

## NEW $(k, k)$ VISUAL SECRET SHARING SCHEMES USING HIERARCHICAL STRUCTURE TECHNIQUE

*Chung-Nung Yang\* and Chi-Sung Laih\*\**

\*Computer Science Department,  
 Training Institute Kaohsiung Branch,  
 Chunghwa Telecomm Co., Ltd.  
 Kaohsiung, R.O.C.. TEL : 886-7-2447580  
 E-mail : cnyang@ms1.ks.chtti.com.tw

\*\*Department of Electrical Engineering,  
 National Cheng Kung University,  
 Tainan, Taiwan, R.O.C.  
 TEL:886-6-2757575 Ext-62369  
 E-mail : laihcs@eembox.ncku.edu.tw

### ABSTRACT

Visual secret sharing(VSS) scheme is a method that encodes a secret image into shadow images (called shadows) and the decoder does not need complex calculations. With the help of overhead projector(or *image editing package*), the shared secret can be decoded directly by the human visual system without the knowledge of cryptography and the cryptographic computations. Most recent papers about VSS scheme are dedicated to study a higher contrast or a smaller share size in VSS schemes. Smaller size means that the number of columns are smaller when the number of rows of the share matrices in VSS scheme[1] are the same. In this paper, we propose a novel hierarchical method for constructing VSS schemes with significantly less share size than other previously methods.

### 1. INTRODUCTION

The concept of secret sharing scheme(or sometimes referred as threshold scheme) to solve the master key sharing problem is first introduced by Blakley[13] and Shamir[14] in 1979, independently. A  $(k, n)$  Visual Secret Sharing(VSS) scheme[1]-[11] is a method by which the shared image is visible by  $k(k \leq n)$  or more participants with stacking their transparencies(or pictures), called shadows, with the help of overhead projector(or *image editing package*). However,  $k-1$  or fewer of them can not obtain any information about the original shared image. The revealed images in [1]-[9] are all black and white. Some authors[9]-[11] proposed colored VSS schemes such that the users can share the colored secret image. Naccache[11] even used hardware(some chromatic filters) that only allows the pass light with a wavelength in certain interval to reveal the original picture. Readers who interested in VSS scheme are encouraged to refer the article "*An Introduction to Visual Cryptography*"[12].

VSS scheme may have some shortcomings. For example, loss in contrast or distortions are due to xeroxing the shares onto transparencies, and stacking them. We know that the xeroxing and printing process will have distortions and it is in practice hard to align more than three transparencies precisely. So, somebody will say that VSS

scheme is far removed from being of any practical use.

Truly, the practical use of VSS scheme seems to be very limited; however, it is great use when teaching. In fact, a dynamic password visual authentication scheme through Internet using  $(2, 2)$  VSS technique is proposed in [15]. The basic model of the proposed authentication scheme is shown in Figure 1, and the authentication process is shown in Figure 2. Readers who want to try this at home may want to have a look at <http://crypto.ee.ncku.edu.tw/cgi-bin/login.html>. Naor and Pinkas[16] also pointed out that VSS scheme can be used in visual authentication and identification. From above descriptions, it tells us that there still exist some nice and interesting research problems in VSS scheme.

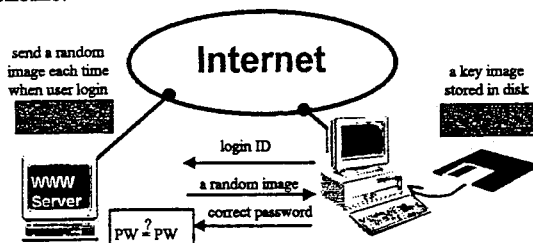
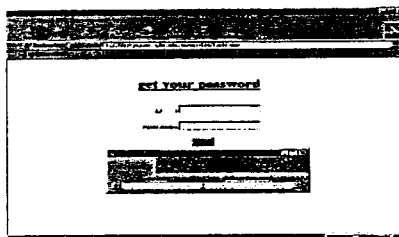
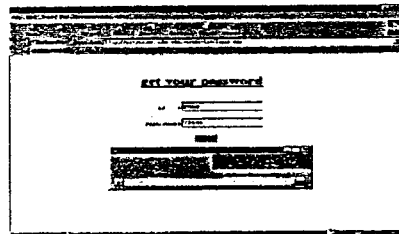


Figure 1 : The block diagram of our proposed visual authentication scheme in [15]



(a) the stacking process of two images



(b) the recovered password

Figure 2 : The authentication process of the proposed visual authentication scheme in [15]

The construction of  $(k, k)$  VSS scheme in [1] with the share size  $2^{k-1}$  had been proven that it is the optimal scheme. Here, we propose a  $(k, k)$  VSS scheme with hierarchical layer structure, such that the share size can be reduced significantly. The shortcoming of our scheme is that the complexity of scheme is proportional to "number of layers". Our  $(k, k)$  VSS scheme contains  $(1+p_1+p_1^2+\dots+p_1^{(a-1)})$ 's  $(p_1, p_1)$  schemes,  $(p_1^{a_1} \times (1+p_2+p_2^2+\dots+p_2^{(a-1)}))$ 's  $(p_2, p_2)$  schemes, ..., and  $\prod_{i=1}^{j-1} p_i^{a_i} \times (\sum_{s=1}^{a_j} p_j^{(s-1)})$   $(p_j, p_j)$  schemes, when  $k=p_1^{a_1} p_2^{a_2} \dots p_j^{a_j}$ , and the share size is now  $2^{a_1(p_1-1) \times \dots \times a_j(p_j-1)}$  instead of  $2^{k-1}$ .

The paper is organized as follows. In Section 2, we will give a brief review of the basic VSS scheme and optimal  $(k, k)$  scheme. In section 3, we propose a hierarchical  $(k, k)$  VSS schemes. The improvement to the hierarchical  $(k, k)$  VSS schemes is also discussed in Section 4. Section 5 gives the compared results between our schemes and Naor-Shamir's optimal scheme. Section 6 concludes the paper and indicates the hierarchical method for  $(k, n)$  VSS scheme.

## 2. THE BASIC VSS SCHEME AND OPTIMAL $(k, k)$ SCHEME

VSS scheme is an encryption technique that stacks some transparencies. The decrypt the secret picture instead of using complex calculations. The decoder is only the "eyes" of human being.

The required conditions of basic  $(k, n)$  VSS scheme (see also [1]):

Let  $C_W$  and  $C_B$  be two collections of  $n \times m$  Boolean matrices. The dealer randomly chooses one of the matrices in  $C_W$  (resp.  $C_B$ ) to share a white (resp. black) pixel; a  $(k, n)$  VSS scheme must satisfy the following conditions where Condition (1) is called *contrast* and Condition (2) is called *security*:

- (1) 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  $d-\alpha m$  (resp. at least  $d$ ), where " $d$ " ( $1 \leq d \leq m$ ) is the threshold value and " $\alpha$ " ( $\alpha > 0$ ) is the relative difference. The grayness can be decoded as white (or black) by human sight if the Hamming weight of corresponding stacked rows no greater than  $d-\alpha m$  (or no less than  $d$ )
- (2) For any subset  $\{i_1, i_2, \dots, i_q\}$  of  $\{1, 2, \dots, n\}$  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  $i_1, i_2, \dots, i_q$  are not visual in the sense that they contain the same matrices with the same frequencies.

In [1], Naor and Shamir have proposed an optimal  $(k, k)$  VSS scheme with the share size  $2^{k-1}$ . Let's look at a basic  $(2, 2)$  example. This means that there are only two black and

white shadows. When they are stacked, a shared picture appears.

The original shared picture is divided into little small dots, called pixels, and then we divide the white (resp. black) into two ( $=2^{2-1}$ ) sub pixels as shown in Figure 3. Every pixel in Shadow 1 and Shadow 2 has one black and one white sub pixels. When we stack the shadows (i.e., Shadow 1 + Shadow 2), black pixels have two black sub pixels, white pixels have only one black sub pixels, so we can reveal the original shared picture.

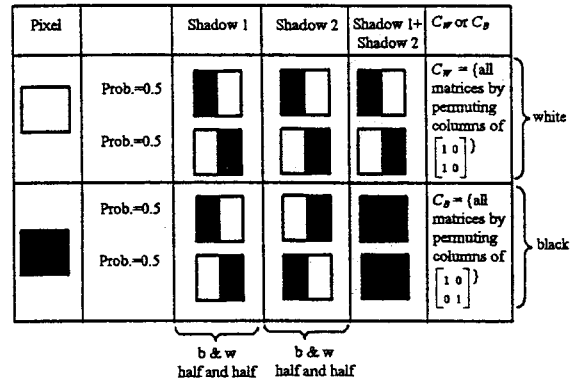


Figure 3 : A  $(2, 2)$  VSS scheme

## 3. HIERARCHICAL $(k, k)$ VSS SCHEME

In this section, we show a method to construct the hierarchical  $(k, k)$  VSS schemes. Our proposed schemes use the same infrastructure of Naor-Shamir's optimal  $(k, k)$  scheme. The basic principle of our hierarchical schemes is that our scheme may combine some small scheme. Let us look at the basic  $(k_1, k_1)$  scheme, i.e. there are  $k_1$  shadows and when they are all stacked, a picture appears. If we use every  $k_1$  shadows as the new original shared pictures of a  $(k_2, k_2)$  scheme, then we can get  $k_1 \times k_2$  shadows. This forms a two-layer  $(k_1 k_2, k_1 k_2)$  VSS scheme with the share size  $2^{(k_1-1) \times (k_2-1) \times 2}$ .

We now describe the hierarchical construction based on the Naor-Shamir's optimal  $(k, k)$  VSS scheme.

*Construction 1*: Let  $k$  be an integer which is greater than 1 and the prime factorization form of  $k$  can be expressed as  $k=p_1^{a_1} p_2^{a_2} \dots p_j^{a_j}$ , where  $p_1, p_2, \dots, p_j$  distinct prime numbers and  $a_1, a_2, \dots, a_j$  are positive integers. Figure 4 shows the block diagram of  $(a_1+a_2+\dots+a_j)$ -layer  $(k, k)$  VSS scheme which includes  $(1+p_1+p_1^2+\dots+p_1^{(a-1)})$ 's  $(p_1, p_1)$  schemes,  $(p_1^{a_1} \times (1+p_2+p_2^2+\dots+p_2^{(a-1)}))$ 's  $(p_2, p_2)$  schemes, ..., and  $\prod_{i=1}^{j-1} p_i^{a_i} \times (\sum_{s=1}^{a_j} p_j^{(s-1)})$   $(p_j, p_j)$  schemes.

The share size is now  $2^{a_1(p_1-1) \times \dots \times a_j(p_j-1)}$ .

The rather proof of Construction 1 is omitted here to clarify the idea of hierarchical method. We now give an example to show the correctness of this construction.

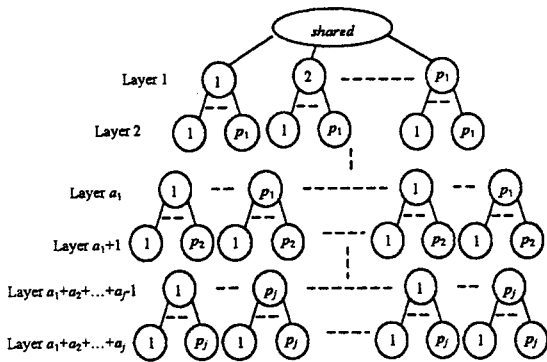


Figure 4 : A  $(a_1+a_2+\dots+a_j)$ -layer  $(k, k)$  VSS scheme with  $k=p_1^{a_1} p_2^{a_2} \dots p_j^{a_j}$

*Example 1:* Observe that a two-layer (4, 4) scheme presented in Figure 5 and 6 uses two Naor-Shamir (2, 2) schemes and the black and white pixels in original picture are divided into four sub pixels in each shadow(S 11, S 12, S 21, S 22). The analyses of "contrast" condition and "security" condition are shown in Figure 7. One can easily verify that 1 out of 4, 2 out of 4, and 3 out of 4 satisfy "security" condition because they contain the same matrices with the same frequencies. The last column in Figure 7 shows 4 out of 4(i.e., S 11 + S 12 + S 21 + S 22) has the "contrast" condition :  $d=4, \alpha=1/4, m=4$ . However, our hierarchical VSS scheme is a probabilistic scheme. This means that we can not see a difference between

black and white original pixels(a combination of four sub pixels) when we stack these four shadows, since the original white pixel in the stacked picture(S 11 + S 12 + S 21 + S 22) may include four all black sub pixels with probability 50%. In fact, considering implementation, this shortcoming of our proposed hierarchical VSS scheme is minor due to the probability. For example, two adjacent white original pixels will have all black sub pixel with probability 1/4, three adjacent white original pixels will have all black sub pixel with probability 1/8, ..., and so on. These four shadows S 11, S 12, S 21, and S 22 are shown as Figure A(a)-(d) in Appendix. When copied on transparencies and stacked carefully (or scanned into the computer and stacked with image editing package such as Adobe Photoshop™), one can reveal the shared image. Figure A(e) shows the result of S 11 + S 12 + S 21 + S 22.

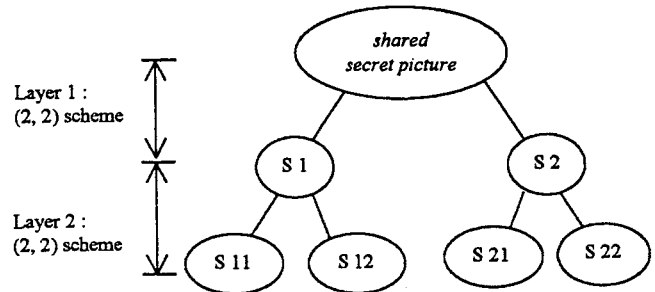


Figure 5 : Two-layer (4, 4) scheme including two (2, 2) schemes

Original Pixel	S 1	S 11	S 12	S 2	S 21	S 22
White	(P.=0.5)	(P.=0.25)	(P.=0.25)	(P.=0.5)	(P.=0.25)	(P.=0.25)
	(P.=0.5)	(P.=0.25)	(P.=0.25)		(P.=0.25)	(P.=0.25)
Black	(P.=0.5)	(P.=0.25)	(P.=0.25)	(P.=0.5)	(P.=0.25)	(P.=0.25)
	(P.=0.5)	(P.=0.25)	(P.=0.25)		(P.=0.25)	(P.=0.25)

Figure 6 : The white and black pixels is divided into 4 sub pixels in a two-layer (4, 4) scheme



Original Pixel	one out of four	two out of four		three out of four	four out of four
		S 11+ S12 or S 21+ S 22	S 11 + S 21 or S 11+ S 12 or S 12 + S 21 or S 12+ S		
	two black and two white sub pixels (P.=1.0)	three black and one white sub pixels (P.=1.0)	1. all 4 sub pixels are black (P.=0.25) 2. two black and two white sub pixels (P.=0.25) 3. three black and one white sub pixels (P.=0.5)	1. all 4 sub pixels are black (P.=0.5) 2. three black and one white sub pixels (P.=0.5)	1. all 4 sub pixels are black (P.=0.5) 2. three black and one white sub pixels (P.=0.5)
	two black and two white sub pixels (P.=1.0)	three black and one white sub pixels (P.=1.0)	1. all 4 sub pixels are black (P.=0.25) 2. two black and two white sub pixels (P.=0.25) 3. three black and one white sub pixels (P.=0.5)	1. all 4 sub pixels are black (P.=0.5) 2. three black and one white sub pixels (P.=0.5)	all 4 sub pixels are black (P.=1.0)

Figure 7 : The analysis of "contrast" and "security" conditions for two-layer (4, 4) scheme

In fact, the implementation may have any choices when we consider the order in which the prime factorization form is listed. For example, the decomposition of 12 can be expressed as  $2 \times 2 \times 3$ ,  $2 \times 3 \times 2$ , and  $3 \times 2 \times 2$ . A hierarchical structure can be implemented as these three types as shown in Figure 8(a)–(c). The type in Figure 8(a) needs 3 (2, 2) schemes and 4 (3, 3) schemes. The type in Figure 8(b) needs 7 (2, 2) schemes and 2 (3, 3) schemes. The type in Figure 8(c) needs 1 (3, 3) schemes and 9 (2, 2) schemes. One can choose the suitable implementation type to reduce the operation time. However, the share size in the construction is independent of the choice of the implementation structure.

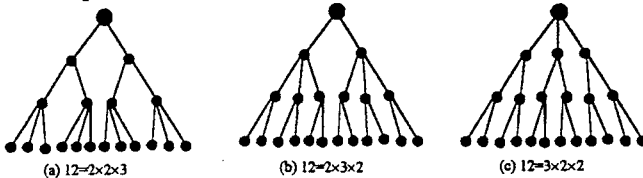


Figure 8 : Different implementation structures considering the listed order

#### 4. IMPROVED PROPOSED HIERARCHICAL (k, k) VSS SCHEME

The basic idea of the improved scheme is based on the following theorem.

**Theorem 1 :** For a  $(k, k)$  VSS scheme, one can make a  $(k-h, k-h)$  VSS scheme by adding any  $h (< k)$  shadows in the  $(k, k)$  schemes to other  $k-h$  shadows.

**Proof:** Let  $S_1, S_2, \dots, S_k$  be the  $k$  shadows of in the  $(k, k)$  VSS scheme. When we add  $S_{i_1}, S_{i_2}, \dots, S_{i_h}$  to other  $k-h$  shadows  $S_{j_1}, S_{j_2}, \dots, S_{j_{k-h}}$ , to form new  $k-h$  shadows  $S'_1 = S_{j_1} + S_{i_1} + S_{i_2} + \dots + S_{i_h}$ ,  $S'_2 = S_{j_2} + S_{i_1} + S_{i_2} + \dots + S_{i_h}, \dots, S'_{k-h} = S_{j_{k-h}} + S_{i_1} + S_{i_2} + \dots + S_{i_h}$ . These new  $k-h$  shadows are just  $h$ -out-of- $k$  cases in the original  $(k, k)$  VSS scheme. So, they also satisfy the conditions of the VSS scheme. Q.E.D.

**Construction 2 :** Let  $k$  be the integer in the range of  $[2^{(b-1)}+1, 2^b]$ . We can construct a  $(k, k)$  VSS scheme by using  $(2^b, 2^b)$  scheme. The scheme uses  $2^b - 1 = (1 + 2 + 2^2 + \dots + 2^{(b-1)})$ 's  $(2, 2)$  schemes, and the share size is now  $2^b$ . The proof that Construction 2 for  $(k, k)$  VSS scheme is very easy when use *Theorem 1*.

Figure 9 shows a (15, 15) VSS scheme using Construction 1. Since  $15 = 3 \times 5$ , this scheme needs one (3, 3) scheme and five (5, 5) schemes, and the share size is  $2^{(3-1)} \times 2^{(5-1)} = 64$ . Since  $15 \leq 2^4$ , thus we can use  $2^4 - 1 = 15$  (2, 2) schemes to construct a (16, 16) VSS scheme, and the share size is  $2^4 = 16$ . Then using the idea of the above theorem, we can get a (15, 15) scheme with share size 16 which is much better than the (15, 15) scheme in Figure 9. The improved (15, 15) scheme is shown in Figure 10.

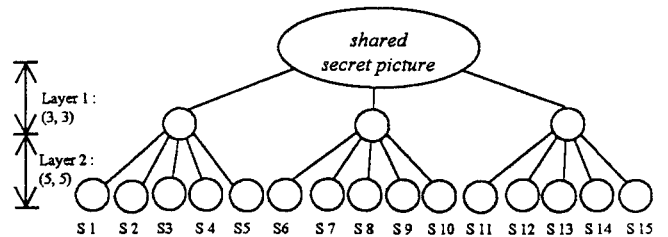


Figure 9 : Two-layer (15, 15) scheme including (3, 3) and (5, 5) schemes

#### 5. COMPARISONS

In this section our proposed schemes are compared with previously optimal scheme. Table 1 shows that our schemes in this paper have the much smaller share size than the optimal scheme. In general, the improved construction(Construction 2) has less share size than the Construction 1.

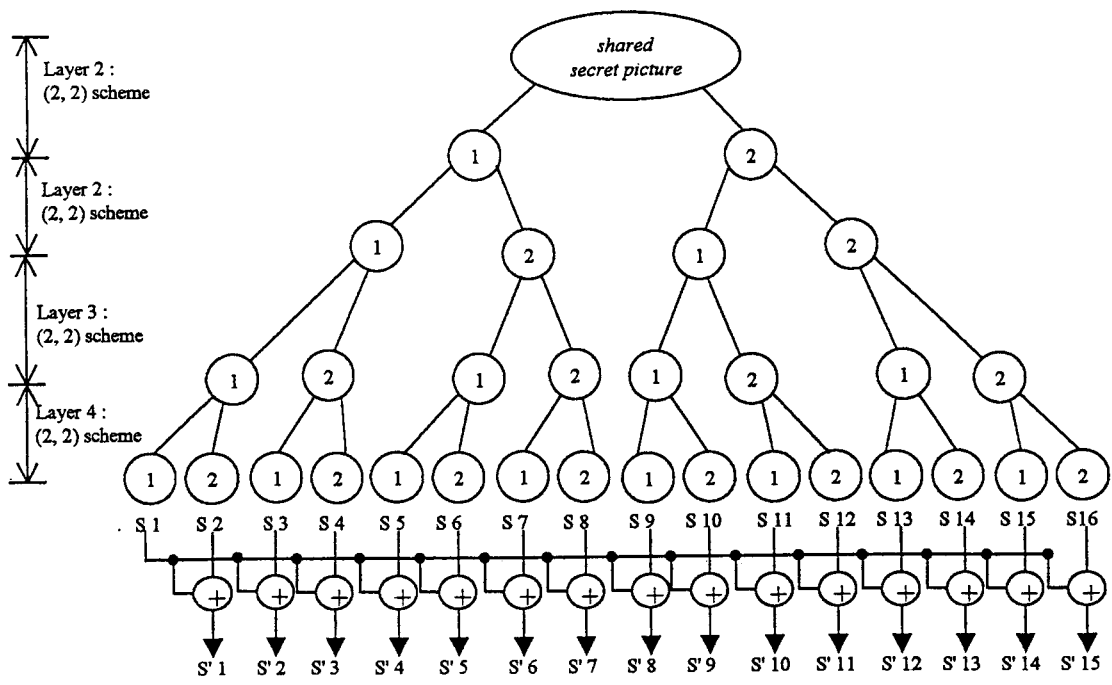


Figure 10 : Four-layer (15, 15) VSS scheme using Construction 2

Table 1 The share size of our proposed  $(k, k)$  VSS schemes and the optimal scheme

$k$	2	3	4	5	6	7	8	9	10	15	20	30	40	50
the optimal share size in [1]*	2	4	8	16	32	64	128	256	1024	$2^{14}$	$2^{19}$	$2^{29}$	$2^{39}$	$2^{49}$
prime factorization of $k$	$1 \times 2$	$1 \times 3$	$2^2$	$1 \times 5$	$2 \times 3$	$1 \times 7$	$2^3$	$3^2$	$2 \times 5$	$3 \times 5$	$2^2 \times 5$	$2 \times 3 \times 5$	$2^3 \times 5$	$2 \times 5^2$
the share size of Construction 1**	2	4	4	16	8	64	8	16	32	64	64	128	128	1024
$2^b \geq k$	2	$2^2$	$2^2$	$2^3$	$2^3$	$2^3$	$2^3$	$2^4$	$2^4$	$2^4$	$2^5$	$2^5$	$2^6$	$2^6$
the share size of Construction 2***	2	4	4	8	8	8	8	16	16	16	32	32	64	64

\* : the share size of optimal Naor-Shamir's scheme [1] is  $2^{k-1}$ .

\*\* : the share size of Construction 1 is  $2^{a_1(p_1-1)} \times \dots \times 2^{a_j(p_j-1)}$ .

\*\*\* : the share size of Construction 2 is  $2^b$ .

One can see that the share size of Naor-Shamir's optimal scheme is 128 when  $k=8$ . Thus, it is not practical from the viewpoint of implementation to use a VSS scheme with share size 128 (i.e., one black or white pixel is divided into 128 sub pixels). However, our proposed construction just needs to divide one pixel into 8 sub pixels. Figure 11 shows the revealed picture of our proposed  $(8, 8)$  scheme with the help of PhotoShop, by reducing 50% image size and arranging threshold value. This result shows that our proposed hierarchical construction for  $(k, k)$  VSS scheme can work really.

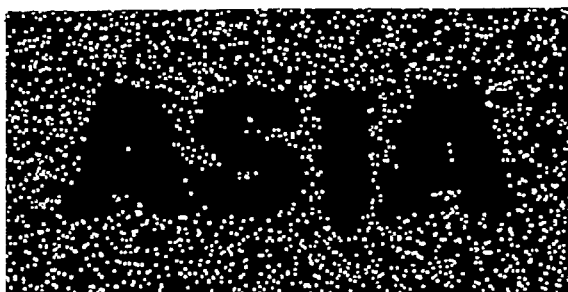
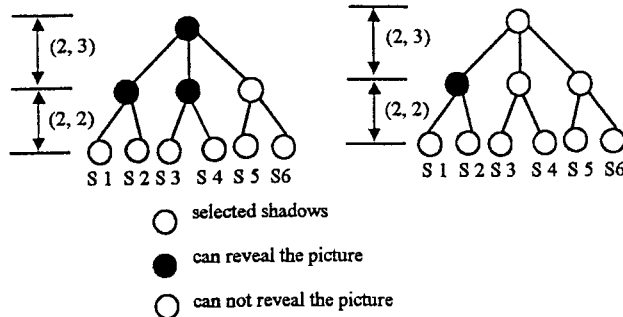


Figure 11 : The revealed picture of our  $(8, 8)$  scheme

## 6. CONCLUDING REMARKS

In this paper, we have presented new constructions of  $(k, k)$  VSS scheme. The construction methods use the optimal Naor-Shamir's optimal  $(k, k)$  scheme as its infrastructure. The basic idea of our proposed constructions is to use some small schemes to form a large scheme. We pay the complexity of construction procedures, but get the fantastic and amazing result. For example, the optimal  $(16, 16)$  needs  $2^{15} = 32,768$  sub pixels to represent one original pixel, but our proposed scheme just needs 16 sub pixels. This gives the practical use of our proposed  $(k, k)$  VSS scheme when  $k$  is large. Furthermore,  $(k, n)$  scheme can also be used in hierarchical construction method. For example, we can use  $(2, 3)$  scheme in the 1st layer, and the  $(2, 2)$  scheme in 2nd layer, to construct one  $(4 \sim 5, 6)$  VSS scheme. This scheme is a soft threshold scheme, it means that 4-out-of-6 may get the revealed shared picture or not (this situation is shown in Figure 12), but 5-out-of-6 and 6-out-of-6 always can get the revealed picture. If  $(2, 3)$  scheme is used in the 1st layer and 2nd layer, then we can get a  $(4 \sim 6, 9)$  scheme.

Hierarchical structure seems very useful for VSS scheme. How to combine different VSS schemes, and what is the optimal structure may need further study.

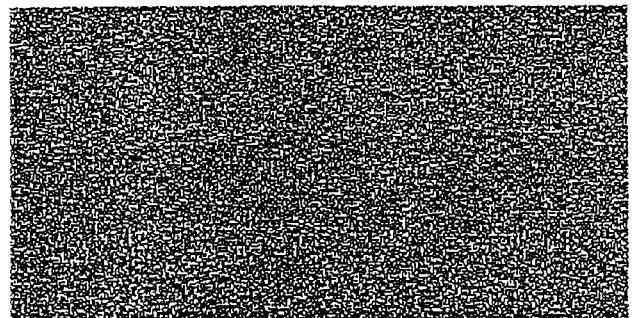


(a) can reveal the picture (b) can not reveal the picture  
 Figure 12 : Different situations for 4-out-of-6 in (4~5, 6)  
 VSS scheme

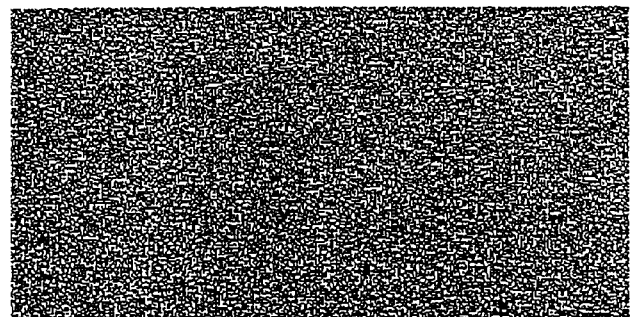
## 7. REFERENCES

- [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)*, via 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 Programming (ICALP'96), Lecture Notes in Computer Science*, Springer-Verlag, 1996.
- [7] 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>.
- [8] 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>.
- [9] 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.
- [10] 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>
- [11] D. Naccache, "Colorful cryptography-a purely physical secret-sharing scheme based on chromatic filters-," *Coding and Information Integrity*, French-Israeli workshop, December 1994.
- [12] D. R. Stinson, "An introduction to visual cryptography," *presented at Public Key Solutions'97*. Available at <http://bibd.unl.edu/~stinson/VCS-PKS.ps>
- [13] G.R. Blakley, "Safeguarding cryptographic keys", *AFIPS conference proceedings*, vol.48, pp.313-317, 1979.
- [14] A. Shamir, "How to share a secret," *Commun. of the ACM*, vol.22, pp.612-613, Nov. 1979.
- [15] C.N. Yang, Y.B. Yeh, and C.S. Laih, "A dynamic password visual authentication scheme through Internet," *International Telecommunications Symposium (ITS'98)*, , vol.III pp.163-167, 1998, Taipei, Taiwan.
- [16] M. Naor and B. Pinkas, "Visual authentication and identification," *CRYPTO'97*, pp.322-336, available at <http://theory.lcs.mit.edu/~tcryptol>.

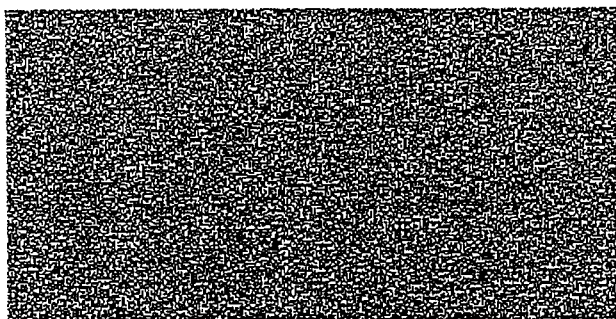
## APPENDIX



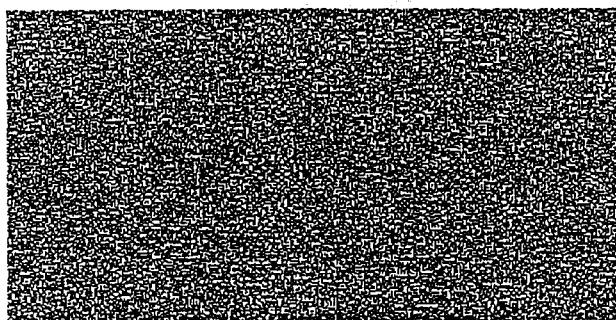
(a) Shadow S 11



(b) Shadow S 12



(c) Shadow S 21



(d) Shadow S22



(e) The shared secret picture  $S_{11} + S_{12} + S_{21} + S_{22}$

Figure A : The shadows and the revealed picture of a two-layer (4, 4) VSS scheme