New visual secret sharing schemes using probabilistic method

Ching-Nung Yang *

Department of Computer Science and Information Engineering, National Dong Hwa University, 1, Sec. 2, Da Hsueh Rd., Shou-Feng 974, Hualien, Taiwan, ROC

Received 6 March 2003; received in revised form 5 November 2003

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 [Naor, Shamir, Visual cryptography, Advances in Cryptology-EUROCRYPT’94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1995, p. 1]) will be expanded. Most recent papers about VSS schemes are dedicated to get a higher contrast or a smaller shadow size.

In this paper, we use the frequency of white pixels to show the contrast of the recovered image. Our scheme is non-expansible and can be easily implemented on a basis of conventional VSS scheme. The term non-expansible means that the sizes of the original image and shadows are the same.

© 2004 Elsevier B.V. All rights reserved.

Keywords: Secret sharing scheme; Visual secret sharing scheme

1. Introduction

The secret sharing scheme, which is sometimes called threshold scheme, was first introduced by Blakley and Shamir independently in 1971. 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 \(n\) different shadows. We can recover the master key by combining any \(k(k \leq n)\) shadows, but \(k-1\) or fewer shadows will get no information.

A new type of secret sharing scheme (Naor and Shamir, 1995; Droste, 1996; Katoh and Imai, 1996; Ateniese et al., 1996a, 1996b; Verheul and Van Tilborg, 1997; Eisen and Stinson, 2002) called visual secret sharing (VSS) scheme, was first proposed by Naor and Shamir in 1994 (Naor and Shamir, 1995). The shared secret is an image (such as printed texts, handwritten notes, pictures, etc.), and the VSS scheme provides an unconditionally secure way to encode the shared secret into shadow images. The decoder is the human visual system. Therefore, we can easily recover the shared secret.
by using the eyes of human beings. For a \((k, n)\) VSS scheme, \(k\) or more participants can get the shared secret by stacking their shadows (transparencies). In the previous VSS schemes, we use several sub pixels in the shadow to represent a pixel in the original secret image, that is, the size of shadow is expanded. Here we define the factor Pixel Expansion as \((\text{the size of the shadow})/(\text{the size of the secret image})\). For example, the Pixel Expansion of \((2, 2), (2, n), (3, n)\) and optimal \((k, k)\) Naor–Shamir VSS schemes are \(2, n, 2n - 2,\) and \(2^{k-1}\), respectively.

In this paper, we use the frequency of white pixels to let human visual system distinguish between “black” and “white”. The new schemes have non-expansible shadow size and the same contrast level of the conventional VSS scheme. The paper is organized as the following. In Section 2, we describe the conventional VSS scheme. In Section 3, we propose our VSS schemes with new definitions of contrast and security conditions and discuss the recognition of small areas in the recovered image for our probabilistic schemes. We also show a transformation from the conventional scheme to our new scheme. Section 4 gives a more reasonable definition of contrast for our scheme. Section 5 concludes the paper.

2. The basic VSS scheme

As described in (Naor and Shamir, 1995), in a \((k, n)\) VSS scheme, the original image consists of a collection of black and white pixels. Each pixel is divided into \(m\) black and white sub pixels in \(n\) shadows. A VSS scheme can be described by \(n \times m\) Boolean matrix \(S = [s_{ij}]\), where \(s_{ij} = 1\) if and only if the \(j\)th sub pixel in the \(i\)th 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”-ed 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 \(V\). For the fixed threshold \(1 \leq d \leq m\) and contrast \(x > 0\), if \(H(V) \geq d\), this gray level is interpreted by the human visual system as black, and if \(H(V) \leq d - xm\), the result is interpreted as white.

Definition 1. A \((k, n)\) VSS Scheme can be represented as two collections of \(n \times m\) Boolean 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 (Naor and Shamir, 1995):

1. For any \(S\) in \(B_0\) (resp. \(B_1\)), the “OR”-ed \(V\) of any \(k\) of the \(n\) rows satisfies \(H(V) \leq d - xm\) (resp. \(H(V) \geq d\)).
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 \(n \times m\) matrix in \(B_0\) to \(B_1\), to rows \(i_1, i_2, \ldots, i_q\) are not distinguishable 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 a basic \((2, 2)\) VSS scheme, we will stack two shadows to recover the shared secret, and now the “black” is 2B0W and the “white” is 1B1W where \(xByW\) denotes that we use \(x\) black sub pixels and \(y\) white sub pixels to represent an original pixel. We cannot get any information from any one shadow because every pixel is represented as 1B1W sub pixels.

3. The proposed VSS schemes with non-expansible shadow size

In this section, we propose new methods to construct the VSS schemes. Our schemes use a different approach, the probabilistic method. The major difference between these two schemes is that our scheme uses pixel operation and the conventional scheme uses sub pixel operation. Our “OR”-ed operation of pixel is the same as the stacking operation of sub pixel in the conventional VSS scheme (see Fig. 1). Instead of expanding the pixel into \(m\) sub pixels, we only use one pixel to
represent one pixel. The conventional VSS scheme uses $x_0B+y_0W$ to represent the white pixel and $x_1B+y_1W$ to represent the black pixel, where $x_0+y_0 = x_1+y_1 = m$. Then, the values of $x_i$, $y_i$, and $m$ will cause different contrast and shadows extension.

Our new approach is not expanded. A black or white pixel can be represented as $xByW$, where $x+y = 1$ ($x = 0$, $y = 1$ or $x = 1$, $y = 0$, i.e., $m = 1$).

As a replacement for using $n \times m$ Boolean matrix, we herein define $n \times 1$ matrix $S = [s_i]$ where $s_i = 1$ if the pixel in $i$-th shadow is black pixel and 0 for white pixel. When shadows $i_1, i_2, \ldots, i_r$ are stacked, we can represent it by “OR”-ed operation of rows $i_1, i_2, \ldots, i_r$ in $S$. The black or white level of this combined pixel $L(V)$ is determined by the “OR”-ed operation of this $r$-tuple column vector $V$, i.e., $L(V) = s_1 + s_2 + \cdots + s_r$, where “+” denotes “OR”-ed operation. The value of $L(V)$ is 0 (white) or 1 (black). Our method is to use the frequency of white pixels in the black and white areas of the recovered image for interpreting black and white pixels by human visual system. Define $p_0$ (resp. $p_1$) as the appearance probability of white pixel in the white (resp. black) area of the recovered image. For the fixed threshold probability $0 \leq p_{TH} \leq 1$ and relative contrast $\alpha > 0$, if $p_0 \geq p_{TH}$ and $p_1 \leq p_{TH} - \alpha$, the frequency of white pixels in the white area of the recovered image will be higher than that in the black area. So, the human visual system can distinguish with high probability between black and white areas. In fact the high probability will be about 99.73\% if we use the recognition criterion “$\mu_0 - 3\sigma_0 > \mu_1 + 3\sigma_1 + N_d$” defined in Section 3.5, where $N_d$ is the minimum difference of white pixels between white and black areas. Fig. 2 shows the contrast of 1B1W and the area with certain frequency of white pixels. Consider two regions $R_0$ and $R_1$ (see Fig. 2). On the brighter side, $R_0$ in Fig. 2(a) is 1B1W pattern of the conventional (2,2) VSS scheme and $p_0$ in $R_0$ of Fig. 2(b)–(d) is 1/2, 1/2, and 1/4. On the darker side $R_1$ in Fig. 2(a)–(d), $p_1$ is 0, 0, 1/6, and 0. Like the conventional scheme, we really can distinguish the white area ($R_0$) and black area ($R_1$) due to the different frequency of white pixels. In fact, the appearance probabilities of white pixels $p_0$ and $p_1$ in Fig. 2(b)–(d) are used for our proposed (2,2), (2,3), and (3,3) schemes, respectively.

Next, we use Definition 2 to show the formal required conditions of our probabilistic VSS scheme. Here we use the term “probabilistic” to point out that our visual system distinguishes the contrast of the recovered image based on the difference of the frequency of white color in black and white areas. For convenience, we use the abbreviation ProbVSS (Probabilistic VSS) scheme to denote our scheme.

**Definition 2.** A $(k,n)$ ProbVSS scheme can be shown as two sets, white set $C_0$ and black set $C_1$, consisting of $n_k$ and $n_{n \times 1}$ matrices, respectively. When sharing a white (resp. black) pixel, the dealer first randomly chooses one $n \times 1$ 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 color level of pixel in
every one of the \( n \) shadows. A ProbVSS Scheme is considered valid if the following conditions are met:

1. For these \( n \) matrices (resp. \( n \)) matrices in the set \( C_0 \) (resp. \( C_1 \)), the “OR”-ed value of any \( k \)-tuple column vector \( V \) is \( L(V) \). These values of all matrices form a set \( \lambda \) (resp. \( \gamma \)).

2. The two sets \( \lambda \) and \( \gamma \) satisfy that \( p_0 \geq p_{TH} \) and \( p_1 \leq p_{TH} - \alpha \), where \( p_0 \) and \( p_1 \) are the appearance probabilities of the “0” (white color) in the set \( \lambda \) and \( \gamma \), respectively.

3. For any subset \( \{i_1, i_2, \ldots, i_q\} \) of \( \{1, 2, \ldots, n\} \) with \( q < k \), the \( p_0 \) and \( p_1 \) are the same.

The first two conditions are called contrast and the third is called condition security. From the above definition, the matrices in \( C_0 \) and \( C_1 \) are \( n \times 1 \) matrices, so the Pixel Expansion is one; however \( B_0 \) and \( B_1 \) in the conventional VSS scheme are \( n \times m \) matrices, and thus the Pixel Expansion is \( m \).

The following content of this section is devoted to show how to construct the ProbVSS schemes satisfying the above three criteria. Sections 3.1–3.3 describe the constructions of the (2, 2), (2, n), and (\( k, k \)) ProbVSS schemes and Section 3.4 shows a method to transform the basis matrices of a general (\( k, n \)) VSS scheme to \( C_0 \) and \( C_1 \) sets in the (\( k, n \)) ProbVSS scheme.

The concept of our ProbVSS scheme that can be constructed using the modification of the conventional VSS scheme is simply described here and the formal construction method will be introduced in Section 3.4. For conventional VSS schemes, a pixel in the original picture is expanded to \( m \) sub pixels and the number of white sub pixels (i.e., the “whiteness”) of a white and black pixel is \( h \) and \( l \). When stacking \( k \) shadows, we will have \( \lceil m - h \rceil \cdot B \lceil k \rceil \) \( W \) sub pixels for a white pixel and \( \lceil m - l \rceil \cdot B \lceil k \rceil \) \( W \) sub pixels for a black pixel.

Hence, from the observation, if we use all the columns of the basis matrices \( B_0 \) and \( B_1 \) of a conventional VSS scheme as the \( n \times 1 \) column matrices in the sets \( C_0 \) and \( C_1 \), we can let the pixel appear in white color with different probability instead of expanding the original pixel to \( m \) sub pixels and the frequency of white pixels in white and black areas in the recovered image will be \( p_0 = \frac{k}{m} \) and \( p_1 = \frac{l}{m} \).

The comparison of contrast of the recovered image using different constructions is given in Table 2 (Section 4). One can see that the ProbVSS scheme using modification of the common VSS scheme is easy but it will not have the highest contrast for all \( k \) and \( n \).

**3.1. A 2-out-of-2 ProbVSS scheme**

For the description of the construction, we first define the notation \( \mu_{i,j} \) to represent the set of all \( n \times 1 \) column matrices with the Hamming weight \( i \) of every column vector, and \( j \) denotes the matrices belonging to \( C_j \) where \( j \in \{0, 1\} \). For example \( n = 3 \), \( \mu_{2,0} \) are three \( 3 \times 1 \) column matrices shown as

\[
\mu_{2,0} = \left\{ \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}
\]

and \( \mu_{2,0} \) belongs to \( C_0 \).

**Construction 1.** Let \( C_0 = \{ \mu_{0,0}, \mu_{2,0} \} \), and \( C_1 = \{ \mu_{1,1} \} \). Then, \( C_0 \) and \( C_1 \) are the white and black sets consisting of \( 2 \times 1 \) matrices for a (2, 2) ProbVSS scheme.

**Theorem 1.** The scheme from Construction 1 is a (2, 2) ProbVSS scheme with non-expansible shadow size and the parameters threshold probability \( p_{TH} = 0.5 \) and the contrast \( \alpha = 0.5 \).

**Proof.** Since the two sets

\[
C_0 = \{ \mu_{0,0}, \mu_{2,0} \} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}
\]

and

\[
C_1 = \{ \mu_{1,1} \} = \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\},
\]

so

\[
\lambda = \left\{ L\left( \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right), L\left( \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right) \right\} = \{0, 1\}
\]
and

\[ \gamma = \{ L(\begin{bmatrix} 0 \\ 1 \end{bmatrix}), L(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) \} = \{ 1, 1 \} \]

when stacking two shadows. The appearance probabilities of white color in \( \lambda \) and \( \gamma \) are \( p_0 = 0.5 \) and \( p_1 = 0 \), the threshold probability \( p_{TH} = 0.5 \) and the contrast \( z = 0.5 \).

For a proof of the third condition “security”, note that we randomly choose one column matrix in \( C_0 \) and \( C_1 \) and then select one row of this column matrix to a relative shadow. Then, for each shadow, every pixel will be “0” (white) or “1” (black) half and half. For shadow 1 \( \lambda = \{ L([0]), L([1]) \} = \{ 0, 1 \} \) and \( \gamma = \{ L([0]), L([1]) \} = \{ 0, 1 \} \), for shadow 2 \( \lambda = \{ L([0]), L([1]) \} = \{ 0, 1 \} \) and \( \gamma = \{ L([1]), L([0]) \} = \{ 1, 0 \} \). That is, the appearance probabilities of the white color in the sets \( \lambda \) and are the same (\( p_0 = p_1 = 0.5 \)), and one cannot see anything from the shadow. □

**Example 1.** For a \((2,2)\) ProbVSS scheme and \( C_0 = \{ \mu_{0,0}, \mu_{2,0} \} \), and \( C_1 = \{ \mu_{1,1} \} \). Fig. 3(a)–(d) are the original secret image, shadow 1, shadow 2, and the recovered image (shadow 1 + shadow 2), respectively. From these figures, we observe that the shadow size is not expansible. At this time, in the recovered image, there are about 50% white pixels and 50% black pixels in white area, and 100% black pixels in the black area.

### 3.2. A 2-out-of-\( n \) ProbVSS scheme

Based on the new probabilistic method, a 2-out-of-\( n \) ProbVSS scheme is described as follows.

**Construction 2.** Let \( C_0 \) and \( C_1 \) be the white and black sets consisting of \( n \times 1 \) column matrices for a \((2,n)\) ProbVSS scheme. Then, \( C_0 \) and \( C_1 \) are defined as the following. \( C_0 = \{ \mu_{0,0}, \mu_{n,0} \} \), and \( C_1 = \{ \mu_{n/2,1} \} \) (even \( n \)) or \( C_1 = \{ \mu_{n/2,1}, \mu_{n/2+1,1} \} \) (odd \( n \)).

**Theorem 2.** The scheme from Construction 2 is a \((2,n)\) ProbVSS scheme with non-expansible shadow size and the parameters threshold probability \( p_{TH} = 0.5 \) and the contrast \( z = \frac{n}{4n-4} \) (even \( n \)) or \( \frac{n+1}{4n-4} \) (odd \( n \)).

**Proof.** For even \( n \), since the two sets \( C_0 = \{ \mu_{0,0}, \mu_{n,0} \} \) and \( C_1 = \{ \mu_{n/2,1} \} \), so \( \lambda = \{ L(\mu_{0,0}), L(\mu_{n,0}) \} \), \( \gamma = \{ 0, \ldots, 0, 1, \ldots, 1 \} \) when stacking any two shadows, where \( n_0 = C_0^2 \times C_{n/2}^{-2} \), \( n_1 = C_1^2 \times C_{n/2-1}^{-2} + C_1^2 \times C_{n/2-2}^{-2} \). The appearance probabilities of white color in \( \lambda \) and are

\[ p_0 = 0.5 \]

and

\[ p_1 = \frac{n_0}{n_0 + n_1} = \frac{C_0^2 \times C_{n/2}^{-2}}{C_0^2 \times C_{n/2}^{-2} + C_1^2 \times C_{n/2-1}^{-2} + C_1^2 \times C_{n/2-2}^{-2}} = \frac{n - 2}{4n-4}. \]

The threshold probability \( p_{TH} = 0.5 \) and the contrast \( z = 0.5 - \frac{n-2}{4n-4} = \frac{n}{4n-4} \), and will be 0.25 for large \( n \).

For a proof of the third condition “security”, it is obvious that \( C_0 = \{ \mu_{0,0}, \mu_{n,0} \} \) and \( C_1 = \{ \mu_{n/2,1} \} \) satisfy that “0” (white) and “1” (black) are half and half. That is, the appearance probabilities of the White color in the sets \( \lambda \) and \( \gamma \) are the same (\( p_0 = p_1 = 0.5 \)), and one cannot see anything from the shadow.

For odd \( n \), by using the same analysis, we get the result.
\[ p_0 = 0.5 \]
and
\[ p_1 = \frac{n_0}{n_0 + n_1} \]

\[
\frac{C^2_0 \times C_{[n/2]}^{n-2} + C^2_0 \times C_{[n/2] + 1}^{n-2} + C^2_1 \times C_{[n/2]-1}^{n-2} + C^2_2 \times C_{[n/2]-2}^{n-2} + C^2_2 \times C_{[n/2]-1}^{n-2}}{4n} = n - 1. \]

The threshold probability is \( p_{T_H} = 0.5 \) and the contrast \( z = 0.5 - \frac{a_{T_H}}{4n} = \frac{a_{T_H}}{4n} \), and will be 0.25 for large \( n \). \( \square \)

**Example 2.** For a \((2, 3)\) ProbVSS scheme and

\[
C_0 = \{\mu_{0,0}, \mu_{3,0}\} = \left\{\begin{array}{ccc} 0 & 1 \\ 0 & 1 \\ 0 & 1\end{array}\right\}, \quad C_1 = \{\mu_{1,1}, \mu_{2,1}\} = \left\{\begin{array}{ccc} 0 & 1 \\ 0 & 1 \\ 0 & 1\end{array}\right\}, \end{align}
\]

\[ \lambda = \left\{L\left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array}\right), L\left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right)\right\} = \{0, 1\} \]

and

\[ \gamma = \left\{L\left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array}\right), L\left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right), L\left(\begin{array}{c} 0 \\ 1 \\ 1 \end{array}\right)\right\} = \{0, 1, 1, 1, 1\} \]

when shadow 1 and shadow 2 are stacked. The probabilities \( p_0 = 1/2 \) and \( p_1 = 1/6 \), the threshold probability \( p_{T_H} = 0.5 \) and the contrast \( z = 1/3 \). Fig. 4(a)–(f) are shadow 1, shadow 2, shadow 3, and the recovered image shadow 1 + shadow 2, shadow 2 + shadow 3, shadow 1 + shadow 3, respectively. From these figures, we observe that the shadow size is not expansible.

**Example 3.** For a \((2, 4)\) ProbVSS scheme, the two white and black sets \( C_0 \) and \( C_1 \) consisting of \( 4 \times 1 \) column matrices are shown below:

\[
C_0 = \{\mu_{0,0}, \mu_{4,0}\} = \left\{\begin{array}{ccc} 0 & 1 \\ 0 & 1 \\ 0 & 1\end{array}\right\}, \quad C_1 = \{\mu_{2,1}\} = \left\{\begin{array}{ccc} 0 & 1 \\ 0 & 1 \\ 0 & 1\end{array}\right\}, \end{align}
\]

\[ \lambda = \left\{L\left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array}\right), L\left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right)\right\} = \{0, 1\} \]

and

\[ \gamma = \left\{L\left(\begin{array}{c} 1 \\ 1 \\ 1 \end{array}\right), L\left(\begin{array}{c} 0 \\ 0 \\ 0 \end{array}\right), L\left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array}\right)\right\} = \{0, 1, 1, 1, 1\} \]

when shadow 1 and shadow 2 are stacked. The probabilities \( p_0 = 1/2 \) and \( p_1 = 1/6 \), the threshold probability \( p_{T_H} = 0.5 \) and the contrast \( z = 1/3 \).

Another construction for a \((2, n)\) ProbVSS scheme is shown below.

**Construction 2’.** Let \( C_0 \) and \( C_1 \) be the white and black sets consisting of \( n \times 1 \) column matrices for a \((2, n)\) ProbVSS scheme. Then, \( C_0 \) and \( C_1 \) are defined as follows. \( C_0 = \{\mu_{n,0}, \ldots, \mu_{n,0}, \mu_{0,0}\} \), and \( C_1 = \{\mu_{n-1,1}\} \).
Theorem 2'. The scheme from Construction 2' is a (2, n) ProbVSS scheme with non-expansible shadow size and the parameters threshold probability \( p_{TH} = 1/n \) and the contrast \( z = 1/n \).

Proof. It is obvious that \( p_0 = 1/n \) and \( p_1 = 0 \). Hence, the threshold probability \( p_{TH} = 1/n \) and the contrast \( z = 1/n - 0 = 1/n \).

Example 4. For a (2, 3) ProbVSS scheme using Construction 2' we get

\[
C_0 = \{\mu_{3,0}, \mu_{3,0}, \mu_{0,0}\} = \left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\},
\]

\[
C_1 = \{\mu_{2,1}\} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}.
\]

\[
\lambda = \left\{ L\left( \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right), L\left( \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right), L\left( \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right) \right\} = \{1, 1, 0\}
\]

and

\[
\gamma = \left\{ L\left( \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right), L\left( \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right), L\left( \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right) \right\} = \{1, 1, 1\}
\]

when shadow 1 and shadow 2 are stacked. The probabilities \( p_0 = 1/3 \) and \( p_1 = 0 \), the threshold probability \( p_{TH} = 1/3 \) and the contrast \( z = 1/3 \).

3.3 A k-out-of-k ProbVSS scheme

Construction 3. Let \( C_0 \) and \( C_1 \) be the two white and black sets consisting of \( k \times 1 \) matrices for a \((k, k)\) ProbVSS scheme. Then, \( C_0 \) and \( C_1 \) are constructed as \( C_0 = \{\mu_{i,0}, \mu_{i,0}, \ldots, \mu_{i,0}\} \) and \( C_1 = \{\mu_{i,1}, \mu_{i,1}, \ldots, \mu_{i,1}\} \) where

\[
\lambda = \{0, 1, \ldots, k\}, \quad \gamma = \{1, 1, \ldots, 1\}.
\]

The appearance probabilities of white color in \( \lambda \) and \( \gamma \) are \( p_0 = 1/2^{k-1} \) and \( p_1 = 0 \), and the threshold probability \( p_{TH} = 1/2^{k-1} \) and the contrast \( z = 1/2^{k-1} \).

For a proof of the third condition “security”, when \( q \) \((< k)\) shadows are stacked, the number of \( V \) with Hamming weight \( j \) in \( C_0 \) and \( C_1 \) is \( C_j \times (\sum_{i \text{even}} C_{i-j}^{k-j}) \) and \( C_j \times (\sum_{i \text{odd}} C_{i-j}^{k-j}) \), where \( 0 \leq j \leq q \) and \( 0 \leq i \leq k \). Since \( C_j \times (\sum_{i \text{even}} C_{i-j}^{k-j}) = C_j \times (\sum_{i \text{odd}} C_{k-j}^{k-j}) \), so the third condition is satisfied.
For odd \( k \), by using the same approach, we get the similar result. \( \square \)

**Example 5.** For a \((3,3)\) ProbVSS scheme and

\[
C_0 = \{ \mu_{0,0}, \mu_{2,0} \} = \begin{bmatrix} 0 & 1 & 1 & 0 \ 0 & 0 & 1 & 1 \end{bmatrix},
\]

\[
C_1 = \{ \mu_{1,1}, \mu_{3,1} \} = \begin{bmatrix} 0 & 1 & 1 & 1 \ 1 & 0 & 0 & 1 \end{bmatrix}.
\]

The set

\[\lambda = \begin{bmatrix} L \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, L \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, L \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, L \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \end{bmatrix} = \{0,1,1,1\},\]

and the set

\[\gamma = \begin{bmatrix} L \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, L \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, L \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, L \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \end{bmatrix} = \{1,1,1,1\} \]

when stacking these three shadows. \( \rho_0 = 1/4 \), \( \rho_1 = 0 \), and the threshold probability is \( \rho_{\text{TH}} = 1/4 \) and the contrast \( \alpha = 1/4 \). Fig. 5(a)–(c) are shadow 1, shadow 2, shadow 3, respectively. Fig. 5(d)–(f) show that we cannot get any information when stacking any two shadows. Fig. 5(g) is the recovered image. We observe that the shadow size is not expansible from the following figures.

**Example 6.** For a \((4,4)\) ProbVSS scheme, the two white and black sets \( C_0 \) and \( C_1 \) consisting of \( 4 \times 1 \) Boolean matrices are shown below:

\[
C_0 = \{ \mu_{0,0}, \mu_{2,0}, \mu_{4,0} \} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},
\]

\[
C_1 = \{ \mu_{1,1}, \mu_{3,1} \} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.
\]

The sets \( \lambda \) and \( \gamma \) will be \( \lambda = \{0,1,1,1,1,1\} \), \( \gamma = \{1,1,1,1,1,1,1,1\} \) when stacking these four

![Fig. 5. The (3,3) ProbVSS 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, (g) shadow 1 + shadow 2 + shadow 3.](image-url)
shadows. \( P_0 = 1/8, \) \( p_1 = 0, \) and the threshold probability \( p_{TH} = 1/8 \) and the contrast \( \alpha = 1/8. \)

### 3.4. A general k-out-of-n ProbVSS scheme

In this section, we show a method to easily construct the \((k, n)\) ProbVSS scheme on a basis of conventional VSS schemes (Naor and Shamir, 1995; Drost, 1996; Katoh and Imai, 1996; Atienzie et al., 1996a, 1996b; Verheul and Van Tilborg, 1997; Eisen and Stinson, 2002). Our scheme has the appearance probabilities of white color \( p_0 = \frac{h}{m} \) and \( p_1 = \frac{l}{m} \) in white and black areas, where parameters \( h \) and \( l \) are the “whiteness” of white and black pixel and \( m \) is the shadow size of the conventional \((k, n)\) VSS scheme. Now the threshold probability and the contrast will be \( p_{TH} = \frac{h}{m} \) and \( \alpha = \frac{h-l}{m}. \)

Before describing the construction, we define a new matrix operation that will be used in our construction, Transfer operation \( T(\cdot) \), as follows. Let \( B = [b_{ij}] \) be an \( n \times m \) Boolean matrix, where \( 1 \leq i \leq n \) and \( 1 \leq j \leq m. \) Then \( T(B) \) is transferred to a set of “\( m\)” \( n \times 1 \) column matrices

\[
\begin{bmatrix}
[b_{11}] & [b_{12}] & ... & [b_{1m}] \\
[b_{21}] & [b_{22}] & ... & [b_{2m}] \\
... & ... & ... & ...
\end{bmatrix}
\]

**Construction 4.** Let \( B_0 \) and \( B_1 \) be the two \( n \times m \) white and black matrices, respectively, as defined in the conventional \((k, n)\) VSS scheme. The parameters are the shadow size \( m, \) the Hamming weight of “OR”-ed \( V \) of any \( k \) of the \( n \) rows in white (resp. black) matrix is \( m - h \) (resp. \( m - l \)) and \( h > l. \) Then, a \((k, n)\) ProbVSS scheme has two white and black sets consisting of \( n \times 1 \) column matrices \( C_0 = T(B_0) \) and \( C_1 = T(B_1). \)

**Theorem 4.** The scheme from Construction 4 is a \((k, n)\) ProbVSS scheme with non-expansible shadow size and the parameters threshold probability \( p_{TH} = \frac{h}{m} \) and the contrast \( \alpha = \frac{h-l}{m}. \)

**Proof.** Since the two sets are \( C_0 = T(B_0) \) and \( C_1 = T(B_1), \) so when “OR”-ed any \( k \) rows,

\[
\lambda = \left\{ L \left( \begin{bmatrix} b_{i1} \\ b_{i1} \\ b_{i2} \\ \vdots \\ b_{i1} \end{bmatrix} \right), \ldots, L \left( \begin{bmatrix} b_{i1} \\ b_{i2} \\ b_{i3} \\ \vdots \\ b_{im} \end{bmatrix} \right) \right\},
\]

where the column matrix \( \in T(B_0) = \{0, \ldots, 0, \underbrace{1, \ldots, 1}_{m-l}, \ldots, \underbrace{1, \ldots, 1}_{m-l} \}, \) and \( \gamma = \{0, \ldots, 0, \underbrace{1, \ldots, 1}_{m-l}, \ldots, \underbrace{1, \ldots, 1}_{m-l} \}. \) The appearance probabilities of white color in \( \lambda \) and \( \gamma \) are \( p_0 = \frac{h}{m} \) and \( p_1 = \frac{l}{m}, \) the threshold probability \( p_{TH} = \frac{h}{m} \) and the contrast \( \alpha = \frac{h-l}{m}. \)

For a proof of the third condition “security”, note that the basic properties of \( B_0 \) and \( B_1 \) in \((k, n)\) VSS scheme are that any \( q < k \) rows of \( \{ \text{all the matrices obtained by permuting the columns of } B_0 \} \) or \{ all the matrices obtained by permuting the columns of \( B_1 \) \} contain the same matrices with the same frequencies. So, consider the two sets \( C_0 \) and \( C_1 \) if “OR-ed” any \( q \) rows of the column matrices in these two sets. Then, the appearance probabilities of the white color in the sets \( \lambda \) and \( \gamma \) are the same. That is, one cannot see anything from the shadow. \( \square \)

**Example 7.** For a Shamir’s \((3, 4)\) VSS scheme with white and black matrices

\[
B_0 = \begin{bmatrix}
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}
\]

and

\[
B_1 = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0
\end{bmatrix}
\]

The \((3, 4)\) ProbVSS scheme can be constructed using Construction 4 as follows:
In a conventional VSS scheme it is guaranteed that for every black and white pixel of the original picture the stacked picture contains a clear difference: e.g., in a (2,2) VSS scheme every black pixel is encoded by 2 black sub pixels while every white pixel is encoded by 1B1W sub pixels. The brighter side $R_0$ in Fig. 2(a) shows 1B1W sub pixels in every original pixel. In a ProbVSS scheme, this is not guaranteed: e.g., in a (2,2) ProbVSS scheme although a black pixel will be encoded by one black pixel with probability $p_1 = 1$, a white pixel will be encoded by a white pixel only with probability $p_0 = 1/2$. Compare Fig. 2(a) and (b), the boundary between $R_0$ and $R_1$ in Fig. 2(b) is interfered from the probabilistic nature of our ProbVSS scheme. Thus the probabilistic nature will diminish the reliability of the scheme as perceived by the human visual system. The disadvantage of our method is that details of the picture are not recognizable to the human visual system, if they do not consist of enough pixels.

Hence, the probability that small areas of the image cannot be recognized is not neglected. In this section, we give a discussion on how many pixels in a black or white area of the secret image are needed for recognizing the color. Let $X_1, X_2, \ldots, X_N$ be random variables (i.e., $N$ pixels and each having the same probabilities $p_0$ (resp. $p_1$) of white pixels in white (resp. black) area). Then the sum $S_N = X_1 + X_2 + \cdots + X_N$ is binomially distributed with parameters $N$ and $p_i$. The mean and variance of $S_N$ is easily calculated as $\mu_i = N \times p_i$ and $\sigma_i^2 = N \times p_i \times (1 - p_i)$, $i = 0, 1$.

Because we want to recognize details of the picture, hence the priori probability of pixel (i.e., white or black) distribution in the secret image is not major interference of our recognition but the shape and size of black or white areas will affect the recognition. For example, if there are two secret images with black background, one is 200×200 pixels and the other is 400×400 pixels. Both of them have one white rectangle (50×50 pixels) located in the center. The clearness of the recovered image will be same using our ProbVSS scheme. Therefore, for discussing on how to distinguish the black and white areas, we use two black and white areas with same size. If the number of white pixels in white area is more than the black area with very high probability, we say that the area can be recognized.

For example, for two black and white areas each having 100 pixels in our (2,3) ProbVSS scheme (Example 2, $p_0 = 1/2$ and $p_1 = 1/6$) the mean of white pixels in white area is $\mu_0 = 100 \times 1/2 = 50$ and its variance is $100 \times 1/2 \times 1/2 = 25$ (i.e., standard deviation is $\sigma_0 = 5$). For the black area with 100 pixels, $\mu_1 = 100 \times 1/6 = 16.7$ and
\[ \sigma_1 = 3.7. \] Fig. 6 shows these two binomial distributions and the solid lines are their normal approximations.

Consider the normal distribution with mean \( \mu \) and standard deviation \( \sigma \). Then, about 99.73% of all values fall within three standard deviations of the mean, i.e., \( \mu \pm 3\sigma \) will contain about 99.73% of the data. This property is called as Empirical Rule. From Fig. 6, we know that for our data. This property is called as Empirical Rule.

Therefore, it is reasonable to use \( \mu_0 - 3\sigma_0 > \mu_1 + 3\sigma_1 + N_d \) as the recognition criterion, where \( N_d \) is the minimum difference of white pixels between white and black areas (the size is \( N \) pixels) that one can distinguish the “black” and “white”. Assume that two black and white areas each having \( N \) pixels and \( N_d = N \times d \), where \( 0 < d < (p_0 - p_1) \).

We have \( Np_0 - 3\sqrt{Np_0(1-p_0)} > Np_1 - 3\sqrt{Np_1(1-p_1)} + N \times d \) and finally we can get the lower bound of \( N \) that one can distinguish the black and white area for the ProbVSS scheme as the following:

\[
N > 9 \left( \frac{\sqrt{p_0(1-p_0)} + \sqrt{p_1(1-p_1)}}{p_0 - p_1 - d} \right)^2.
\]

For the (2, 2) \((p_0 = 1/2 \text{ and } p_1 = 0)\), (2, 3) \((p_0 = 1/2 \text{ and } p_1 = 1/6)\), and (3, 3) \((p_0 = 1/4 \text{ and } p_1 = 0)\) ProbVSS schemes, the lower bound of \( N \) for different values of \( d \) is shown in Table 1. For example, if one can distinguish the black and white areas when \( N_d = N/10 \), i.e., \( d = 0.1 \), the requirement of small area for the (2, 3) ProbVSS scheme is 126 pixels at least.

Fig. 7 shows that the white small areas for both conventional (2, 2) VSS schemes (the left side) and (2, 2) ProbVSS schemes (the right side) cannot be recognized clearly. From Fig. 8(a)-(c), it is observed that when the size of the white area is large, we can get the clearer secret image. So, if we select the secret image more carefully and satisfy the lower bound of \( N \), we can get the recovered secret image using our probabilistic method; even the boundary of black and white area in our recovered image is interfered due to the probabilistic nature of the pixel.

### Table 1

<table>
<thead>
<tr>
<th>Types of ProbVSS schemes</th>
<th>(2, 2)</th>
<th>(2, 3)</th>
<th>(3, 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d = 0.00 )</td>
<td>9</td>
<td>62</td>
<td>27</td>
</tr>
<tr>
<td>( d = 0.05 )</td>
<td>12</td>
<td>85</td>
<td>43</td>
</tr>
<tr>
<td>( d = 0.10 )</td>
<td>15</td>
<td>126</td>
<td>75</td>
</tr>
<tr>
<td>( d = 0.15 )</td>
<td>19</td>
<td>203</td>
<td>169</td>
</tr>
<tr>
<td>( d = 0.20 )</td>
<td>25</td>
<td>384</td>
<td>675</td>
</tr>
<tr>
<td>( d = 0.25 )</td>
<td>36</td>
<td>981</td>
<td>–</td>
</tr>
<tr>
<td>( d = 0.30 )</td>
<td>57</td>
<td>6131</td>
<td>–</td>
</tr>
<tr>
<td>( d = 0.35 )</td>
<td>100</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>( d = 0.40 )</td>
<td>225</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>( d = 0.45 )</td>
<td>900</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

### 4. Contrast of the ProbVSS scheme

For conventional VSS schemes, the pixel is represented as \( m \) sub pixels. One can distinguish the black and white color in the recovered image because every \( m \) sub pixels in black area will have more black sub pixels than in white area. According to the code book of our constructions, we randomly choose one \( n \times 1 \) column matrix in \( C_0 \) (resp. \( C_1 \)) to represent a white (resp. black) pixel, if the element in this column matrix is “0” we use white pixel otherwise black pixel. Hence, for our proposed ProVSS scheme, the pixel is not extended but only transferred to black or white pixel. The frequency of white pixels in white area is higher than that in black area, so we can see the contrast
of the black and white in the recovered image. The concept of these two methods seems to be the same but the conventional VSS scheme is deterministic and our scheme is probabilistic. “Deterministic” means that we can decide that the pixel (m sub pixels) is black (“m − l”B“l”W) or white (“m − h”B“h”W). “Probabilistic” means that we cannot decide whether the pixel is black or white but only know that there will be nearly \( \frac{h \times 100}{m} \) % white pixels and nearly \( \frac{l \times 100}{m} \) % white pixels in white area and nearly \( \frac{m - h \times 100}{m} \) % black pixels and \( \frac{m - l \times 100}{m} \) % black pixels in black area, i.e., we can distinguish the black and white areas.

In this section, we use these three ProbVSS schemes to test the contrast of the recovered image. Fig. 8(a)–(c) show the recovered images for \((2,2)\) (Example 1), \((2,3)\) (Example 2), and \((3,3)\) (Example 5) ProbVSS schemes, respectively. The contrast for each scheme is \( \alpha_{(2,2)} = 1/2 \), \( \alpha_{(2,3)} = 1/3 \) and \( \alpha_{(3,3)} = 1/4 \), where the subscript denotes the scheme type.

From the above figure, it is observed that Fig. 8(a) is the clearest in these three images. However, Fig. 8(b) and (c) have almost the same clearness, but the value of \( \alpha_{(3,3)} = 1/4 \) is even less than \( \alpha_{(2,3)} = 1/3 \). It is inadequate now because the value of contrast is not consistent with the recovered image. The contrast \( \alpha \) of our ProbVSS scheme is defined as \( \alpha = p_0 - p_1 \). Therefore, we need to modify the contrast to consist with the real situation.

First, we introduce the former definitions of contrast in conventional VSS schemes. The quality of the recovered image in a conventional VSS scheme is usually called contrast. Since the original black or white pixel 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 but there is no consensus on the definition of contrast. Naor and Shamir defined contrast as \( \alpha_{NS} = \frac{h}{m} \) (Naor and Shamir, 1995). Verheul and Van Tilborg demonstrated 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 two different levels of clearness in the recovered images. They gave the new contrast as \( \alpha_{VV} = \frac{h - l}{m[h + l]} \) (Verheul and Van Tilborg, 1997). When \( l = 0 \), \( \alpha_{VV} \) is always \( 1/m \). In fact, for larger \( h \) the recovered image is clearer. The definition of \( \alpha_{VV} \) does not seem to be reasonable. Recently, Eisen and Stinson improved the previous disadvantages and defined their contrast as \( \alpha_{ES} = \frac{h - l}{m + l} \) (Eisen and Stinson, 2002).
Table 2

The contrast $\alpha$ for the ProbVSS schemes

<table>
<thead>
<tr>
<th>Types of ProbVSS schemes</th>
<th>$(2,2)$</th>
<th>$(2,n)$</th>
<th>$(3,n)$</th>
<th>$(k,k)$</th>
<th>$(k,n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contrast $\alpha$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{n+1}{5n-1}$</td>
<td>$\frac{n^2}{2n-1}$</td>
<td>$\frac{1}{2^{k-1}}$</td>
<td>$\frac{h/m - l/m}{1 + l/m}$</td>
</tr>
<tr>
<td>$n$ odd</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{5n-1}$</td>
<td>$\frac{1}{2^{k-1}}$</td>
<td>$\frac{h/m - l/m}{1 + l/m}$</td>
<td></td>
</tr>
<tr>
<td>$n$ even</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2n-2}$</td>
<td>$\frac{1}{2^{k-1}}$</td>
<td>$\frac{h/m - l/m}{1 + l/m}$</td>
<td></td>
</tr>
</tbody>
</table>

The superscript * and ** denote that Constructions 2 and 3 are used. The others mean that our construction has the same matrices as using the conventional VSS scheme and Transfer operation $T(\cdot)$.

A new contrast is defined by our observation of the real results. We also use the methodology to define the contrast of the ProbVSS scheme and make sure that the definition of contrast is consistent with the recovered image. By using the similar definition of $\alpha_{ES}$,

$$\alpha_{ES} = \frac{h - l}{m + l} = \frac{(h - l)/m}{(m + l)/m} = \frac{h/m - l/m}{1 + l/m},$$

the contrast of our ProbVSS $\alpha$ is defined as $\alpha = \frac{n^{n^2} \cdot p_2}{1 + p_1}$.

For $(2,2)$, $(2,3)$ and $(3,3)$ ProbVSS schemes, the new contrasts are $\alpha_{(2,2)} = 1/2$, $\alpha_{(2,3)} = 2/7$ and $\alpha_{(3,3)} = 1/4$. Note that the value $\alpha_{(2,3)}$ is now near to $\alpha_{(3,3)}$. The contrast $\alpha$ for different ProbVSS schemes is shown in Table 2.

For example, if we use Naor and Shamir’s $(2,3)$ VSS scheme to construct a $(2,3)$ ProbVSS scheme. Then,

$$C_0 = T(B_0) = T\left(\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}\right) = \{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}\},$$

and

$$C_1 = T(B_1) = T\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right) = \{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}\}. $$

The contrast $\alpha = \frac{2^{3-1/3}}{1+1/3} = 1/4$. In Example 2, when Construction 2 is used, the contrast is $\frac{1/2 - 1/6}{1 + 1/6} = 2/7$. Example 4 uses Construction 3, and the contrast is improved to $\frac{1/3 - 0}{1 + 0} = 1/3$.

5. Conclusion

In this paper, we have presented new $(k,n)$ ProbVSS schemes with non-expansible shadow size based on the probabilistic method. Our method has the same contrast level as the conventional VSS scheme. Moreover, we also demonstrated that the conventional VSS scheme can be transferred to ProbVSS scheme by using Transfer operation $T(\cdot)$. The ProbVSS scheme is a different view of the conventional VSS scheme.

Acknowledgements

The author wishes to thank the anonymous reviewers for their many valuable suggestions and comments.

References


