A K Out of K+1 Visual Cryptography Scheme

Benlan Liu[1, 2 a], Shundong Li[3, b], Daoshun Wang[1, 2 c]

[1]School of Tsinghua University, Beijing 100084, China;

[2]Key Laboratory of Information Security Beijing, China;

[3]School of Shaanxi Normal University, Xi'an.71000, China;

[a]455676912@qq.com, [b]shundong@snnu.edu.cn, [c]daoshun@mail.tsinghua.com

Keywords: visual cryptography, visual secret sharing scheme, basic matrices

Abstract. Naor and Shamir proposed an optimal (*k*, *k*) visual cryptography scheme (VCS). Droste extended the (*k*, *k*) scheme to (*k*, *n*) scheme. Based on properties of 0 and 1's permutations of basic matrices, we use basic matrices of the (*k*, *k*) scheme to constrict basic matrices of (*k*, *k+1*) scheme.

Introduction

An optimal (*k*, *k*) visual cryptography scheme (VCS for short) of binary images was first proposed by Naor and Shamir [1]. Based the scheme, Droste [2] construct a (*k*, *n*) VCS. Blundo et al.[3] proposed a method to sharing gray images by combining the basic matrices of the scheme to share a binary image. Yang et al. [4] found new colored visual secret sharing schemes, one of these schemes based on Droste's (*k*, *n*) VCS; Wang et al. [5] presented a general construction for extended marix of binary image and gray image and color iamge and multi-image visual secret sharing schemes. Shyu et al. [5] used linear programming method two solve the problem of sharing multiple secret iamges.

In this paper, based on Naor and Shamir (*k*, *k*) VCS, we analyze the property of basic matrices and obtain a (*k*, *k+1*) VCS.

Related Works

A. Naor and Shamir's (*k*, *k*) *VCS*

Definition1 [1]: Let B_0 and B_1 be two $k \times 2^{k-1}$ Boolean matrices with exactly all the columns of all even or odd number of 1's,so that $C_0$and C_1 construct a k out of k visual secret sharing scheme

From the definition we know that B_0 owns a column of all "0"**s**, but B_1 owns no such a column. So the Hamming weight of the OR of all the rows of B_0 is 2^{k-1} while B_1 is $(2^{k-1}-1)$, then the contrast is fulfilled.

In **Definition1** we know there k participants and pixel expansion is 2^{k-1}, then, for $\mathrm{i} \in \{0,1,2,\ldots,\mathrm{k}\}$, we get the two basic matrices of the k out of k scheme as follows:

$B_0 = M_k^0 \circ M_k^2 \circ \ldots \circ M_k^j (j = 2.\left\lfloor \frac{k}{2} \right\rfloor)$ $\quad B_1 = M_k^1 \circ M_k^3 \circ \ldots \circ M_k^j \left(j = 2\left\lceil \frac{k}{2} \right\rceil - 1\right)$

Now we give the example of the basic matrices of (*k*, *k*) VCS.

Example1: the basic matrices of (3,3) VCS in **Definition1.**

$$B_0 = M_3^0 \circ M_3^2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad B_1 = M_3^1 \circ M_3^3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Pay attention to B_0 and B_1 in example1, we can see B_0 has a column of all 0's, but B_1 does not, then the contrast is fulfilled.

B. Droste's (k, n) VCS

© 2015. The authors - Published by Atlantis Press

Lemma1 [2] Let B_0 and B_1 be two $\mathrm{n} \times \mathrm{m}$ matrices with arbitrarily k out of n rows own exactly all the columns of all even or odd number of 1's and other $\mathrm{m} - 2^{k-1}$ same columns. Then $C_0$and C_1 construct a k out of n visual secret sharing scheme

Based on **Lemma 1**, we can construct the basic matrices of (k,n)VCS with the follow algorithm.

Algorithm1

a) For all $p \in \{0,\ 1,\ \ldots,\ k\}$, *when* $p < k - p$ *let* $q = p$, *when* $p > k - p$ *let* $q = n - k + p$. *Then when* p *is even, add all the columns of* M_n^p *to* B_0, *when* p *is odd add all the columns of* M_n^p *to* B_1

b) Select k rows of B_0 *and* B_1, *remove all the columns of a k out k scheme and the same columns of two matrices. If the rest columns of* B_0 (B_1) *own i 1's, when* $i < k - p$ *let* $q = i$, *when* $i > k - p$ *let* $q = n - k + i$. *Add all the columns of* M_n^i *to* $B_1(B_0)$

c) While the rest is not empty repeat 2.

Example2: construction of $(3,4)$ VCS by using **Algorithm1**.

i. First when *n*=4 and $p = \{0,\ 1,\ 2,\ 3\}$ all the matrices of M_n^i are

$$M_4^0 = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} M_4^1 = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} M_4^2 = \begin{bmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} M_4^3 = \begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&1&1\\0&1&1&1\end{bmatrix} M_4^4 = \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

ii. Second be sure any k rows own exactly all the columns of all even or odd number of 1's

a) $p = 0\ \&\ p < k - p$, *let* $q = p$, *add all the columns of* M_4^0 *to* B_0

b) $p = 1\ \&\ p < k - p$, *let* $q = p$, *add all the columns of* M_4^1 *to* B_1

c) $p = 2\ \&\ p > k - p$, *let*$q = n - k + p$, *add all the columns of* M_4^3 *to* B_1

d) $p = 3\ \&\ p > k - p$, *let*$q = n - k + p$, *add all the columns of* M_4^4 *to* B_1

And then

$$B_0 = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} \circ \begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&1&1\\0&1&1&1\end{bmatrix} \quad B_1 = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \circ \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

iii. Third be sure the rests are empty

For B_0 *i=3, add all the columns of* M_4^4 *to* B_1

For B_1 *i=3, add all the columns of* M_4^0 *to* B_0

And then we get the two basic matrix as follows:

$$B_0 = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} \circ \begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&1&1\\0&1&1&1\end{bmatrix} \circ \begin{bmatrix}0\\0\\0\\0\end{bmatrix} \quad B_1 = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \circ \begin{bmatrix}1\\1\\1\\1\end{bmatrix} \circ \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

Pay attention to B_0 and B_1 in example1, we can see any 3 out 4 rows in B_0 has two columns of all 0's, but B_1 has only one, then the contrast is fulfilled.

Construct Basic Matrices Use Permutation and Combination

In basic matrices, there are only two elements (0 and 1), so we can consider them as permutations of 0's and 1's. In this case, the two basic matrices of (k,k)VCS can be expressed as:

$$B_0: \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} \quad B_1: \sum_{i=1}^{\lceil k/2 \rceil} \binom{k}{2i-1}$$

Then we can use characteristics of permutation and combination to proof the security of the scheme.

Proof 1:

$$B_0 \quad \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} = \sum_{i=0}^{\lfloor (k-1)/2 \rfloor} \binom{k-1}{2i}\binom{1}{0} + \sum_{i=0}^{\lfloor (k-1)/2 \rfloor} \binom{k-1}{2i+1}\binom{1}{1} = \sum_{i=0}^{k-1} \binom{k-1}{i}\binom{1}{1}$$

$$B_1 \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i-1} = \sum_{i=0}^{\lceil (k-1)/2 \rceil} \binom{k-1}{2i}\binom{1}{1} + \sum_{i=0}^{\lceil (k-1)/2 \rceil} \binom{k-1}{2i+1}\binom{1}{0} = \sum_{i=0}^{k-1} \binom{k-1}{i}\binom{1}{1}$$

Where $\binom{n}{i}\binom{1}{0}$ represents a $(\mathrm{n}+1) \times \binom{n}{i}$ Boolean matrix with rows content all the permutations of I 1's and (n-i) 0's and a row of all 0's. So that any k-1 rows of B_0 and B_1 have the same columns of the matrix that $\sum_{i=0}^{k-1}\binom{k-1}{i}$ indecaded, and this certified any k-1 rows of B_0 and B_1 contend the same columns. Then the security of the scheme is guaranteed.

The Proposed $(\boldsymbol{k}, \boldsymbol{k}+\mathbf{1})$VCS

In this section, we express the basic matrices of the k out k scheme as permutations of 0's and 1's, then we get that the matrices have the characteristics of permutation and combination. Using these features, we extend Naor and Shamir's *k* out of k scheme to a k out of k+1 scheme.

Construction 2: B_0 and B_1 are the basic matrices of Naor and Shamir's k out of k scheme. If B_0 and B_1 do the changes as follows we will get new basic matrices $B_0{}'$ and $B_1{}'$ which are the basic matrices of a k out of k+1 scheme (If the number of 0 of the column vectors of the matrix B_0 and B_1 is *k-p,* and p for the number of 1):

a) If in a matrix, $p < k - p$, add 0 vector in k+1 line and the matrix $\binom{k}{p-1}\binom{1}{1}$, then combine $\binom{k+1}{p-1}$ to the other basic matrix;

b) If $p - 1 \neq 0$, repeat step a;

c) If in a matrix, $p > k - p$, add 1 vector in k+1 line and the matrix $\binom{k}{p+1}\binom{1}{0}$, then combine $\binom{k+1}{p+1}$ to the other basic matrix;

d) If $p + 1 \neq k$, repeat step c.

Because of the features of permutation and combination, the construction has the following form:

Construction 3: The basic matrices of (*k*, *k*) VCS are B_0 and B_1, following the previous construction4.1, we can get the basic matrices of a (*k*, *k+1*) VCS by using combination.

We use result of Lemma 1 to obtain next formulas.

$$B_0: \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} \quad B_1: \sum_{i=1}^{\lceil k/2 \rceil} \binom{k}{2i-1}$$

1) *Extended row vector:*

$$B_0: \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{k}{2i} \cdot \binom{1}{0} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lfloor k/2 \rfloor} \binom{k}{2i} \cdot \binom{1}{1}$$

$$B_1: \sum_{i=1}^{\lfloor k/4 \rfloor} \binom{k}{2i-1} \cdot \binom{1}{0} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k}{2i-1} \cdot \binom{1}{1}$$

2) *Extended column vector($\binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}$):*

$$B_0: \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{k}{2i} \cdot \binom{1}{0} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lfloor k/2 \rfloor} \binom{k}{2i} \cdot \binom{1}{1} + \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{k}{2i-1} \cdot \binom{1}{1} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k}{2i+1} \cdot \binom{1}{0}$$

$$= \sum_{i=0}^{\lfloor k/4 \rfloor} \binom{k+1}{2i} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k+1}{2i+1}$$

$$B_1: \sum_{i=1}^{\lfloor k/4 \rfloor} \binom{k}{2i-1} \cdot \binom{1}{0} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k}{2i-1} \cdot \binom{1}{1} + \sum_{i=1}^{\lfloor k/4 \rfloor} \binom{k}{2i-2} \cdot \binom{1}{1} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k}{2i} \cdot \binom{1}{0}$$

$$= \sum_{i=1}^{\lfloor k/4 \rfloor} \binom{k+1}{2i-1} + \sum_{i=\lfloor k/4 \rfloor+1}^{\lceil k/2 \rceil} \binom{k+1}{2i}$$

3) Get the same residual vector：

$$B_0:\ \sum_{i=0}^{\lfloor k/4\rfloor}\binom{k+1}{2i}+\sum_{i=\lfloor k/4\rfloor+1}^{\lceil k/2\rceil}\binom{k+1}{2i+1}$$

$$+\sum_{i=0}^{\lfloor k/4\rfloor}\sum_{j=1}^{i}\binom{k+1}{2i-(2j+1)}+\sum_{i=\lfloor k/4\rfloor+1}^{\lceil k/2\rceil}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{k+1}{2}\right\rceil-i\right)}\binom{k+1}{2i+(2j-1)}$$

$$+\sum_{i=0}^{\lfloor k/4\rfloor}\sum_{j=1}^{i}\binom{k+1}{2i-2j}+\sum_{i=\lfloor k/4\rfloor+1}^{\lceil k/2\rceil}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{k+1}{2}\right\rceil-i\right)}\binom{k+1}{2i+(2j+2)}$$

$$B_1:\ \sum_{i=1}^{\lfloor k/4\rfloor}\binom{k+1}{2i-1}+\sum_{i=\lfloor k/4\rfloor}^{\lceil k/2\rceil}\binom{k+1}{2i}+\sum_{i=0}^{\lfloor k/4\rfloor}\sum_{j=1}^{i}\binom{k+1}{2i-(2j+1)}+\sum_{i=\lfloor k/4\rfloor+1}^{k/2}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{k}{2}\right\rceil-i\right)}\binom{k+1}{2i+2j}$$

$$+\sum_{i=0}^{\lfloor k/4\rfloor}\sum_{j=1}^{i}\binom{k+1}{2i-(2j-1)}+\sum_{i=\lfloor k/4\rfloor+1}^{k/2}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{k}{2}\right\rceil-i\right)}\binom{k+1}{2i+(2j)}$$

Experimental Results

The Construction 3 is demonstrated as follows through an examples (4, 5) scheme.

Example3: Extend (4,4)VCS to (4,5)VCS

i. Substitute *k=4* into the above formula of B_0 and B_1

$$B_0=\sum_{i=0}^{\lfloor 4/4\rfloor}\binom{4+1}{2i}+\sum_{i=\lfloor 4/4\rfloor+1}^{\lceil 4/2\rceil}\binom{4+1}{2i+1}$$

$$+\sum_{i=0}^{\lfloor 4/4\rfloor}\sum_{j=1}^{i}\binom{4+1}{2i-(2j)}+\sum_{i=\lfloor 4/4\rfloor+1}^{\lceil 4/2\rceil}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{4+1}{2}\right\rceil-i\right)}\binom{4+1}{2i+(2j-1)}$$

$$+\sum_{i=0}^{\lfloor 4/4\rfloor}\sum_{j=1}^{i}\binom{5}{2i-2j}+\sum_{i=2}^{\lceil 4/2\rceil}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{4+1}{2}\right\rceil-i\right)}\binom{5}{2i+(2j+2)}$$

$$B_1:\ \sum_{i=1}^{\lfloor 4/4\rfloor}\binom{4+1}{2i-1}+\sum_{i=\lfloor k/4\rfloor}^{\lceil 4/2\rceil}\binom{4+1}{2i}+\sum_{i=1}^{\lfloor 4/4\rfloor}\sum_{j=1}^{i}\binom{4+1}{2i-(2j+1)}+\sum_{i=\lfloor k/4\rfloor+1}^{4/2}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{4+1}{2}\right\rceil-i\right)}\binom{4+1}{2i+2j}$$

$$+\sum_{i=1}^{\lfloor 4/4\rfloor}\sum_{j=1}^{i}\binom{4+1}{2i-(2j-1)}+\sum_{i=\lfloor 4/4\rfloor+1}^{4/2}\ \sum_{j=1}^{\min\left(i,\left\lceil\frac{4+1}{2}\right\rceil-i\right)}\binom{4+1}{2i+(2j)}$$

ii. According to values of different *i* to obtian corresponding unit of Boolean matrix

$$B_0=M_5^0\circ M_5^2\circ M_5^5\circ M_5^0\circ M_5^5\circ M_5^0=\begin{bmatrix}0&1&1&1&1&0&0&0&0&0&0&1&0&1&0\\0&1&0&0&0&1&1&1&0&0&0&1&0&1&0\\0&0&1&0&0&1&0&0&1&1&0&1&0&1&0\\0&0&0&1&0&0&1&0&1&0&1&1&0&1&0\\0&0&0&0&1&0&0&1&0&1&1&1&0&1&0\end{bmatrix}$$

$$B_1 = M_5^1 \circ M_5^4 \circ M_5^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

From the experimental results above, the two basic matrices of a $(4,5)$VCS is the same as Droste's scheme. Further experimental results of pixel expansion of **Construction 3** are listed in the following table I.

Table I Two scheme comparing

Scheme	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9
Droste's	3	6	15	30	70	140	315	630
Our	3	6	15	30	70	140	315	630

Acknowledgment

This research was supported in part by the National Natural Science Foundation of China (Grant Nos. 61170032, 61272435, and 6173020), and was also supported in part by State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences (Grand No.2015-MS-13).

References

[1] Naor M, Shamir A. Visual cryptography[C]//Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1995: 1-12.

[2] Droste S. New results on visual cryptography[C]//Advances in Cryptology—CRYPTO'96. Springer Berlin Heidelberg, 1996: 401-415

[3] Blundo C, De Santis A, Naor M. Visual cryptography for grey level images [J]. Information Processing Letters, 2000, 75(6): 255-259.

[4] C.N. Yang, C.S. Laih. New colored visual secret sharing schemes, Designs, Codes and Cryptography 20 (2000), vol. 20(3): 325-335.

[5] Wang D, Yi F, Li X. On general construction for extended visual cryptography schemes [J]. Pattern Recognition, 2009, 42(11): 3071-3082.

[6] Shyu S J, Jiang H W. General constructions for threshold multiple-secret visual cryptographic schemes [J]. Information Forensics and Security, IEEE Transactions on, 2013, 8(5): 733-743.