International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Study of (2, n) – Threshold Visual Cryptography Scheme using Different Techniques

Maneesh Kumar

Department of Mathematics, University of Delhi

Abstract: ***A visual cryptography scheme (VCS) for a set of n participants is a method to encode a secret image, consisting of black and white pixels, into n transparencies, one for each participant. Certain qualified subsets of participants can "visually" recover the secret image by stacking their transparencies, whereas, other, forbidden, subsets of participants, cannot gain any information about the secret image. Visual cryptography is a cryptographic paradigm introduced by Naor and Shamir. Some predefined set of participants can decode a secret message (a black and white image) without any knowledge of cryptography and without performing any cryptographic computation: Their visual system will decode the message. In this paper, we define and analyze (2,n) visual cryptography schemes using different models.***

Keywords: Visual Cryptography schemes, (2, n) schemes, black and white images, encoding, optimal relative contrast

1. Introduction

A visual cryptography scheme for a set of *n* participants is a method to encode a secret image, consisting of black and white pixels, into *n* transparencies, one for each participant. Each transparency is constituted by a certain number of shares, one for each pixel of the original image. Each share is a collection of black and white subpixels. The encoding is done in such a way that certain subsets of participants, called qualified sets, can "visually" recover the secret image by stacking their transparencies, but other subsets of participants, called forbidden sets, cannot gain any information (in an information – theoretic sense) about the secret image by inspecting their transparencies.

This cryptographic paradigm was introduced by Naor and Shamir [1]. They analyzed the case of (k,n) – threshold visual cryptography schemes, in which the qualified subsets of participants have cardinality k, whereas, the forbidden subsets of participants have cardinality less than k. further results on (k,n) – threshold visual cryptography schemes can be found in [2 - 7].

Visual cryptography schemes are characterized by two parameters: the pixel expansion, corresponding to the number of subpixels contained in each share and the contrast, which measures the difference between a black and a white pixel in the reconstructed image. VCS such that, in the reconstructed image, all the subpixels associated to a black pixel are black, are referred to as visual cryptography schemes with perfect reconstruction of black pixels. Such schemes are proposed in [8, 9]. In particular, in [9] it has been shown how to construct a VCS with perfect reconstruction of black pixels for any access structure. In this paper, the construction of (2, n) VCS from different models are studied and are presented.

2. The Model

We assume that the secret image consists of a collection of black and white pixels. Each pixel appears in *n* versions called *shares*, one for each transparency. Each share is a collection of *m* black and white sub pixels. In a *k* out of *n* visual threshold scheme, the secret image is visible if any *k* or more transparencies are stacked together, but if fewer than *k* transparencies are superimposed it is impossible to decode the original image. For the construction of such schemes, we consider two *n* x *m* Boolean matrices, *S*0 and *S*1, called *basis matrices* satisfying the following definition:

Definition1. *Let k and n be two integers such that* $k \leq n$ *and P be the set of n participants. A* (*k, n*)-threshold Visual Cryptography Scheme *with pixel expansion m, relative contrast* $\alpha(m)$ *and set of thresholds* $\{ f(X, tX) \}X \subseteq P: | X | = k$, *is realized using the two n* x *m* Basis matrices *S*0 *and S*1 *if the following two conditions hold.*

1. If X = {i1, i2…….. ik} $\subseteq$ P (i.e., if X is the qualified set), then the "OR" V of rows i1,i2……ik of S0 satisfies w (V) $\leq$ tX - α (m).m. whereas, for S1 it results that w (V) $\geq$ tX,
2. If X= {i1, i2…….. ik} $\subseteq$P and p<k (i.e., if X is a forbidden set), then the two p m matrices obtained by restricting S0 and S1 to rows i1, i2…….. ip, are equal up to column permutation.

Two collections of *nxm* matrices, *C*0 and *C*1 are obtained by permuting the columns of the basis matrices (*S*0 for *C*0, and *S*1 for *C*1) in all possible ways. The size of each collection *Ci*, $i \in \{0, 1\}$ is *m*! and it is denoted by *r*. Note that any matrix from *Ci* can act a *Si* , $i \in \{0, 1\}$. In the technique introduced in [1], each pixel of the original image is encoded into *n* pixels, each of which consists of *m* sub pixels. To share a white (black, resp.) pixel, we randomly choose one of the matrices in *C*0 (*C*1, resp.), and distribute row *i* to participant *i*. The chosen matrix defines the *m* sub pixels in each of the *n* transparencies.

Licensed Under Creative Commons Attribution CC BY

3. A (2, n)-threshold VCS with Optimal Relative Contrast using techniques of Coding Theory

In [5], Hofmeister, Krause and Simon, used a different approach via coding theory which allowed them to prove an optimal tradeoff between the relative contrast and the number of sub pixels i.e, the pixel expansion. To prove the results, they used the following notations. For $v, w \in \{0, 1\}^m$, d $(v, w) = |\{i: vi \neq wi\}|$ denote the Hamming distance between v and w. The minimum hamming distance d(S) of a matrix an n x m matrix S is given by

$$d(S) = \min_{v \neq w \in row(S)} d(v, w)$$

And the contrast $\alpha(S)$ of a matrix S is given by

$$\alpha(S) := \frac{1}{m}\left(\min_{v \neq w \in row(S)} (vORw) - \max_{v \notin row(S)} H(v) \right)$$

where $H(v)$ denotes the hamming weight of v.
A Boolean matrix is said to be *balanced* if each row of S contains the same number of 1's. In [5], the problem of finding a (2, n)-threshold VCS with maximal relative contrast is reduced to the problem of finding a matrix with maximal minimum Hamming distance. They made use of *Hadamard matrices* defined as follows.

Definition 2 *Hadamard matrices n H can be recursively defined as follows:*

$$H_1 = [1]$$

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{bmatrix}$$

Where [A | B] denotes the matrix obtained by "horizontal concatenation" of A and B, $\begin{bmatrix} A \\ B \end{bmatrix}$ *denotes the matrix obtained by "vertical concatenation" of A and B and A denotes the matrix obtained from A by negating the entries of A.*

A balanced matrix can be constructed from Hadamard matrix as follows: Let us consider the Hadamard matrix H_n From H_n we define the nx $2(n\text{-}1)$ matrix S_n , where $S_n = [B_n \quad \overline{B_n}]$ and B_n is obtained from H_n by deleting the constant 1 column i.e, the column containing all 1's and by replacing the -1's of H_n by 0's. Then, S_n is balanced and $d(S_n) = n$.

Lemma 1 *Each n x m-matrix S satisfies the inequality* $\alpha(S) \leq d(S) / 2m$. *If S is balanced,then equality holds.*

Proof: Choose u,v such that $d(S) = d(u, v)$ and $w(u) \leq w(v)$. By definition, $\alpha(S) \leq (w(u\ OR\ v) - w(v)) / m$. Define $f(u, v) := w(u\ OR\ v) - w(v)$ which counts the number of positions where $ui = 1$ and $vi = 0$. Since $w(u) \leq w(v)$, the number of positions where $ui = 0$ and $vi = 1$ is at least that number. Hence, $d(S) = d(u, v) \geq 2f(u, v) \geq 2.m.\alpha(S)$. If S is balanced, i.e, every row has Hamming weight t, then for all u, v, $H(u\ OR\ v) = t + d(u, v)/2$. Hence, $\alpha(S) = d(u, v)/2m$.

Theorem 1 *(a) Let C = (C0, C1) be a* (2, n)*-threshold VCS with m subpixels and relative contrast* α (m). *Then*

$$\alpha(m) \leq \min_{S \in C_1} \frac{d(S)}{2m}$$

(b) Given a balanced n xm matrix S, one can define a (2, n)-threshold VCS C (S) with relative contrast d(S)/2m and m sub pixels.

Lemma 2 (**Plotkin's bound.**) *Let S be an nxm-matrix with entries from* {0, 1}. *If* $d(S) > m/2$, *then* $n \leq 2d(S)/(2d(S) - m)$. *The following are corollaries:*
(i) $d(S) \leq (n/2(n - 1))m$.
(ii) If $d(S) \geq m/2$, *then* $n \leq 2m$.
(iii) If $d(S) \geq m/2$ *and S is balanced, then* $n \leq 2m - 1$.

Proof: The first statement follows directly. The second statement can be proved by considering the sub-matrix $S1$ ($S0$, resp.) of S which consists of those rows which have a 1 (0, resp.) in the first column. Deleting the first column of $S0$ and $S1$ and then applying Plotkin's bound, we obtain $n \leq 4d(S)/(2d(S) - m + 1)$. For $d(S) \geq m/2$, this gives $n \leq 2m$. For the third statement, assume w.l.o.g. that every row in S has Hamming weight exactly $t \leq m/2$. We can add a constant 1-row to S and obtain a matrix S' which still has minimum Hamming distance $m/2$. We apply part (ii) to S'.

Theorem 2 *(a) The contrast of a* (2, n)*-VCS is at most* $n / 4(n - 1)$.
(b) For all $n = 2k$, $k \geq 1$, *there is a* (2, n)*-scheme with contrast* $n/4(n - 1)$ *and* $m = 2n - 2$ *sub pixels.*

Proof: (a) is proved by Theorem 1, part (a), and Lemma 2, part (i). For the proof of (b), we note that the Hadamard matrix H_n has a constant 1 column as well as a constant 1 row, all other rows have Hamming weight $n = 2$. Furthermore, $d(H_n) = n/2$. Define the n x $2(n\text{-}1)$-matrix S_n $S_n = [B_n \quad \overline{B_n}]$ by where B_n is obtained from H_n by deleting the constant 1 column. n S is balanced, and $d(S_n) = n$. By Theorem 1, part (b), this matrix leads to the desired scheme.

4. A (2, *n*)-threshold VCS with Optimal Relative Contrast using Combinatorial Structures

In [4], the authors described two methods for constructing a (2, n)-threshold VCS. In the first method, the basis matrices were constructed as follows:
The columns of the $n \times m$ matrix $S1$ consists of all binary n-vectors of weight $\lceil n/2 \rceil$. Hence, $m = \binom{n}{n/2}$ and any row of S_1 has weight equal to $\binom{n-1}{\lceil n/2 \rceil - 1}$. S_0 constructed from n identical row vectors of length m, and weight $\binom{n-1}{\lceil n-1 \rceil - 1}$.
Clearly, Property 2 of Definition 1 is satisfied. We can prove that these matrices satisfy Property 1 of Definition 1 also. Consider any $q \geq 2$ distinct indices, say $i1, i2, \ldots iq$, and

Licensed Under Creative Commons Attribution CC BY

let $X = i1, i2, \cdots . . iq$. Let S_x^i, $i \in \{0, 1\}$ denote the 'OR' of the rows of Si whose indices are given by the set X. We now compute the difference $w\left(S_x^1\right) - w\left(S_x^0\right)$. It is easy to see that

$$w\left(S_x^0\right) = \left(\frac{n-1}{\lceil n-2 \rceil - 1}\right).$$

Moreover, for $q > n - \lceil n/2 \rceil = \lceil n/2 \rceil$, we have that $w\left(S_x^1\right) = m$. For $2 \le q \le \lceil n/2 \rceil$ it is immediate to see that $w\left(S_x^1\right)$ is equal to m minus the number of columns having entries all 0's in the rows indexed by $i1, i2, \cdots\cdots, iq$. That is,

$$w\left(S_x^1\right) = \left(\frac{n}{\lceil n/2 \rceil}\right) - \left(\frac{n-q}{\lceil n/2 \rceil}\right).$$

Since, for any $1 \le k \le n$, it holds that

$$\binom{n}{k} = \binom{n-1}{k-1} - \binom{n-1}{k},$$

We obtain that

$$w\left(S_x^1\right) - w\left(S_x^0\right) = \begin{cases} \left(\frac{n-1}{\lceil n/2 \rceil}\right) - \left(\frac{n-q}{\lceil n/2 \rceil}\right) & if\ 2 \le q \le \left\lceil \frac{n}{2} \right\rceil \\ \left(\frac{n-1}{\lceil n/2 \rceil}\right) & if\ \left\lceil \frac{n}{2} \right\rceil < q \le n. \end{cases}$$

The above quantity $w\left(S_x^1\right) - w\left(S_x^0\right)$ does not depend on the actual set X but only its size. Let $\beta(q) = w\left(S_x^1\right) - w\left(S_x^0\right)$. The quantity β (q) reaches its minimum at $q = 2$. Define $\alpha(m) = \beta$ $(2)/m$. Hence,

$$\alpha(m) = \left(\frac{n-1}{\lceil n/2 \rceil}\right) - \left(\frac{n-2}{\lceil n/2 \rceil}\right)$$
$$= \left(\frac{n}{\lceil n/2 \rceil}\right) - \left(\frac{n-1}{\lceil n/2 \rceil - 1}\right) - \left(\frac{n-2}{\lceil n/2 \rceil}\right)$$
$$= \left(\frac{n-2}{\lceil n/2 \rceil - 1}\right).$$

Since, $m = \left(\frac{n}{\lceil n/2 \rceil}\right)$, we get that

$$\alpha(m) = \frac{\left(\frac{n-2}{\lceil n/2 \rceil - 1}\right)}{\left(\frac{n}{\lceil n/2 \rceil}\right)} = \frac{\lceil n/2 \rceil \lceil n/2 \rceil}{n(n-1)}$$

For convenience we define

$$\alpha(n) = (\lceil n/2 \rceil \lceil n/2 \rceil) / n(n-1).$$

Observe that we can express α*(n) in the following form:

$$\alpha^*(n) = \begin{cases} \frac{n}{4n-4} & if\ 'n'\ is\ even \\ \frac{n+1}{4n} & if\ 'n'\ is\ odd \end{cases}$$

For any set X of at least 2 participants, if we set $t_x = w\left(S_x^1\right)$ and α (m) = $\alpha*(n)$, then Property 1 of Definition 1 is satisfied. Theorem proves that the value of $\alpha*(n)$ is the best possible value for the relative difference of a (2, n)-threshold VCS. In [4], they summarized the above discussion in the following theorem.

Theorem 3 For any n ≥ 2, there exists a (2, n)-threshold VCS with pixel expansion

$$m = \binom{n}{\lfloor n/2 \rfloor},$$

Example 1 Let us consider an example with n = 4, we construct a (2, 4)-threshold VCS by considering the two basis matrices as follows:

$$S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \text{ and}$$

$$S^0 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

5. Construction of (2, *n*)-threshold VCS using BIBDs and PBD

Here, basis matrices are constructed by making use of combinatorial design with certain properties. Again, we need a few definitions.

Definition 3 *Let n, k, and λ be positive integers with* $2 \le k < n$. *A* (*n, k, λ*)*-BIBD (* balanced incomplete block design*) is a pair* (*X, B*)*, where X is a set of n elements (called* points*) and B is a collection of subsets of X (called* blocks*), such that each block contains exactly k points and each pair of points is a subset of exactly λ blocks.*

We use *r* to denote the number of blocks in which each point occurs and *b* to denote the total number of blocks in a BIBD.

Example 2 Consider an example of a (7, 3, 1)-BIBD given below.

Block points in the block
1 (1, 2, 4)
2 (2, 3, 5)
3 (3, 4, 6)
4 (4, 5, 7)
5 (5, 6, 1)
6 (6, 7, 2)
7 (7, 1, 3)

Definition 4 *Let n and λ be positive integers, and let K be a set of positive integers such that* $2 \le k < n$ *for every* $k \in K$. *A* (*n, K, λ*)*-PBD (* pair wise balanced design*) is a pair* (*X, B*)*, where X is a set of n elements (called* points*) and B is a collection of subsets of X (called* blocks*), such that* $|B| \in K$ *for every* $B \in \beta$*, and each pair of points is a subset of exactly λ blocks.*

Licensed Under Creative Commons Attribution CC BY

Example 3 An example of a (5, {2, 3}, 2)-PBD where X = {1, 2, 3, 4, 5} is given below

Block points in the block
1 (1, 2, 5)
2 (2, 3)
3 (2, 3, 4)
4 (1, 3, 4)
5 (2, 4, 5)
6 (3, 5)
7 (4, 5)
8 (1, 2)
9 (1, 3, 5)
10 (1, 4)

As with BIBDs, we will use b to denote the number of blocks. Note that it is not necessarily the case in a PBD that there is a fixed integer r such that every point occurs in exactly r blocks. Observe also that a PBD with $|K| = 1$ is a BIBD.

Definition 5 *Suppose that (X, β) is a PBD (or a BIBD). The point-block incidence matrix of this design is the $n \times b$ matrix M, in which the rows are indexed by X and the columns are indexed by β, where*

$$m_{xB} = \begin{cases} 1 & \text{if } x \in B, \\ 0 & \text{otherwise.} \end{cases}$$

Example 4 The incidence matrix of the (7, 3, 1)-BIBD (see Example 3.3.1) is given below.

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Using the incidence matrix of this BIBD as basis matrix S^1, a (2, 7)-VTS can be constructed. By using the combinatorial design BIBD, the authors in [5] proposed a (2, n)-VCS as follows:
Let S^1 be the incidence matrix of an (n, k, λ)-BIBD. Define S^0 to be the Boolean matrix in which every row consists of r 1's followed by (b - r) 0's.

Then S^0 and S^1 form the basis matrices of a (2, n)-VCS with pixel expansion $m = b$ and relative contrast $\alpha(m) = \frac{2r - \lambda - r}{b} = \frac{r - \lambda}{b}$. We have the following results characterizing threshold VCSs with optimal pixel expansion in terms of BIBDs and PBDs.

Theorem 4 (Stinson et al [4]) *Suppose n is even. Then there exists a* (2, *n*)*-threshold VCS with pixel expansion m and (optimal) relative difference* α (*m*) = α*(*n*) *if and only if there exists an* (*n*, *n*/2, *m* (*n*- 2)/ (4*n*- 4))*-BIBD.*

Proof: Suppose that we have a (2, n)-threshold VCS with pixel expansion m and optimal relative difference. Let $M \in C_1$. We will show that the M is the incidence matrix of an (n, $n/2$, m (n - 2)/ (4n - 4))-BIBD, (X, B). The verifications follow from Lemma 3 in a straightforward manner. Since M has n rows, we have $|X| = n$, and since M has m columns, we have $|B| = m$.
Since every column of M has weight $n/2$, every block $B \in \beta$ has size $n/2$. Since every row of M has weight $m/2$, the design has constant replication number $r = m/2$. Finally, since the Hamming distance between any two rows of M is exactly 2.α (m).m, we see that any two points in X occur in exactly

$$r - \alpha(m).m = \frac{m}{2} - \frac{mn}{4n-4} = \frac{m(n-2)}{4n-4} = \lambda$$

blocks. Hence the desired BIBD is obtained.

Conversely, suppose we have an (n, $n/2$, m (n - 2)/ (4n - 4))-BIBD. Let M be its point-block incidence matrix. Then we can obtain a (strong) (2, n)-threshold VCS with pixel expansion m and optimal relative difference by taking basis matrices S^1 and S^0, where $S^1 = M$ and S^0 is a matrix of n identical rows, each consisting of $m/2$ 1's followed by $m/2$ 0's.

For n odd, we have the following theorem.

Theorem 5 (Stinson et al. [4]) *Suppose n is odd. Then there exists a* (2, *n*)*-threshold VCS with pixel expansion m and (optimal) relative difference* α (*m*) = α*(*n*) *if and only if there exists an* (*n*, {(*n* - 1)/2, (*n* + 1)/2}, *w* - *m* (*n*+1)/ (4*n*))*-PBD such that every point occurs in exactly w blocks, where w is an integer such that*

$$\frac{(n-1)m}{2n} \le w \le \frac{(n+1)m}{2n}.$$

Example 5 The (5, {2, and 3}, 2)-PBD given in Example 3.3.2 would give rise to the following incidence matrix M:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Using the incidence matrix M of this PBD as basis matrix S^1 and S^0 to be the matrix in which every row is equal to (1111100000), a (2, 5)-threshold VCS can be constructed.

Licensed Under Creative Commons Attribution CC BY

6. An Implementation of a (2, 4)-threshold VCS constructed using Hadamard Matrices



Figure 1: Original image

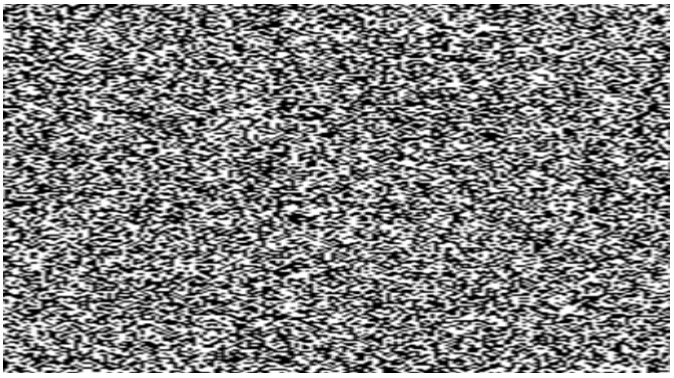


Figure 2: Share 1

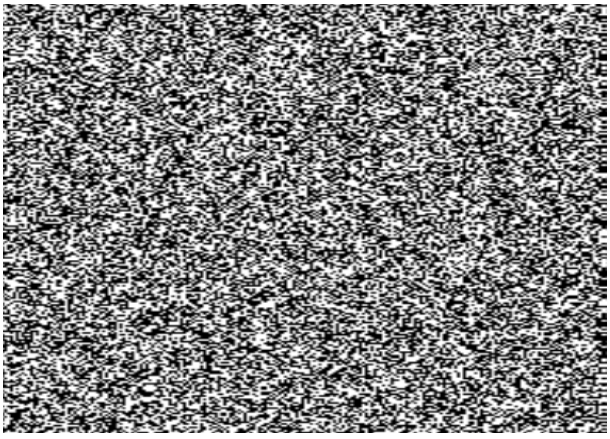


Figure 3: Share 2

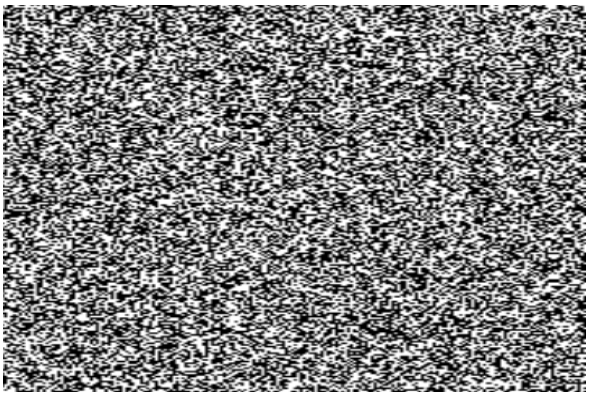


Figure 4: Share 3



Figure 5: Superimposition of Shares 2 and 4

7. An example implementation of a (2, 2)-threshold VCS

The basis matrices used here are

$$S^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \text{ And } S^1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

IITKGP

Figure 6: Original image

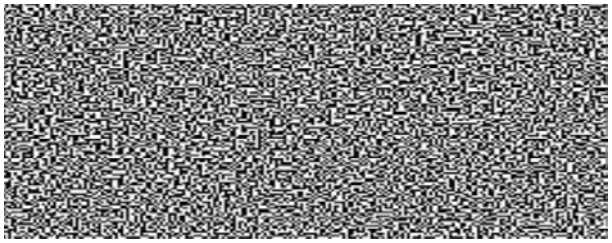


Figure 7: Share 1

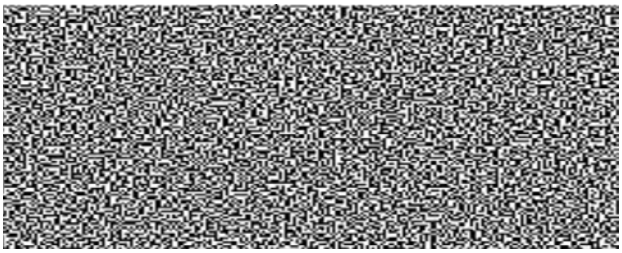


Figure 8: Share 2



Figure 9: Superimposition of Share 1 and Share 2

Licensed Under Creative Commons Attribution CC BY

8. Conclusions

In this paper we have defined and analyzed different (2,n) threshold visual cryptography schemes for level images. We gave a necessary and sufficient condition for such schemes to exist. We proved the optimality of theorems related to these problems. An interesting open problem which deserves further investigation is the encoding of grey level images for different models of VCS such as in [10].

References

[1] Naor M. and Shamir A., Visual cryptography, Eurocrypt' (1994) Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, pp. 1- 12.
[2] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson (1996), Visual Cryptography for general access structures, Inform. Comput. 129(2), pp. 86-106.
[3] C. Blundo, P. D'Arco, A. De Santis, D. R. Stinson (2003), Contrast optimal threshold visual cryptography schemes, SIAMJ. Discrete Math. 16(2), pp. 224-261.
[4] C. Blundo, A. De Santis, D. R. Stinson (1999), On the contrast in visual cryptography schemes, J. Cryptology, 12(4), pp. 261-289.
[5] T. Hofmeister, M. Krause, H. U. Simon (2000), Contrast optimal k out of n secrets sharing schemes in visual cryptography, Theoret. Comput. Sci. 240(2), pp. 471-485.
[6] M. Krause, H. Simon (2003), Determining the optimal contrast for secret sharing schemes in visual cryptography, Comb. Probab. Comptu. 12(3), pp. 285-299.
[7] E. R. Verheul, H. C. A. van Tilborg (1997), Constructions and properties of k out of n visual secret sharing schemes, Des. Codes Cryptography, 11(2), pp. 179-196.
[8] C. Blundo, A. De Bonis, A. De Santis (2001), Improved Schemes for visual cryptography, Des. Codes Cryptography, 24, pp. 255-278.
[9] C. Blundo, A. De Santis (1998), Visual cryptography schemes with perfect reconstruction of black pixels, J. Comput. Graphics, 22(4), pp. 449-455.
[10] M. Naor, A. Shamir (1997) Visual cryptography, II: Improving the contrast via the cover base, in: Security Protocols, Lecture Notes inComputer Sci., vol. 1189, Springer Berlin, pp. 197-202.

Authors Profile

Maneesh Kumar received his M.Tech Degree in Computer Science and Data Processing from Indian Institute of Technology, Kharagpur in 2012. He is currently working in the Department of Mathematics, University of Delhi. His research interests include techniques in visual cryptography schemes.

Licensed Under Creative Commons Attribution CC BY