Some New Types of Visual Secret Sharing Schemes

Ching-Nung Yang
Department of Computer Science & Information Engineering,
National Dong Hwa University,
TEL: (03)8662500 Ext-22120
FAX: (03)8662781
E-mail: cnyang@csie.ndhu.edu.tw

Chi-Sung Laih
Communication Labarotory,
Department of Electrical Engineering,
National Cheng Kung University,
TEL: (06)2757575 Ext-62369
FAX: (06)2345482
E-mail: laihcs@eembox.ncku.edu.tw

Abstract

Visual secret sharing(VSS) scheme [1] is used to protect the visual secret by send ing n transparencies to different participants such that k -1 or fewer of them have no information about the original image, but the image can be seen by stacking k or more transparencies. In this paper, we propose some new types of VSS schemes for differen t applications, and also show that VSS schemes could be interestingly applied to some real systems for identification. The new schemes include a VSS scheme which has the ability to detect the forged transparencies, a (1→n) VSS scheme which can share n-1 secret images, and a new (2, n) scheme with large number of shadows than the previously proposed (2, n) scheme for the same share size. We also show that a hierarchical scheme is possible and easy for VSS scheme.

Index Terms – Visual cryptography, secret sharing scheme.

1 Introduction

For most cryptosystems, it is needed to protect many important secrets, such as encryption and decryption keys or passwords while they are used to protect the sensitive data or log in the server. We usually use a single -master key to protect these encryption and decryption keys. An interesting problem is how to protect this single master key. In 1979, Blakley[7] and Shamir[8] independently introduced the concept of secret sharing scheme(or sometimes referred as threshold scheme) to solve the master key sharing problem. The (k, n) threshold scheme is a scheme which is designed to break the single master key to n different shadows, such that the master key is recoverable from any $k(k \leqq n)$ shadows and knowledge of k-1 or fewer shadows provide absolutely no information about the master key. Since the concept of (k, n) threshold scheme was introduced by Blakely and Shamir , several algorithms and various researches have been proposed in the literature [9].

In the basic secret sharing schemes, all the schemes need complex algorithms to generate the shadows and recover the secrets. For example : Blakely's scheme[7] is a probabilistic approach based on *linear projective geometry*, Shamir's sch eme[8] is based on *Lagrange interpolating polynomials*, and Asmuth-Bloom scheme[10] is a method based on *Chinese Remainder Theorem*, ..., and therefore when someone uses the secret sharing scheme, he needs the knowledge of cryptography and the cryptographic computations to get the share secret. Thus, the computer or the other hardware is needed when using secret sharing schemes.

A new type of secret sharing scheme [1] -[6], [13]~[18],[21]called visual secret sharing(VSS) scheme, is firstly introduced by Naor a nd Shamir in 1994. The key concept of VSS scheme is that the original shared secret is image (printed text, handwritten notes, pictures, etc.), and the decoder for this VSS scheme is "*eyes*" of human being, i.e., the shared secret is decoded directly by the human visual system. To decrypt the secret image the reader should xerox each random pattern, called share, on a separate transparency and then recover the secret image by stacking some of transparencies. Next we quote a statement from the introduction in [1] below to know how to work for VSS scheme in real application : " *To decrypt the secret image , the reader should photocopy each pattern on a separate transparency, align them carefully, and project the result with an overhead projector.*" . In this paper, we present some new types of VSS schemes and show the new applications of VSS schemes.

This paper is organized as follows. In Section 2, we will propose some real applications of VSS schemes. Section 3 gives a brief review of the (k, n) VSS scheme. In section 4, we present some new types of VSS schemes. Section 5 concludes the paper.

2 New applications of VSS schemes

The revealed image in [1]-[6], can not be recognized clearly because all results were shown by the transparencies. The projected image on the screen will be damaged due to the copied transparency and the lumens of the overhead projector. So for real application (k, n) VSS scheme using transparency as the shadow material is not practical. The revealed image will be more indistinguishable for large k, such as 4, 5, or more, due to the alignment of these transparencies.

From the above descriptions, we know that although VSS scheme is a good concept (i.e, the decoder is easy); however, it is not a good idea from the viewpoint of applications to use transparency as shadow. Here, we use *image editing package* , such as Adobe Photoshop™ or a simple accessory Microsoft Mspaint, to replace the overhead projector and stack the pictures(shadows) directly in the computer and the shared picture will be show n on monitor. In this time, we still do not need the knowledge of cryptography and cryptographic computations to get the shared secret, but just use the simple feature of the *image editing package*. It herein has the same simplicity like that

of the origina l visual cryptographic scheme using transparency.

In this paper, we point out that VSS scheme will be a good and easy tool to share the secret through Internet. The following figures show an authentication example by using the technology in [1]. Figure 1(a) shows the log in user ID, Figure 1(b) is the corresponding key in the local server, and by stacking Figure 1(a) and 1(b) with *image editing package*, the user's pass word can be got and shown in Figure 1(c). The server verifies the right pass word, and then believes that the user is a legitimate subscriber. If we add the key in the shared secret, then the communication between server and subscriber can be encrypted with this session key [19],[20].

What can be imaged can be achieved. The wide applications of VSS scheme can be found anywhere. In this section, we will show some interesting applications of VSS scheme for identification. In fact, we have tried to apply VSS scheme as the eye shield screen which is originally used in UV protections for our eyes a gainst monitor. The protection screen can also be used to prevent attacker to peep at the decoded image on the monitor. Since there is a space between eye shield screen and monitor, it is a some kind of limiting the visible secret sharing(LVSVSS) schemes [4], and due to the space, the LVSVSS scheme is secure against peeping.

We can furthermore apply the concept to mobile phone handsets for enhancing the security of wireless mobile network, by manufacturing a thin film and covered on the LCD monitor of Handset [22]. First, the mobile network operator makes a thin film and gives it to the mobile station(MS) secretly. Then, makes a random image so that a challenge (pass word) can be decoded when the random image shown on the monitor covered on the thin film. In identification process, the MS decodes the challenge by the human sight of user, and then user key in the password and return it to the network side. Finally, the network operator verifies the MS. The scheme uses simple challenge-response protocol [4], [1 1], [19],[20]so that the user can make response by themselves. Moreover, the thin film covered on the LCD display of handset has the following benefits: "easy",(2) "low price",(3) "passive device", and "updated quickly".

3 The basic VSS scheme

A (k, n) VSS scheme is a method by which the shared image(printed text, handwritten notes, pictures, etc.) is visible by k or more participants with stacking their transparencies(or pictures) with the help of overhead projector(or *image editing package*) [1]-[6]. However, k-1 or fewer of them can not see the original shared image.

If the smallest graphic unit in an original black/white picture is called pixel, then the key concept of VSS scheme is to transform the pixel to m sub pixels. For a (k, n) VSS scheme, the dealer produces n transparencies and each pixel in transparency contains m sub pixels. So, the m sub pixels in n transparencies can be represented as $n\times m$ Boolean matrix $S=[s_{ij}]$, where $s_{ij}=1$, if and only if the j-th sub pixel of the i-th transparency is black. The grayness of q stacked transparencies $\{i_1, i_2, \ldots, i_q\}$ is proportional to the Hamming weight of the "OR" of the corresponding rows $i_1, i_2, \ldots, i_q$ of S. The grayness can be decoded as white(or black) by human sight if the Hamming weight of corresponding stacked rows no greater than d-αm(or no less than d), where "d"($1 \leqq d \leqq m$) is the threshold value and "α"($\alpha>0$) is the relative difference. The basic model of (k, n) VSS scheme is shown in Figure 2.

The required conditions of basic (k, n) VSS scheme :
Let C_W and C_B be two collections of $n\times m$ Boolean matrices. The dealer rand omly chooses one of the matrices in C_W(resp. C_B) to share a white(resp. black) pixel; a (k, n) VSS scheme satisfies the following conditions where Condition C1 is called *contrast* and Condition C2 is called *security*(see also [1]) :

C1. For any S in C_W(resp. C_B), the "OR" of any k of the n rows has a Hamming weight of at most d-αm(resp. at least d).

C2. 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 C_i, $i \in \{W, B\}$, 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.

In [2], Droste proposed an efficient (k, n) VSS scheme with the small share size m (i.e., the number of column in share matrix C_W and C_B). For example, the size m of a (4, 7) scheme needed in [1] is at least 19208(using *Galois fields*) or 2^{45}(using a small-bias probability space), and then is instead of m=35 now. Katoh and Imai also have the same results as [2] (see Table 1 i n [2] and Table 3 in [3]) by using different method.

The conventional (k, n) VSS schemes need k or more shadows to reveal the one secret image. In [5], [6], Ateniese et al have presented visual cryptography schemes for general access structures, where an access structure is a specification of all qualified and forbidden subsets of participants. The sets in qualified sets can share one secret image. Droste [2] also proposed a S-extended n out of n scheme based on the basic (k, k) scheme in [1]. It is a general method to share specified images for specified groups of participants, i.e., more than one secret image can be shared by participants in any qualified subsets of {1,2, ..., n}. The share size for S-extended n out of n scheme is $m=\sum_{q=1}^{n} 2^{q-1} b_q$, where b_q is the number of elements of S containing exactly q elements.

4 Some new types of VSS schemes

4.1 A VSS scheme with the ability to detect forged shadows

In conventional secret sharing schemes, there are many methods to overcome the problem when the shadows are forged or corrupted by errors [10], [12]. Same as the conventional secret sharing schemes, VSS schemes may be used in the circumstances that the participants are mistrustful. In this case we need a VSS scheme which has the ability to detec t the forged shadows. The conventional (k, n) VSS schemes in [1] -[6] are insecure when the mistrustful participants are involved. Here, a VSS scheme is proposed to overcome this problem when the shadows are forged.

Approach 1 : With trusted authority(denoted by TA)

In this approach, we consider that we will have TA that is responsible for such things as verifying the identities of users, holding a check shadow, ..., etc. There is a direct and trivial method to overcome this problem by using Droste {{1, 2}={1, 3}= ...={1, n}, any subset {i_1, i_2, ..., i_q} of {2, 3, .., n+1} with $q>k$}-extended n+1 out of n+1 scheme to construct a (k, n) scheme with the ability of detecting forged shadows. The first secret image can be seen when the first shadow is stacked with the other shadow, and the second secret image is recovered from any stacked k or more shadows of {2, 3, ..., n+1}. The first shadow can be hold in TA, and used for distinguishing the identification of user. However, there is a large share size $m=2\times\binom{n}{2}+\sum_{q=k}^{n+1}2^{q-1}b_q$.

Construction 1 : Let C_i={all the matrices obtained by permuting the columns of S_i}, $i\in\{W, B\}$, be the two $n\times m$ matrices as defined in conventional (k, n) VSS scheme. Then, a new (k, n) VSS scheme with detecting forged shadows has the following four $(n+1)\times(m+2)$ matrices C_{ij}, i, $j\in\{W, B\}$. A share matrix derived from C_{WW} reconstruct the white pixels of the first secret image (used for verification) and the second secret image (the original shared secret of (k, n) scheme), ..., etc. C_{ij}, i, $j\in\{W, B\}$, matrices are defined as the following :

C_{WW}={all the matrices obtained by permuting the

columns of $\left[\begin{array}{c|c} 10 & 0\ldots0 \\ 10 & \\ \vdots & S_W \\ 10 & \end{array}\right]$},

C_{WB}={all the matrices obtained by permuting the

columns of $\left[\begin{array}{c|c} 10 & 0\ldots0 \\ 10 & \\ \vdots & S_B \\ 10 & \end{array}\right]$},

C_{BW}={all the matrices obtained by permuting the

columns of $\left[\begin{array}{c|c} 10 & 0\ldots0 \\ 01 & \\ \vdots & S_W \\ 01 & \end{array}\right]$},

C_{BB}={all the matrices obtained by permuting the

columns of $\left[\begin{array}{c|c} 10 & 0\ldots0 \\ 01 & \\ \vdots & S_B \\ 01 & \end{array}\right]$}.

The proofs that C_{WW}, C_{WB}, C_{BW}, and C_{BB} are white/white, white/black, black/white, and black/black share matrices are straightforward and will be omitted.

Then, every shadow of {2, 3, ..., n+1} is delivered to each participant and the first shadow is hold in TA which is used to detect the forged shares of {2, 3, ..., n+1}. Although the weight of first row in matrix is different to the other rows, however, the weight of rows in matrices for black share and white share in one shadow are always equal, so it satisfies the security.

Example 1 : For a (2, 4) VSS scheme with TA of the ability to detect forged shadows, the matrices are defined as the following :

C_{WW}={all the matrices obtained by permuting the

columns of $\begin{bmatrix} 1&0&0&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&1&0&0&0 \end{bmatrix}$},

C_{WB}={all the matrices obtained by permuting the

columns of $\begin{bmatrix} 1&0&0&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&0&1&0&0 \\ 1&0&0&0&1&0 \\ 1&0&0&0&0&1 \end{bmatrix}$},

C_{BW}={all the matrices obtained by permuting the

columns of $\begin{bmatrix} 1&0&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&1&1&0&0&0 \\ 0&1&1&0&0&0 \\ 0&1&1&0&0&0 \end{bmatrix}$},

C_{BB}={all the matrices obtained by permuting the

columns of $\begin{bmatrix} 1&0&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&1&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&1&0&0&0&1 \end{bmatrix}$}.

The five shadows {1}, {2}, {3}, {4}, and {5} are shown as Figure 6(a)~ Figure 6(e). When copied on transparencies and stacked carefully (or scanned to the computer and stacked with *image editing package*), one can reveal the above two images.

Approach 2 : Without TA

In some cases, we will not have a TA for verification. For example, if we do not want to use an on-line TA server, then we are forced to do the verification of users by ourselves. In this section, we propose a (2, k, n) VSS scheme which has the ability to detect forged shadows without the help of TA, where $k\geqq3$. The scheme can share two secret images, the first secret image can be used for verification and can be revealed from every two shadows. The second shared information can be recovered from k or more shadows.

Construction 2 : Let C_W and C_B be the two $n\times m$ matrices, as defined in *Construction 1*. Then, a new (k, n) VSS scheme with detecting forged shadows without TA has the following four $n\times(m+2\times\binom{n}{2})$ black/white matrices C_{ij}={all the matrices obtained by permuting the columns of S_{ij}}, i, $j\in\{W, B\}$. A share matrix derived from C_{WW} reconstructs the white pixel of the first secret image (used for verification) and the second secret image (the original

shared secret of (k, n) scheme), and the share matrix derived from C_{WB} reconstruct the white pixel of the first secret image and the black pixel of the second image, ..., etc.

S_{ij}, $i, j \in \{W, B\}$ matrices are defined as the following :

$$S_{WW}=\left[\begin{array}{cccc|c} 10 & 10 & \cdots & 11 & \\ 10 & 11 & \cdots & \vdots & \\ 11 & 10 & \cdots & \vdots & S_W \\ \vdots & 11 & \cdots & 11 & \\ \vdots & \vdots & \cdots & 10 & \\ 11 & 11 & \cdots & 10 & \end{array}\right], S_{WB}=\left[\begin{array}{cccc|c} 10 & 10 & \cdots & 11 & \\ 10 & 11 & \cdots & \vdots & \\ 11 & 10 & \cdots & \vdots & S_B \\ \vdots & 11 & \cdots & 11 & \\ \vdots & \vdots & \cdots & 10 & \\ 11 & 11 & \cdots & 10 & \end{array}\right],$$

$$S_{BW}=\left[\begin{array}{cccc|c} 10 & 10 & \cdots & 11 & \\ 01 & 11 & \cdots & \vdots & \\ 11 & 01 & \cdots & \vdots & S_W \\ \vdots & 11 & \cdots & 11 & \\ \vdots & \vdots & \cdots & 10 & \\ 11 & 11 & \cdots & 01 & \end{array}\right], S_{BB}=\left[\begin{array}{cccc|c} 10 & 10 & \cdots & 11 & \\ 01 & 11 & \cdots & \vdots & \\ 11 & 01 & \cdots & \vdots & S_B \\ \vdots & 11 & \cdots & 11 & \\ \vdots & \vdots & \cdots & 10 & \\ 11 & 11 & \cdots & 01 & \end{array}\right].$$

Theorem 1 : The scheme from Construction 2 is a VSS scheme which has the ability to detect the forged shadows without TA.

Proof : The "OR"ed any two rows of S_{WW} and S_{WB} is a row vector [$2\times\binom{n}{2}$-tuple with weight $2\times\binom{n}{2}$-1 | "OR"ed 2 rows of S_W], and [$2\times\binom{n}{2}$-tuple with weight $2\times\binom{n}{2}$-1 | "OR"ed 2 rows of S_B], respectively. The "OR"ed any two rows of S_{BW} and S_{BB} is a row vector [$2\times\binom{n}{2}$-tuple with weight $2\times\binom{n}{2}$ | "OR"ed 2 rows of S_W], and [$2\times\binom{n}{2}$-tuple with weight $2\times\binom{n}{2}$ | "OR"ed 2 rows of S_B], respectively, where the line "|" is same as matrices S_{ij}. Since $S_W(S_B)$ is white(black) share matrix of (k, n) scheme for $k\geqq 3$, so S_{WW} and S_{WB} are white share matrix and S_{BW} and S_{BB} are black share matrix for every two shadows stacked. Similarly, The "OR"ed any $k(\geqq 3)$ rows of S_{WW} and S_{BW} is [1...1 | "OR"ed k rows of S_W], and The "OR"ed any k rows of S_{WB} and S_{BB} is [1...1 | "OR"ed k rows of S_B]. Thus, it is just a (k, n) scheme with the parameters m'(share size), d'(threshold value), and α'(relative difference) as $m'=m+2\times\binom{n}{2}$, $d'=d+2\times\binom{n}{2}$ and $\alpha'=1/m'$, where m and d are parameters of the original (k, n) scheme.

□

In fact, the above proposed construction is a method using a combination of the two processes(S-extended n out of n schemes in [2] and (k, n) scheme). Then for every shadow of {1, 2, ..., n} is delivered to participants. The first secret image can be seen when every two shadows are stacked, and the second secret image is recovered from any stacked k or more shadows of {1, 2, ..., n}.The Hamming weights of rows of the four matrices in one shadow are equal, so the construction satisfies the security.

A visual (2, 3, 3) scheme in [3] is a special case of our (2, k, n) VSS scheme when k=n=3. Actually, one can use the above construction to design a (2, 3, 3) scheme proposed in [3]. For example, S_{WW} constructed as the following :

$$S_{WW}=\left[\begin{array}{cccccc|cccc} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{array}\right]$$ is same as S_{WW} in [3].

4.2 A visual (1→n) secret sharing scheme

In this section, we construct a (1 →n) VSS scheme. The notation (1 →n) means that the following qualified sets {1}, {1, 2}, {1, 2, 3}, ..., {1, 2, 3, 4, ..., n} can reveal different images. The scheme can share n-1 secret images, step by step. The first shadow containing an arbitrary image can share the first secret image when stacked with the second shadow. Then stack the third shadow to the first secret image to get the second secret image, add the other shadow in series (shadow 3, shadow4, ...), we can get other shared secret images each time when stacked with a new shadow.

Construction 3 : Let $S_W^{(u,u)}$ and $S_B^{(u,u)}$ be two $u\times 2^{u-1}$ white and black share matrices for (u, u) VSS scheme, and $S_{W...}^{(1\to u)}$ (resp. $S_{B...}^{(1\to u)}$) of a (1→u) VSS scheme be the share matrix which we can reconstruct a white(resp. black) pixel for the u-th secret image from this matrix. Then, $S_{WW...}^{(1\to u+1)}$, $S_{WB...}^{(1\to u+1)}$, $S_{BW...}^{(1\to u+1)}$, and $S_{BB...}^{(1\to u+1)}$ of a (1→u+1) VSS scheme are defined recursively by $S_W^{(1\to 1)}$=[0] and $S_B^{(1\to 1)}$=[1] as follows.

$$S_{WW...}^{(1\to u+1)} = \left[\begin{array}{c|c} S_W^{(u+1,u+1)} & \begin{array}{c} 1\cdots 1 \\ \\ S_{W...}^{(1\to u)} \end{array} \end{array}\right]$$

$$S_{WB}^{(1\to u+1)}=\left[\begin{array}{c|c} S_W^{(u+1,u+1)} & \begin{array}{c} 1\cdots 1 \\ \\ S_{B...}^{(1\to u)} \end{array} \end{array}\right],$$

$$S_{BW...}^{(1\to u+1)} = \left[\begin{array}{c|c} S_B^{(u+1,u+1)} & \begin{array}{c} 1\cdots 1 \\ \\ S_{W...}^{(1\to u)} \end{array} \end{array}\right].$$

$$S_{BB...}^{(1\to u+1)}=\left[\begin{array}{c|c} S_B^{(u+1,u+1)} & \begin{array}{c} 1\cdots 1 \\ \\ S_{B...}^{(1\to u)} \end{array} \end{array}\right],$$

where the number of columns of all $S_{WW...}^{(1\to n)}$, $S_{WB...}^{(1\to n)}$, $S_{BW...}^{(1\to n)}$, and $S_{BB...}^{(1\to n)}$ is 2^n-1.

Theorem 2 : The scheme from Construction 3 is a (1 →n) VSS scheme.

Proof : For {1, 2, ..., u+1}, the "OR"ed u+1 rows of $S_{BW...}^{(1\to u+1)}$ and $S_{BB...}^{(1\to u+1)}$ is a row vector ["OR"ed u+1 rows of $S_B^{(u+1,u+1)}$ | 1...1], and the "OR"ed u+1 rows of $S_{WW...}^{(1\to u+1)}$ and $S_{WB}^{(1\to u+1)}$ is a row vector ["OR"ed u+1 rows of $S_W^{(u+1,u+1)}$ | 1...1]. Thus, it is just a (u+1, u+1) VSS scheme with the parameters m(share size), d(threshold value), and α(relative difference) as $m=d=\sum_{q=1}^{u+1} 2^{q-1} = 2^{u+1}-1$, and $\alpha=1/(2^{u+1}-1)$. □

Example 2 : For a (1→3) VSS scheme , the eight 3×7 share matrices are constructed as follows.

$$S_{WWW}^{(1\to 3)} = \begin{bmatrix} 0&1&1&0&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&1&0&0 \end{bmatrix},$$

$$S_{WWB}^{(1\to 3)} = \begin{bmatrix} 0&1&1&0&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&1&0&1 \end{bmatrix},$$

$$S_{WBW}^{(1\to 3)} = \begin{bmatrix} 0&1&1&0&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&0&1&0 \end{bmatrix},$$

$$S_{WBB}^{(1\to 3)} = \begin{bmatrix} 0&1&1&0&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&0&1&1 \end{bmatrix},$$

$$S_{BWW}^{(1\to 3)} = \begin{bmatrix} 1&0&0&1&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&1&0&0 \end{bmatrix},$$

$$S_{BWB}^{(1\to 3)} = \begin{bmatrix} 1&0&0&1&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&1&0&1 \end{bmatrix},$$

$$S_{BBW}^{(1\to 3)} = \begin{bmatrix} 1&0&0&1&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&0&1&0 \end{bmatrix},$$

$$S_{BBB}^{(1\to 3)} = \begin{bmatrix} 1&0&0&1&1&1&1\\ 0&1&0&1&1&0&1\\ 0&0&1&1&0&1&1 \end{bmatrix}.$$

The other two shadows {2} and {3} are shown as Figure 7(a) and Figure 7(b). When copied on transparencies and stacked carefully (or scanned to the computer and stacked with image editing package), one can reveal t he above two images.

In the (1→n) scheme VSS scheme, it is possible to share n-1 secret images one by one (by mail, fax or Internet), by sending one random image with mail, fax or Internet each time.

4.3 An extension of Katoh-Imai (2, n) VSS scheme

In [3], Katoh and Imai proposed a new type of (2, n) VSS scheme which uses the balanced code. A binary code of length m and each codeword has the Hamming weight $\lfloor m/2 \rfloor$ is called balanced code, where $\lfloor m/2 \rfloor$ is the integer part of $m/2$. Katoh-Imai (2, n) VSS scheme uses codewords of a balanced code with semi-distance 4 for the black share matrix S_B and uses anyone codeword of length m and Hamming weight $\lfloor m/2 \rfloor$ as every row of the white share matrix S_W.

The threshold value d and relative difference α of Katoh-Imai (2, n) VSS scheme are $d=\lfloor m/2 \rfloor+p$, and the corresponding $\alpha=p/m$, where $2 \leqq p \leqq \lfloor m/2 \rfloor$, i.e. the Hamming weight of a black pixel is $\lfloor m/2 \rfloor+p$ and the white pixel is $\lfloor m/2 \rfloor$. The number of shadows n is the cardinality of optimal balanced code with semi-distance 4, for example n=14 when m=8.

It is observed that the revealed image is also easily recognized when choosing $\leqq p \leqq \lfloor m/2 \rfloor$(i.e., using the balanced code with the Hamming weight [$m/2$]) accord with the experimental results. The number of shadows is increased significantly using $1 \leqq p \leqq \lfloor m/2 \rfloor$ for the same share size.The number of shadows can be $\binom{m}{\lfloor m/2 \rfloor}$ when the share size is m, because the maximum number of codewords in a balanced code with length m is $\binom{m}{\lfloor m/2 \rfloor}$. Table 1 shows some share sizes of (2, n) VSS scheme for different methods.

The revealed image in the e xtended (2, n) VSS scheme is a little lighter from a comparison of p=1 with p=2. However, its major benefit is a large number of shadows, for example for m=8, any subset of {1, 2, ..., 70} still has the probability of 20%(=14/70) to share a recovered image w ith $p \geqq 2$. The revealed images of the different (2, n) VSS schemes in Table 1 are illustrated in Figure 5 to show that the extended scheme is still acceptable. Note that the revealed image of [5] is same as our system, i.e., $p \geqq 1$, when the share size m is 8 or less.

4.4 A hierarchical VSS scheme

A hierarchical structure for Shamir's threshold scheme [8] is possible, where the number of shadows given to each user is proportional to the user's importance. For example , a president of a company can be given thre e shadows, each vice-president two and so forth. However, in other words, the number of shadows for a VIP user will increase for this case.

VSS scheme has one fantastic property for hierarchical structure, the shadows given to the specified participant can be pre-processed by "OR" operation as a new shadow with the same size of the original one.

Construction 4 : Let C_W={all the matrices obtained by permuting the columns of S_W} and C_B={all the matrices obtained by permuting the columns of S_B} be the two $n\times m$ matrices, respectively, defined in conventional (k, n) VSS scheme, and S_W and S_B shown as below :

$$S_W = \begin{bmatrix} s_W^1 \\ s_W^2 \\ \vdots \\ s_W^n \end{bmatrix}, \text{ and } S_B = \begin{bmatrix} s_B^1 \\ s_B^2 \\ \vdots \\ s_B^n \end{bmatrix},$$

where s_W^i and s_B^i, i=1, 2, ..., n, are all m-tuple row vectors.

A (k, n-l+1) VSS scheme with one VIP user can be done by "OR" any l rows ($S_W^{i_1}$, $S_W^{i_2}$, ..., $S_W^{i_l}$) of S_W and any l rows ($S_B^{i_1}$, $S_B^{i_2}$, ..., $S_B^{i_l}$) of S_B with $2 \leqq l < k$, where i_1, i_2, ..., and i_q are of {1, 2, ..., n} and the value of l is according the importance of the user. Then, the two (n-l+1)×m white and black share matrices for (k, n-l+1) VSS scheme becomes as follows.

$$S_W = \begin{bmatrix} S_W^{i_1} + S_W^{i_2} + \ldots + S_W^{i_l} \\ S_W^{i_{l+1}} \\ \vdots \\ S_W^{i_n} \end{bmatrix}$$,and

$$S_B = \begin{bmatrix} S_B^{i_1} + S_B^{i_2} + \ldots + S_B^{i_l} \\ S_B^{i_{l+1}} \\ \vdots \\ S_B^{i_n} \end{bmatrix}$$, where "+" is the "OR".

The first shadow, as observed from the above construction, is weighting with a factor " l". The first shadow only needs other k-l shadows to recover the secret image, and still has the same size of shadow.

From the descriptions of hierarchical VSS schemes, one can point out a possible scenario that if l sharers stack their shares and publish the reveal image, then only other k-l shadows are needed to recover the secret image. This will damage the security of the (k, n) VSS scheme. How to overcome the lack of security for this situation is also an interesting and open problem.

5. Conclusion

In this paper, we have presented some new types of VSS scheme and the corresponding constructions, such as VSS scheme with detecting fake shadows and (1→n) VSS scheme for different applications. We also give an extension for Katoh-Imai (2, n) VSS scheme which has the large number of shadows for the same share size. Furthermore, we point out that VSS scheme is most suitable for hierarchical structure due to the shadows are stacked directly(i.e., the "OR" operation).

In [1], it is stated that "*transparencies are stacked together(or analyzed by any other method)*". Here, using an image editing package instead of transparencies is a good idea, and thus we will have good performance and make VSS scheme as a practical application to be possible. The "*any other method*" means that VSS may be applied to many fields, such as eye shield screen on monitor (or on the screen of mobile phone handsets), ..., etc. to enhance the security of computer (or wireless mobile network).

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] Kazukuni. Kobara and Hideki Imai, "Limiting the visible space visual secret sharing schemes and their application to human identification," *Advances in Cryptology-ASISCRYPTO'96*, *Lecture Notes in Computer Science* , No.1163, pp.185 -195, Springer-Verlag, 1996.

[5] 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), vi a WWW using http://www.eccc.uni-trier.de/eccc/.

[6] 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.

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

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

[9] G.J. Simmons(Editor), Contemporary Cryptology; The Science of Information Integrity, Chapter 9, *IEEE press*, 1992.

[10] A. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Trans. On Information Theory* , Vol. IT-29.547, pp.208-210, 1983.

[11] T. Matsumoto and Hideki Imai, "Human identification through insecure channel," *Advances in Cryptology-EUROCRYPTO'91*, *Lecture Notes in Computer Science* , No.547, pp.409 -421, Springer-Verlag, 1991.

[12] E.D. Karnin, J.W. Greene and M.E. Hellman, "On secret sharing systems," *IEEE Trans. On Information Theory*, Vol. IT-29.547, pp.35-41, 1983.

[13] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography Schemes," *Theory of Cryptography Library*: Record 96-13, ftp://theory.lcs.mit.edu/ pub/tcryptol/96-13.ps.

[14] M. Naor and A. Shamir, "Visual cryptography II: improving the contrast via the cover base," *Theory of Cryptography Library*: Record 96-07, ftp://theory.lcs.mit.edu/ pub/tcryptol/96-07.ps.

[15] 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.

[16] V. Rijmen and B. Preneel, "Efficient Colour Visual Encryption or 'Shared Colors of Benetton'," *Eurocrypt*

'96 rumpsession talk . http://www.esat.kuleuven.ac.be/%7Erijmen /vc/euro96/tekst.html

[17] D. Naccache, "Colorful cryptograph -a purely physical secret-sharing scheme based on chromatic filters-," *Coding and Information Integrity* , French-Israeli workshop, December 1994.

[18] D. R. Stinson, "An introduction to visual cryptography," *presented at Public Key Solutions'97.* Available at http://bibd.unl.edu/ ~stinson/VCS-PKS.ps.

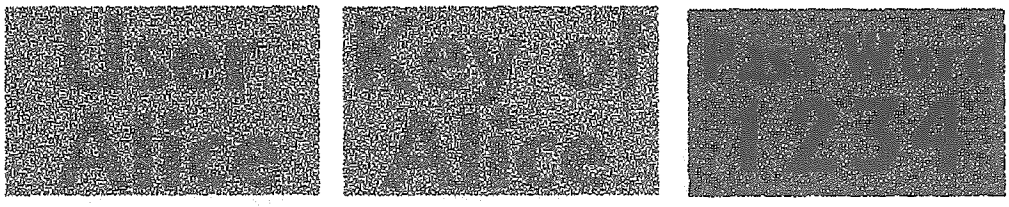
[19] C.N. Yang, Y.B. Yeh, and C.S. Laih, "A dynamic password visual authentication scheme through Internet," 16-th International Telecommunication Symp. (ITS'98), vol. III, pp.163-167, Sep., 1998.

[20] M. Naor and B. Pinkas, "Visual authentication and identification," *CRYPTO'97*, pp.322 -336, available at http://theory.lcs.mit.edu/~tcryptol.

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

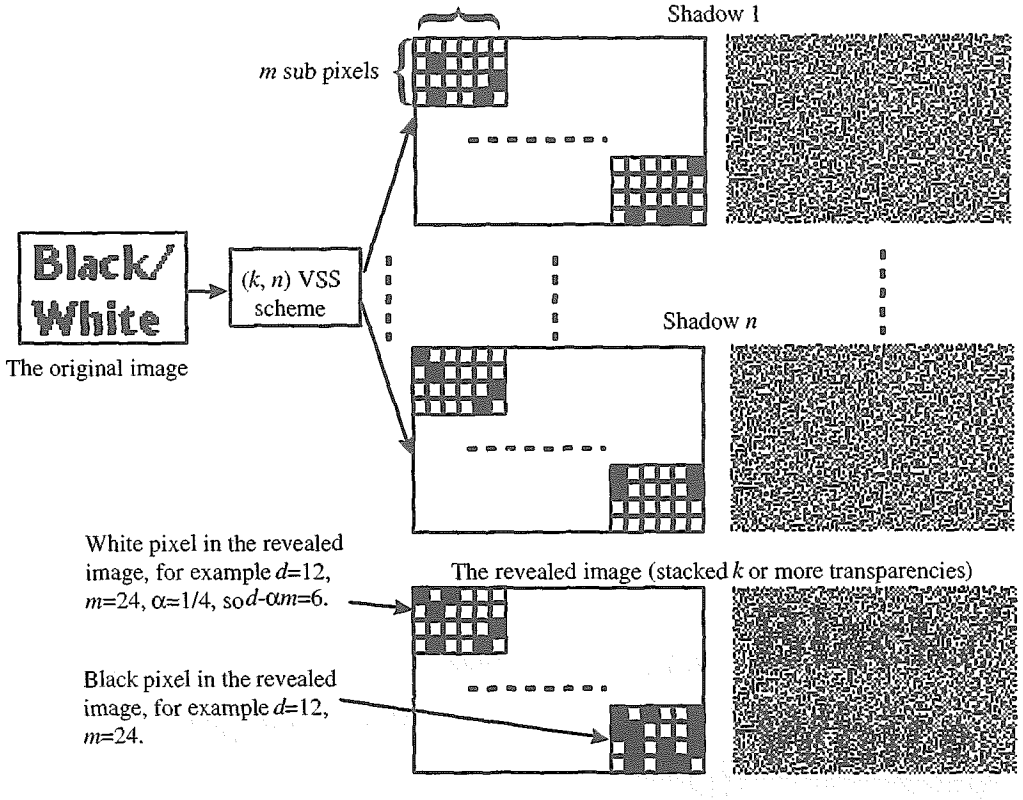
[22] C.S. Laih and Far EasTone Labs. , wireless research project, "Apply VSS Technique to Mobile Phone Handset for Enhancing the Security in Mobile Network",1997-1998.

[23] C.S. Laih and C.N. Yang, ROC PATENT, " Visual Secret Sharing Technique", July, 1997.

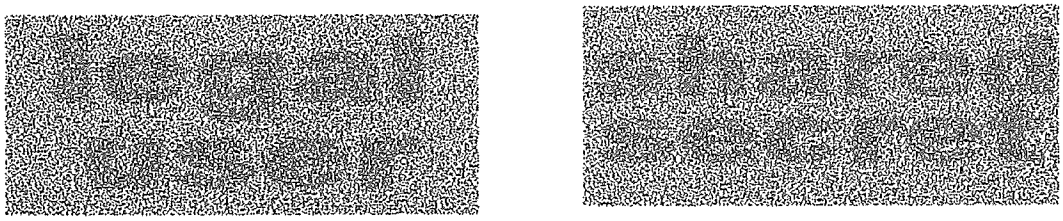


(a) User ID image (b) User's key image (c) The recovered user's pass word

Figure 1 : VSS scheme used in WWW with the help of image editing package



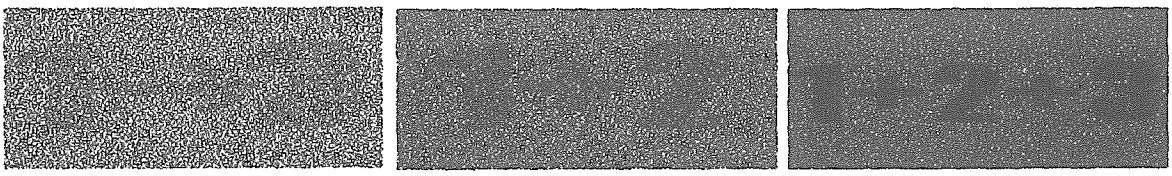
Fi gure 2 : The basic (k, n) VSS scheme model



(a) The TA use this identification image {1, 2}={1, 3} ={1, 4}={1, 5} for verification

(b) The shared secret image {2, 3}={2, 4}={2,5} ={3, 4}={3, 5}={4, 5}

Figure 3 : A (2, 4) VSS scheme with TA of the ability to detect forged shadows

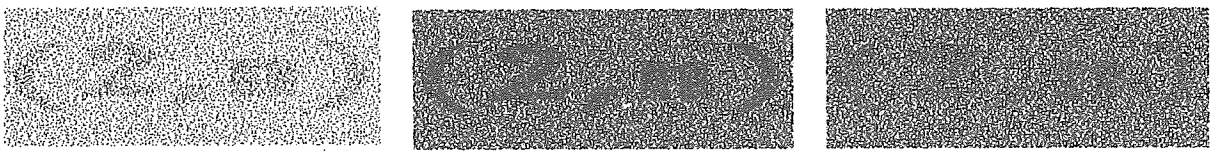


(a) Any arbitrary image {1} (the first shadow)

(b) The shared secret {1, 2}(first shadow stacked with second shadow)

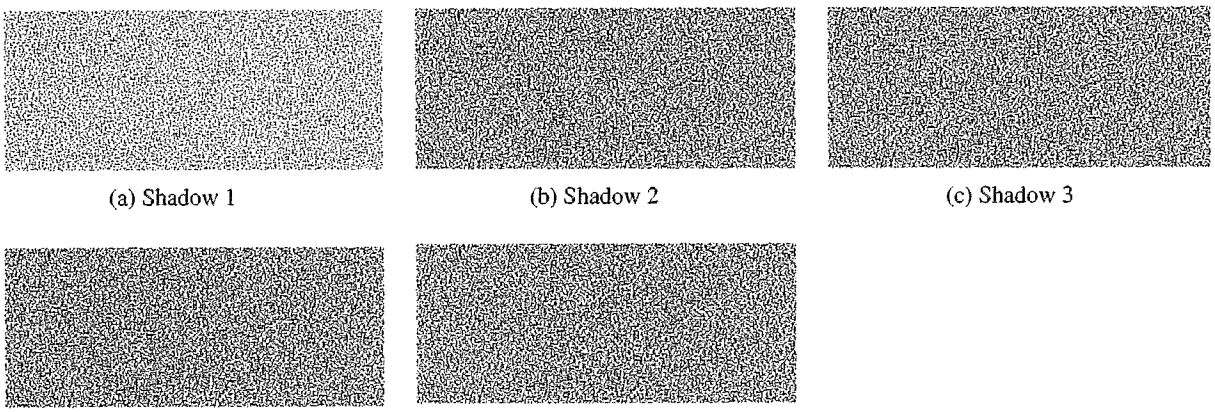
(c) The shared secret{1, 2, 3 (when three shadows are stacked)

Figure 4 : A concr ete example of (1→n) VSS scheme for n=3



(a) Naro-shamir (2, 8) scheme (b) Katoh -Imai (2, 14) scheme (c) Extended (2, 70) scheme

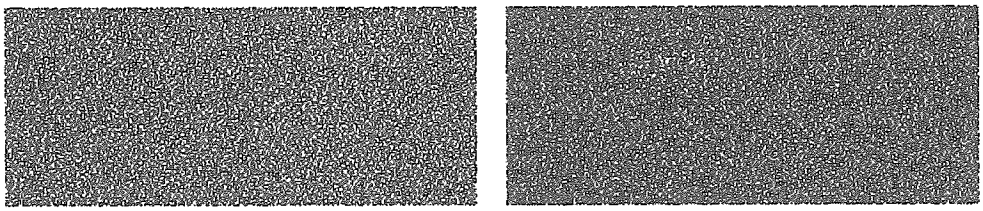
Figure 5: The reve aled images of the different (2, n) VSS schemes (m=8 for this case)



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

(d) Shadow 4 (e) Shadow 5

Figure 6 : a (2, 4) VSS scheme with TA of the ability to detect forged shadows where (a) is hold in TA for verification



(a) Shadow 2 of (1→3) VSS scheme (b) Shadow 3 of (1 →3) VSS scheme

Figure 7 : A (1 →3) VSS scheme of Example 2

Table 1 The number of shadows n for the share size m=2, …, 10

Construction method	m=2	3	4	5	6	7	8	9	10
Naro-Shamir [1]#1	2	3	4	5	6	7	8	9	10
Katoh-Imai [3]#2	*	*	2	2	4	7	14	18	36
Ateniese [5]#3	2	*	4	*	8	*	16	*	32
An extension of [3]#4	2	3	6	10	20	35	70	126	252

* can not be implemented

#1 : m=n.

#2 : using a balanced code with semi -distance 4.

#3 : $m=2\lceil \log n \rceil$.

#4 : $n=\binom{m}{\lfloor m/2 \rfloor}$.