections $C_0 = \{m_{0,0}, m_{n,0}\}$ and $C_1 = \{m_{n/2,\,1}\}$, so $l = \{G(m_{0,0}), G(m_{n,0})\} = \{0, 2\}$ and $g = \{\overbrace{0,\ldots,0}^{n_0}, \overbrace{1,\ldots,1}^{n_1}, \overbrace{2,\ldots,2}^{n_2}\}$ when stacking any two shadows, where $n_0 = C_0^2 \times C_{n/2}^{n-2}$, $n_1 = C_1^2 \times C_{n/2-1}^{n-2}$, $n_2 = C_2^2 \times C_{n/2-2}^{n-2}$. The probability of "0" and "2" in l are all 0.5; however the probability of "0" and "2" in g

$= \frac{n_0}{n_0+n_1+n_2} = \frac{n_2}{n_0+n_1+n_2} = \frac{C_0^2 \times C_{n/2}^{n-2}}{C_0^2 \times C_{n/2}^{n-2} + C_1^2 \times C_{n/2-1}^{n-2} + C_2^2 \times C_{n/2-2}^{n-2}} = \frac{1}{1+2n/(n-2)+1} = \frac{n-2}{4n-4}$, and the probability of "1" in g $= \frac{n_1}{n_0+n_1+n_2} = \frac{2n/(n-2)}{1+2n/(n-2)+1} = \frac{2n}{4n-4}$.

Since "0" is the dominant color among "0", "1", and "2", and P_l=1/2, P_g= $\frac{n-2}{4n-4}$ 1/4 for large n. The difference P_l-P_g=1/4, thus holds the second condition, and our (2, n) NEVSS scheme can show the shared secret correctly due to the difference probability.

For a proof of the third condition "*security*", the probability of $G(\vec{v})$=0 in C_0 is 1/2, and the probabilityr of $G(\vec{v})$=0 in C_1 is $\frac{C_{n/2}^{n-1}}{C_{n/2}^{n}} = 1/2$. As the same reason, the probability of $G(\vec{v})$=1 in C_0 is 1/2, and the number of $G(\vec{v})$=1 in C_1 is $\frac{C_{n/2-1}^{n-1}}{C_{n/2}^{n}} = 1/2$. So, it satisfies that "0"(white) and "1"(gray) half and half, and one cannot see any thing from the shadow.

For odd n, using the same approach, we can get the similar result. □

Example 2 : For a (2, 3) NEVSS scheme and

$$C_0 = \{m_{0,0}, m_{3,0}\} = \{\begin{bmatrix}0\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix}\},$$

$$C_1 = \{m_{1,1}, m_{2,1}\} = \{\begin{bmatrix}0\\0\\1\end{bmatrix}\begin{bmatrix}0\\1\\0\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}\begin{bmatrix}1\\0\\1\end{bmatrix}\begin{bmatrix}0\\1\\1\end{bmatrix}\}.$$

I= $\{G(\begin{bmatrix}0\\0\\0\end{bmatrix}), G(\begin{bmatrix}1\\1\\1\end{bmatrix})\}$ ={0, 2}, and g = $\{G(\begin{bmatrix}0\\0\\1\end{bmatrix}), G(\begin{bmatrix}0\\1\\0\end{bmatrix}), G(\begin{bmatrix}1\\0\\0\end{bmatrix}), G(\begin{bmatrix}1\\1\\0\end{bmatrix}), G(\begin{bmatrix}1\\0\\1\end{bmatrix}), G(\begin{bmatrix}0\\1\\1\end{bmatrix})\}$

={0, 1, 1, 2, 1, 1} when shadow 1 and shadow 2 are stacked. The dominant color is "0", P_l=1/2, P_g=1/6, thus the difference P_l-P_g=1/3. Fig.3(a)~(f) are shadow 1, shadow2, shadow 3, and the recovered image shadow 1 + shadow 2, shadow 2 + shadow 3, shadow 1 + shadow 3. We can observe that the shadow size is not expansible from the following figures.

Example 3 : For a (2, 4) NEVSS scheme, the two white and black collections C_0 and C_1 of 4×1 column matrices are shown below :

$$C_0 = \{m_{0,0}, m_{4,0}\} = \{\begin{bmatrix}0\\0\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}\},$$

$$C_1 = \{m_{2,1}\} = \{\begin{bmatrix}1\\1\\0\\0\end{bmatrix}\begin{bmatrix}0\\0\\1\\1\end{bmatrix}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}\begin{bmatrix}0\\1\\0\\1\end{bmatrix}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}\}.$$

3.3 A (*k*, *k*) NEVSS Scheme

Construction 3 : Let C_0 and C_1 be the two white and black collections of k×1 Boolean matrices for a

(k, k) NEVSS scheme. Then, for even k

$C_0 = \{m_{0,0}, m_{2,0}, ..., m_{k,0}\}$,

$C_1 = \{m_{1,1}, m_{3,1}, ..., m_{k-1,1}\}$, and for odd k,

$C_0 = \{m_{0,0}, m_{2,0}, ..., m_{k-1,0}\}$,

$C_1 = \{m_{1,1}, m_{3,1}, ..., m_{k,1}\}$.

Theorem 3: The scheme from *Construction 3* is a (k, k) NEVSS scheme with non-expansible shadow size..

Proof: For even k, since the collections $C_0 = \{m_{0,0}, m_{2,0}, ..., m_{k,0}\}$ and $C_1 = \{m_{1,1}, m_{3,1}, ..., m_{k-1,1}\}$ so I={ $\overbrace{0,\ldots,0}^{n_0}$, $\overbrace{2,\ldots,2}^{n_2}$, $\overbrace{4,\ldots,4}^{n_4}$, ..., $\overbrace{k,\ldots,k}^{n_k}$ }, where n_0 = C_0^k, n_2 = C_2^k, n_4 = C_4^k, ..., n_k = C_k^k, and g={ $\overbrace{1,\ldots,1}^{n_1}$, $\overbrace{3,\ldots,3}^{n_3}$, $\overbrace{5,\ldots,5}^{n_5}$, ..., $\overbrace{k-1,\ldots,k-1}^{n_{k-1}}$ }, where n_1 = C_1^k, n_3 = C_3^k, n_5 = C_5^k, ..., n_{k-1} = C_{k-1}^k. Since "0" is the dominant color among "0"~"k", and $P_l = C_0^k / 2^{k-1} = 1/2^{k-1}$, P_g=0. The difference $P_l - P_g = 1/2^{k-1}$ holds the second condition.

For a proof of the third condition "*security*", for even n, when q(<k) shadows are stacked, the number of $G(\vec{v})=j$ in C_0 is $C_j^q \times (\sum_{i:even} C_{i-j}^{k-q})$, and the number of $G(\vec{v})=j$ in C_1 is $C_j^q \times (\sum_{i:odd} C_{i-j}^{k-q})$, where j=0, 1, ..., q, and $i \leqq k$-q. Since $C_j^q \times (\sum_{i:even} C_{i-j}^{k-q}) = C_j^q \times (\sum_{i:odd} C_{i-j}^{k-q})$, so the third condition is satisfied.

For odd n, using the same approach, we can get the similar result. □

Example 4 : For a (3, 3) NEVSS scheme and

$$C_0 = \{m_{0,0}, m_{2,0}\} = \{\begin{bmatrix}0\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\0\end{bmatrix}\begin{bmatrix}1\\0\\1\end{bmatrix}\begin{bmatrix}0\\1\\1\end{bmatrix}\} ,$$

$$C_1 = \{m_{1,1}, m_{3,1}\} = \{\begin{bmatrix}0\\0\\1\end{bmatrix}\begin{bmatrix}0\\1\\0\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix}\} .$$

$I = \{G(\begin{bmatrix}0\\0\\0\end{bmatrix}), G(\begin{bmatrix}1\\1\\0\end{bmatrix}), G(\begin{bmatrix}1\\0\\1\end{bmatrix}), G(\begin{bmatrix}0\\1\\1\end{bmatrix})\}$ ={0, 2, 2, 2}, and g = $\{G(\begin{bmatrix}0\\0\\1\end{bmatrix}), G(\begin{bmatrix}0\\1\\0\end{bmatrix}), G(\begin{bmatrix}1\\0\\0\end{bmatrix}), G(\begin{bmatrix}1\\1\\1\end{bmatrix})\}$ ={1, 1, 1, 3} when stacking these three shadows. $P_l = 1/2^{(3-1)} = 1/4$, P_g=0, thus the difference $P_l - P_g$=1/4. Fig.4(a)~(c) are shadow 1, shadow2, shadow 3. Fig.4(d)~(f) show that we can not get any information when stacking any two shadows. Fig.4(g) is the recovered image. We can observe that the shadow size is not expansible from the following figures.

Example 5 : For a (4, 4) NEVSS scheme, the two white and black collections C_0 and C_1 of 4×1 Boolean matrices are shown below

$$C_0 = \{m_{0,0}, m_{2,0}, m_{4,0}\} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

,

$$C_1 = \{m_{1,1}, m_{3,1}\} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

.

4.Experimental Results and Contrast of the NEVSS Scheme

4.1 Experimental Results

Example 1, Example 2, and Example 4 show the (2, 2), (2, 3), and (3, 3) NEVSS schemes. In this section, we use these three NEVSS schemes to show how to choose the optimal gray level of sub pixel such that we can get the clear recovered image. Fig.5~Fig.7 shows the recovered images using different gray levels of the basic sub pixel for (2, 2), (2, 3), and (3, 3) NEVSS schemes. The gray levels we use are GL-0, GL-30, GL-60, GL-90, GL-120, GL-150. Here, GL-0 means black and GL-255 means white.

From the above experimental results, Fig.5(a), Fig.6(a), Fig.7(a) have the best contrast a. We find an interesting observation that the optimal choice of the gray level will be the "*black*". The reason is that when the sets l or g have the element "0", the "0" (white) will perceive *big* contrast relative "*black*" color.

According the experiment, we will define the "contrast" of our NEVSS scheme to meet the real situation in next section.

4.2 Contrast of the NEVSS Scheme

The quality of the recovered image in a VSS scheme is usually called *contrast*. Since the original black and white pixels will be expanded to the black and white sub pixels, the recovered image is less clear to the human visual system than the original image. *Contrast* provides a measurement for the quality of the recovered image; however, there is no consensus on the definition of contrast. First, we introduce the former definitions about *contrast*. The parameters h and l are the "whiteness" of a white and black pixel, and m is the *Pixel Expansion*. Naor and Shamir defined contrast as $\alpha_{NS} = \frac{h-l}{m}$ [1]. Verheul and Van Tilborg showed that Naor and Shamir's definition is inadequate. For example, two schemes with the parameters h=2, l=0, m=7, and h=4, l=2, m=7 will have the same contrast value. However, these two schemes have different clearness of the recovered images. They gave the new *contrast* as $\alpha_{VV} = \frac{h-l}{m(h+l)}$ [7]. The definition of α_{VV} does not show the correctness. Since α_{VV} is always $1/m$, when l=0, but in fact for larger h the recovered image will more clear. Eisen and Stinson improved the previous disadvantages and defined their *contrast* as $\alpha_{ES} = \frac{h-l}{m+l}$ [6].

The authors defined their own *contrast* by the observation of the real results. We also use the methodology to define the *contrast* of the NEVSS scheme such that the definition of contrast is consistent with the recovered image. The contrast of NEVSS α_{NEVSS} is defined as the following:

$$\alpha_{NEVSS} = |P_l - P_g| \times \frac{255 - (gray\ level\ of\ the\ sub\ pixel)}{255},$$

where P_l is the probability of the *dominant* color in the set $\boldsymbol{l}$, and P_g is the probability of the *dominant* color in the set $\boldsymbol{g}$.

The first term in $\boldsymbol{a}_{NEVSS}$ is the difference of the probability for the *dominant* color, and the second term is the background color. The *dominant* color means the biggest *contrast* relative other colors in the set $\boldsymbol{l}$ and $\boldsymbol{g}$ mentioned in the early section. For example, for (2, 2), (2, 3), and (3, 3) NEVSS schemes, the *dominant* color is "0" (white). The contrast of the recovered images in Fig.5 ~ Fig.6 are calculated and shown in Table 1.

From Table 1, and Fig.5~Fig.7, we see that our definition of *contrast* is consistent with the experimental results.

Obviously, the value of $\boldsymbol{a}_{NS}$, $\boldsymbol{a}_{VV}$, $\boldsymbol{a}_{ES}$, and $\boldsymbol{a}_{NEVSS}$ will be different for one recovered image due to the different definitions. Here, we make a test to show the relation between clearness and the contrast value for different definitions of contrast. First, we choose five typical recovered images for the conventional (2, 2) VSS scheme and use a score of 5 to 1 as "*excellent*" to "*poor*" to represent them. Then, select five recovered images for the (2, 2) NEVSS scheme with the same clear quality of the recovered images compared to the conventional (2, 2) VSS scheme. Calculate each contrast value, and we find every slope of line raises when the clearness increases shown in Fig.8. This shows the truth that these contrast $\boldsymbol{a}_{NS}$, $\boldsymbol{a}_{VV}$, $\boldsymbol{a}_{ES}$, and $\boldsymbol{a}_{NEVSS}$ really give a measurement of how clear the recovered image is.

5. Concluding remarks

In this paper, we have presented new (2, 2), (2, *n*), and (*k*, *k*) NEVSS schemes with non-expansible shadow size based on the new infrastructure and operation of the sub pixel. In fact, we can also construct (*k*, *n*) NEVSS schemes by choosing the suitable sets $\boldsymbol{l}$ and $\boldsymbol{g}$. Here, we give the white and black collections C_0, C_1 for (3, 4) NEVSS scheme to show the feasibility of (*k*, *n*) NEVSS schemes. $C_0 = \{\boldsymbol{m}_{0,0}, \boldsymbol{m}_{3,0}\}$, $C_1 = \{\boldsymbol{m}_{1,1}, \boldsymbol{m}_{4,1}\}$, and $\boldsymbol{l}$ = {0, 0, 2, 2, 2, 3}, $\boldsymbol{g}$ = {0, 1, 1, 1, 3, 3}, then P_l - P_g =1/3-1/6=1/6. If we use the gray level of sub pixel = GL-0, i.e., black, then $\boldsymbol{a}_{NEVSS}$ $= (\frac{2}{6} - \frac{1}{6}) \times (\frac{255-0}{255}) = \frac{1}{6}$. However, the general method for constructing (*k*, *n*) NEVSS schemes may need the further studies.

References

[1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology- EUROCRYPT'94*, *Lecture Notes in Computer Science*, No.950, pp.1-12, Springer-Verlag, 1995.

[2] S. Droste, "New results on visual cryptography," *Advances in Cryptology-EUROCRYPT'96*, *Lecture Notes in Computer Science*, No.1109, pp.401-415, Springer-Verlag, 1996.

[3] T. Katoh and Hideki Imai, "Some visual secret sharing schemes and their share size," *Proceedings of International Conferences on Cryptology and Information Security*, pp.41-47, DEC. 1996.

[4] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," *ECCC, Electronic Colloquium on Computational Complexity* (TR96-012), via

WWW using http://www.eccc.uni-trier.de/eccc/.

[5] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Constructions and bounds for visual cryptography," *Proc. 23rd International Colloquium on Automata, Languages, and Progrramming (ICALP'96), Lecture Notes in Computer Science* , Springer-Verlag, 1996.

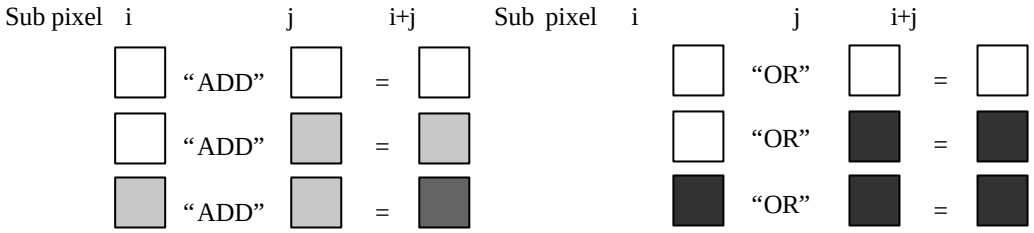
[6] P.A. Eisen and D.R. Stinson, "Threshold Visual Cryptography Schemes With Specified Whiteness", submitted to Designs, Codes and Cryptography, available at http://cacr.math.uwaterloo.ca/~dstinson/visual.html.

[7] E.R. Verheul and H.C.A. Van Tilborg, "Constructions and properties of *k* out of *n* visual secret sharing schemes," *Designs, Codes and Cryptography*, vol.11, No.2, pp.179-196, May, 1997.

[8] C. N. Yang and C.S. Laih, "New colored visual secret sharing schemes," accepted and to be published, *Designs, Codes and Cryptography*.

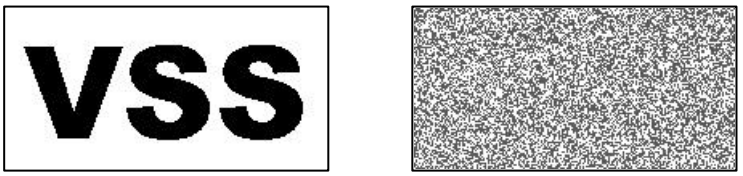
[9] G.R. Blakley, "Safeguarding cryptographic keys", *AFIPS conference proceedings*, vol.48, pp.313-317, 1979.

[10] A. Shamir, "How to share a secret," *Commun. of th ACM*, vol.22, pp.612-613, Nov. 1979.



(a) "ADD" operation for gray sub pixels (b) "OR" operation for black and white sub pixels

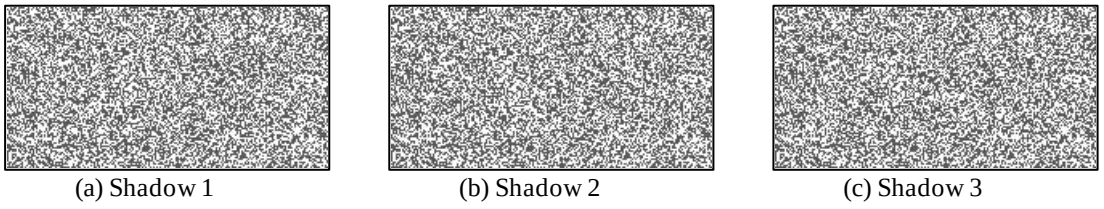
Figure 1. The sub pixels of the proposed scheme and conventional scheme and their operations.



(a) Shared secret (b) Shadow 1

(c) Shadow 2 (d) Shadow 1 + Shadow 2

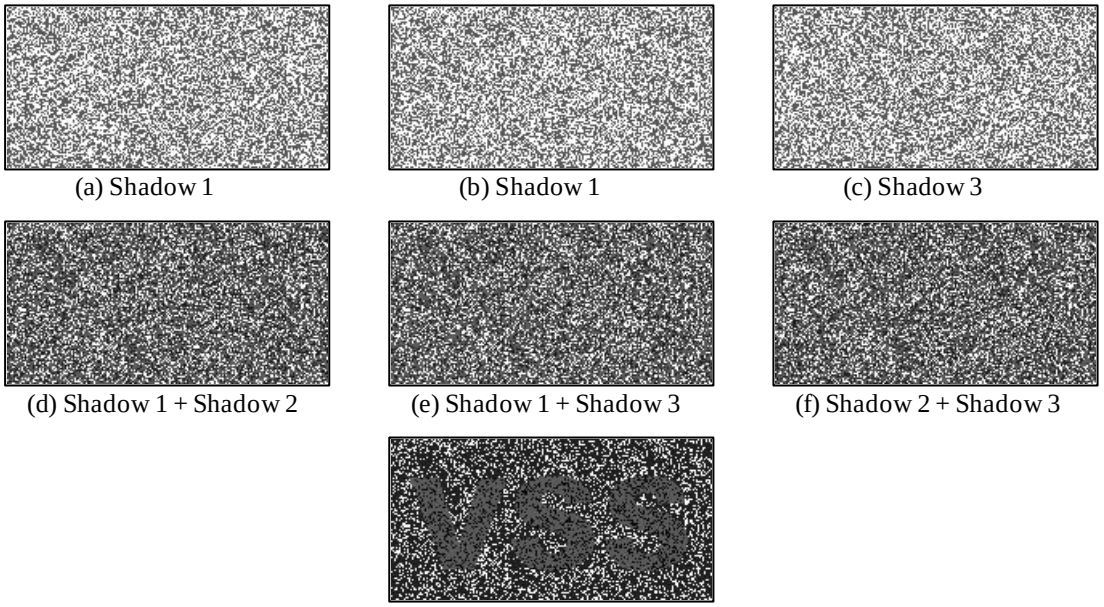
Figure 2. The (2, 2) NEVSS scheme



(a) Shadow 1 (b) Shadow 2 (c) Shadow 3

(d) Shadow 1 + Shadow 2 (e) Shadow 2 + Shadow 3 (f) Shadow 1 + Shadow 3

Figure 3. The (2, 3) NEVSS scheme

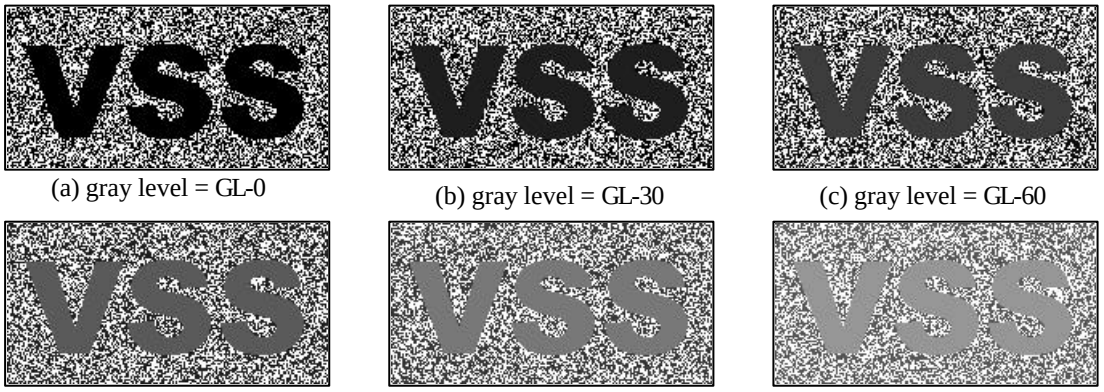


(a) Shadow 1 (b) Shadow 1 (c) Shadow 3

(d) Shadow 1 + Shadow 2 (e) Shadow 1 + Shadow 3 (f) Shadow 2 + Shadow 3

(g) Shadow 1 + Shadow 2 + Shadow 3

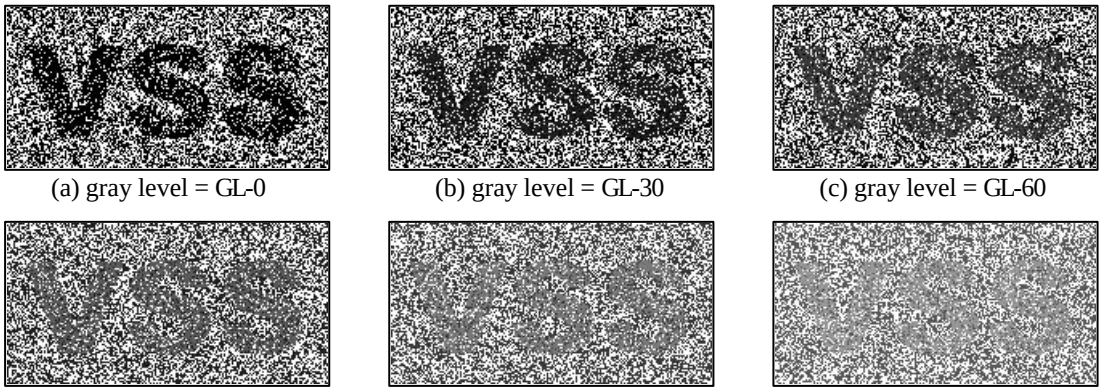
Figure 4. The (3, 3) NEVSS scheme



(a) gray level = GL-0 (b) gray level = GL-30 (c) gray level = GL-60

(c) level = GL-90 (e) gray level = GL-120 (f) gray level = GL-150

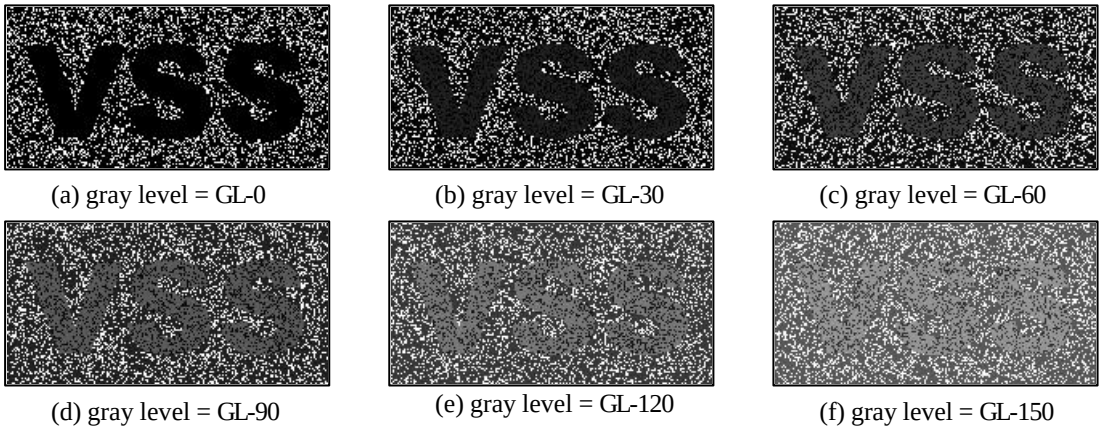
Figure 5. The recovered images for (2, 2) NEVSS scheme with different gray levels of sub pixel



(a) gray level = GL-0 (b) gray level = GL-30 (c) gray level = GL-60

(d) gray level = GL-90 (e) gray level = GL-120 (f) gray level =GL-150

Figure 6. The recovered images for (2, 3) NEVSS scheme with different gray levels of sub pixel



(a) gray level = GL-0 (b) gray level = GL-30 (c) gray level = GL-60

(d) gray level = GL-90 (e) gray level = GL-120 (f) gray level = GL-150

Figure 7. The recovered images for (3, 3) NEVSS scheme with different gray levels of sub pixel

Table 1. The contrast α_{NEVSS} for different NEVSS schemes

Types of NEVSS schemes	Gray level of the sub pixel					
	GL-0	GL-30	GL-60	GL-90	GL-120	GL-150
(2, 2)	0.50	0.44	0.38	0.32	0.26	0.21
(2, 3)	0.33	0.29	0. 25	0.21	0.17	0.14
(3, 3)	0.25	0.22	0.19	0.16	0.13	0.11

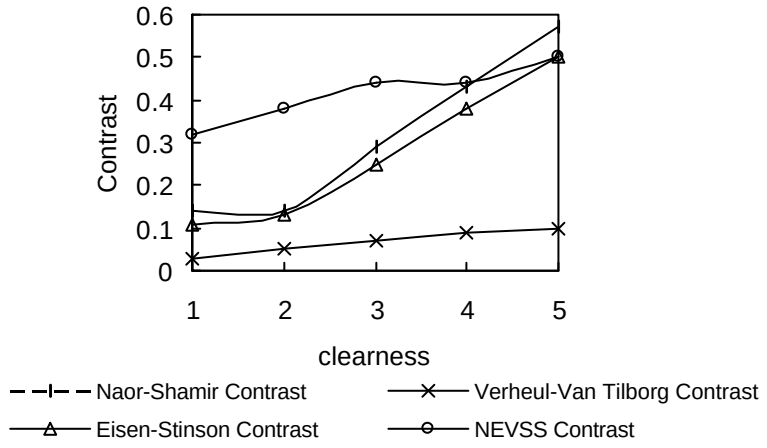


Figure 8. The value of α_{NS}, α_{VV}, α_{ES}, and α_{NEVSS}