A Project Report on

THE STUDY ON VISUAL CRYPTOGRAPHY USING THRESHOLD SCHEMES

Thesis submitted in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology (B. Tech)

In

Electronics and Communication Engineering

Submitted by

M.Venkata Varun Babu

B. Sarala Kumari K. Silpa

V.Srujana N .S.Sekhar Varma

Under the esteemed guidance of

Ms T.Jyothirmayee, M.Tech

Department of Electronics and Communication Engineering
Bapatla Engineering College

(Affiliated to Acharya Nagarjuna University)

Accredited by NBA, ISO 9001:2000 Certified Institute

BAPATLA-522 101, A.P, INDIA

April 2010

CERTIFICATE

(Affiliated To Nagarjuna University)

THE STUDY ON VISUAL CRYPTOGRAPHY USING THRESHOLD SCHEMES

This is to certify that the report **"THE STUDY ON VISUAL CRYPTOGRAPHY USING THRESHOLD SCHEMES"** entitled is the bonafide work of

M.Venkata Varun Babu(Y6EC512)

B. Sarala Kumari(Y6EC470)
V.Srujana (Y6EC494)

K. Silpa (Y6EC474)
N.SomaSekharVarma(Y6EC483)

Submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology (**B. Tech**) in **Electronics & Communication Engineering** by **Acharya Nagarjuna University** during the academic year 2009 – 2010.

Guide:

Ms T.Jyothirmayee, M.Tech
Lecturer,
Department of ECE,
Bapatla Engineering College,
Bapatla.

Head of Dept:

Dr.B.ChandraMohan, Ph.D,
Professor & Head,
Department of ECE,
Bapatla Engineering College,
Bapatla.

ACKNOWLEDGEMENT

It is with immense pleasure that we would like to express our indebted gratitude to our guide, **T.Jyothirmayee,** Lecturer Department of E.C.E, Bapatla Engineering College, who has guided us a lot and encouraged us in every step of our project work. Her invaluable guidance throughout the project helped us to a great extent.

We would like to take this opportunity to express our gratitude to our principal, **Dr.K.Lakshmi Prasad**, and Head of the Department, **Dr. B .Chandra Mohan,** for providing us with the latest software to complete our project & for giving us this opportunity to do the project.

Finally, we acknowledge with gratitude the unflagging support of the non-teaching staff for their espouse during the completion of the report dissertation.

Last but not the least; we would like to express our sincere thanks to our parents, encouraging friends and all those who have been helping us for the successful completion of this project.

Above all, we thank God Almighty for his blessings showered on us to complete this work successfully.

M.Venkata Varunbabu

B. Sarala kumari

K.Silpa

V.Srujana

N.SomaSekhar Varma

Contents

Chapter 1

Introduction

1.1Visual Threshold Scheme:

The visual secret sharing scheme (VSSS) proposed by Naor and Shamir is one of the cryptographic schemes applicable to secret sharing of black-white images. In VSSS , a black-white image called a secret image, which is required to be kept secret , is encrypted to n black-white images called shares, where $n \geq 2$ is the number of participants. The n shares are printed on n transparencies and are distributed to n respective participants.

A (t,n)-threshold visual cryptography scheme for a set *P* of *n* participants is a method to encode a secret image *SI* (Secret Image) into n shares, where each participant in *P* receives one share. Any (qualified) set of *t* or more participants can “visually” recover the secret image, but (forbidden) sets of participants of cardinality less than *t* have no information (in an information-theoretic sense) on *SI*. A “visual” recovery for a set $X \subseteq P$ consists of xeroxing the shares given to the participants in *X* onto transparencies, and then stacking them. The participants in a qualified set *X* will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. Visual Cryptography schemes are characterized by two parameters. The pixel expansion, which is the number of sub pixels each pixel of the original image in encoded into, and the relative contrast which means the “difference” between a black and a white pixel in the reconstructed image. we consider the security of shares in visual cryptography and generating more meaningful shares with respect to basic cryptographic scheme.Basically visual cryptography is used for the encryption of visual information like written materials, textual images, and handwritten notes, print and scanned etc. in a perfectly secure way so that the decryption can be performed by human visual system. The formal definition of visual cryptography was first introduced by Naor and Shamir. The idea of the visual cryptography model proposed cryptography model proposed is to split an image into two random shares (printed on transparencies) which separately reveal no information about the original secret image other than the size of the secret image. The image is composed of black and white pixels. The original image can be recovered by superimposing the two shares. The underlying operation of this visual cryptography model is OR.

Advantage of Visual Cryptography

1. Simple to implement
2. Encryption don't required any Hard problem dependency
3. Decryption algorithm not required (Use a human Visual System). So a person unknown to cryptography can decrypt the message.
4. We can send cipher text through FAX or E-MAIL
5. Infinite Computation Power can't predict the message

1.2 Basis Matrices:

Most of the constructions in this project were realized using two $n \times m$ matrices, S^0 and S^1 called *basis matrices* satisfying the following definition.

Definition 1 Let *(*$\Gamma_{Qual}, \Gamma_{Forb}$*)* be an access structure on a set of n participants. A *(* Γ_{Qual}, Γ_{Forb} *,m)*VCS with relative difference $\alpha(m)$ and set of thresholds $\{t_x\}_{X \in \Gamma_{Qual}}$ is realized using the $n \times m$ basis matrices S^0 and S^1
if the following two conditions hold:

1. If $X = \{i_1, i_{2,} ...., i_p\} \in \Gamma_{Qual}$ is a qualified set, then the "or" *V* of rows $\{i_1, i_2 ....i_p\}$ of S^0 satisfies $w(v) \leq t_x - \alpha(m)$ · m; whereas, for S^1 it results that $w(v) \geq t_x$.

2. If $X = \{i_1, i_{2,} ...., i_p\} \in \Gamma_{Forb}$ is not a qualified set then the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $\{ i_1, i_2, ..., i_p \}$ are equal up to a column permutation.

The collections C_0 and C_1 are obtained by permuting the columns of the corresponding matrix (S^0 for C_0 and $S^1$for C_1) in all possible ways. In this case, the size of the collections and C_1 is the same and it is denoted by *r*.

1.2.1. Threshold Schemes:

A (k,n) -threshold structure is any access structure ($\Gamma_{Qual}, \Gamma_{Forb}$) in which

$$\Gamma_0 = \{B \subseteq \mathrm{p} : |\mathrm{B}| = k\}$$

And

$$\Gamma_{Ford} = \{B \subseteq p : |B| \le k-1\} \ .$$

In any (k,n) -threshold VCS, the image is visible if any k or more participants stack their transparencies, but totally invisible if fewer than k transparencies are stacked together or analyzed by any other method. In a strong (k,n) -threshold VCS, the image remains visible if more than k participants stack their transparencies.

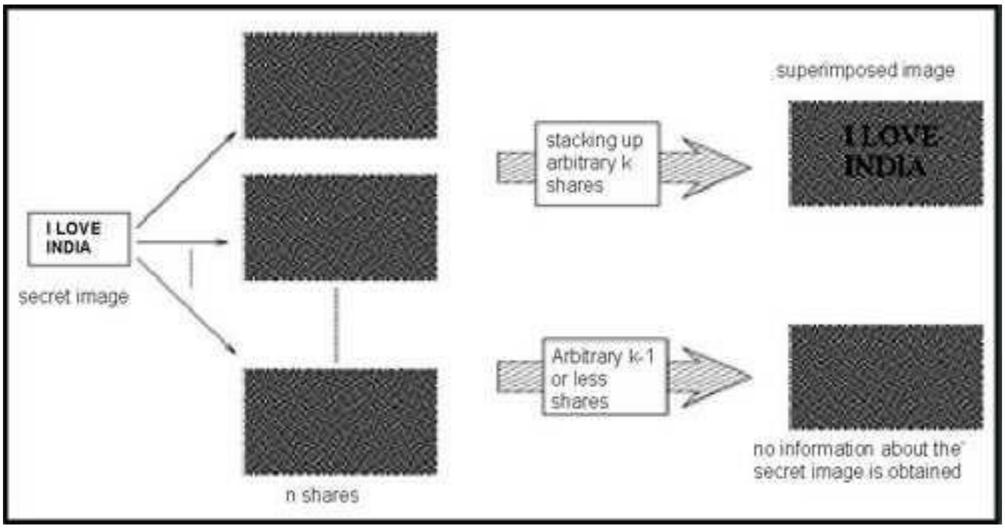

I LOVE
INDIA
secret image
n shares
stacking up arbitrary k shares
superimposed image
I LOVE
INDIA
Arbitrary k-1 or less shares
no information about the secret image is obtained

Figure 1: (k,n) VTS for black and white image

1.2.2. (2,2)-Threshold VTS:

In this section we consider (2,2)-VTS for black and white images. In Naor and Shamir first proposed a (2,2)-VTS for black and white images. They constructed the 2 out of 2 visual secret sharing scheme by considering the two 2 × 2 basis matrices S^0 and S^1 given as follows.

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

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

When we encrypt a white pixel, we apply a random permutation to the columns of S^0 to obtain matrix *T*. We then distribute row *i* of *T* to participant *i*. To encrypt a black pixel, we apply the permutation to S^1. Two shares of a white pixel have a combined Hamming weight of 1, while that of a black pixel have a combined Hamming weight of 2, which looks darker. The relative contrast in this case is 1/2 while pixel expansion is 2.

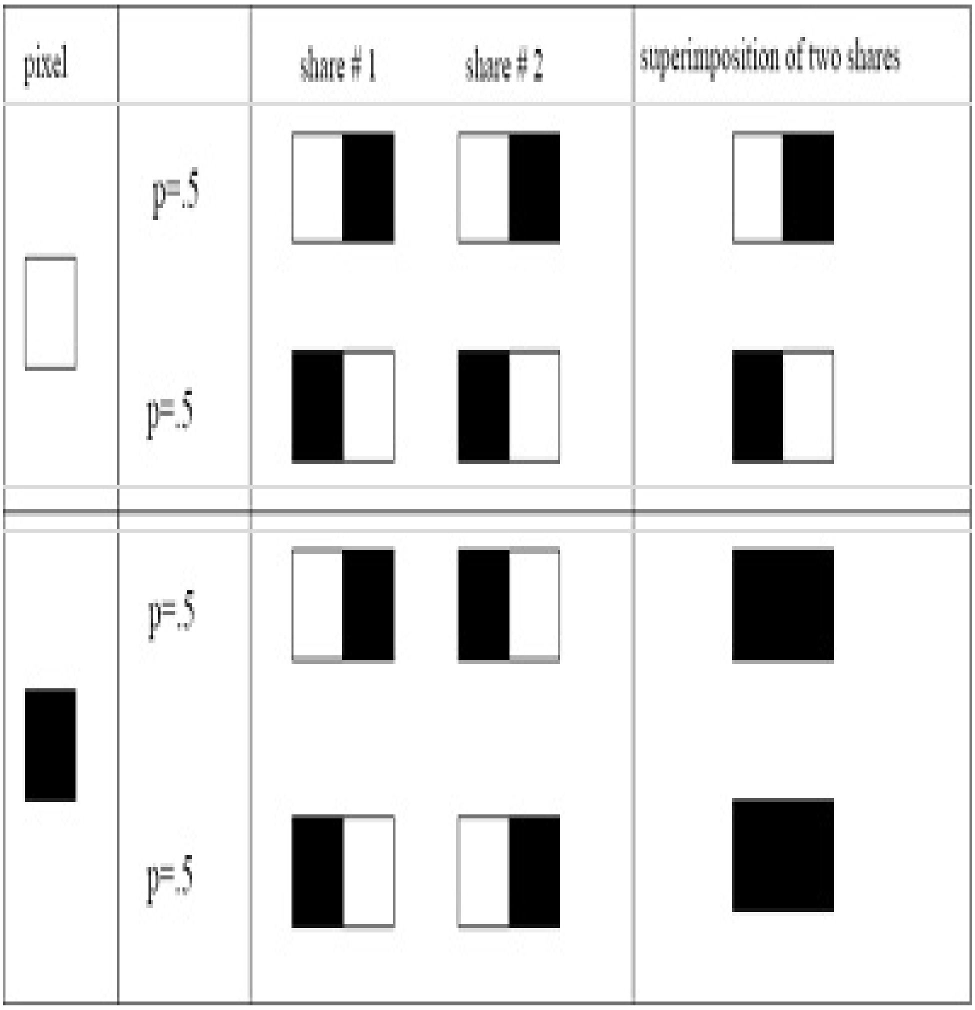


Figure 2: (2,2) VTS for black and white image

Chapter 2

Historical Background

2.1. Visual Cryptography of Tuyls model:

Tuyls proposed a new physical system for VCS, which can realise the XOR operation. Their main idea is to insert a new liquid crystal (LC) layer into a liquid crystal display (LCD) that already has an LC layer. Thus, such a system contains five layers which are the back-light, the first polariser, the first LC layer, the second LC layer and the second polariser. Depending on the voltage that is applied to an LC cell, this LC cell will rotate the polarisation of the light that enters it to a certain angle. The angle rotated by the cell of the first LC layer is denoted as $\alpha_1 \in [0, \pi]$ and that by the cell of the second LC layer as $\alpha_2 \in [0, \pi]$. Then, the total angle rotated by the two LC layers is denoted as $\alpha = \alpha_1 + \alpha_2$. The second polariser emits the same light of the first polariser. Let *I_r* denote the normalised intensity of the recovered pixel, then we have

$$I_r = \cos^2 \alpha = \cos^2(\alpha_1 + \alpha_2)$$

When $\alpha_1, \alpha_2 \in \{o, \pi / 2\}$, since $\cos(\pi) = \cos(0) = 1$, the system forms a black and white visual cryptography model with an underlying operation of XOR. As LC layers can be driven electronically (as in LCDs), the key can be easily updated (using pseudo random number generators), which leads to a practical updating mechanism. Finally, the encryption display will be rather simple, it is only equipped with simple dedicated hardware such as a pseudo random number generator and a storage device, and having interaction with the untrusted communication device, which is purely optical. These traits make this system practical.

2.2 Definition of VCS:

In general, a (k, n)-VCS divides a secret image into n shares, which are distributed to n participants. Any k out of n shares can recover the secret image, but any less than k shares do not have any information about the secret image other than the size of the secret image. Besides, a colour (k, n)-VCS should assume that the secret image, the shares and the recovered secret image are all colourful. Because all the constructions of colour VCS of this study take their corresponding black and white VCS as building blocks, in this section, we will give some definitions about the black and white VCS, where we denote a black pixel by1 and a white pixel by 0.

For a vector $v \in GF^{m}(2)$, we denote the Hamming weight of the vector *v* by $w(v)$ A black and white (k,n)-VCS, denoted by (*C$_0$*, *C$_1$*), consists of two collections of $n \times m$ binary matrices, *C$_0$* and *C$_1$*. To share a white (resp. black) pixel, a dealer (the one who sets up the system) randomly chooses one of the matrices in *C$_0$*(resp. *C$_1$*) and distributes its rows (shares) to the *n* participants of the scheme. More precisely, we give a formal definition of the black and white (k,n)-VCS as follows, where we use a dot $(\bullet)$ operation to denote an OR or XOR operation in a VCS.

Definition 1: Let *k*, *n*, *m* and *h* be non-negative integers satisfying $2 \leq k \leq n$ and $0 < h \leq m$. The two collections of $n \times m$ binary matrices (*C$_0$*, *C$_1$*) constitute a black and white (k,n)-VCS if there exists a value α (> 0) satisfying:

1. (Contrast) for any $s \in C_0$, the $\bullet$ operation of any *k* out of the *n* rows of *s* is a vector *v* that satisfies $w(v) \leq h - \alpha_m$.

2. (Contrast) for any $s \in C_1$, the $\bullet$ operation of any *k* out of the *n* rows of *s* is a vector v that satisfies $w(v) \geq h$.

3. (Security) for any $i_1 < i_2 < .... < i_t$. in $\{1,2,.........,n\}$ with $t < k$, the two collections of $t \times m$ matrices *D$_j$* , *j = 0, 1*,obtained by restricting each $n \times m$ matrix in *C$_j$* , *j = 0, 1,* to rows $i_1, i_2, ..., i_t$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

In the above definition,

1. v is the resulting vector of the restricted *k* out of the *n* rows under the operation ($\bullet$). The notation ($\bullet$) stands for the operation OR or XOR for the black and white VCS, and for colour VCS, the underlying operation of this study will be defined in Basic principles of colour models

2. m is the pixel expansion of the scheme.

3. α is called the contrast of the scheme.In Definition 1, the first two contrast conditions ensure that the stacking of *k* out of *n* shares can recover the secret image. The security condition ensures that, any less than *k* shares cannot obtain any information about the secret image other than its size.

We consider VCS where C_0 and C_1 are constructed from a pair of $n \times m$ matrices M_0 and M_1, which are called basis matrices. The set $C_i(i = 0, 1)$ consists of the *m!* matrices obtained by applying all permutations to the columns of M_i. This approach of VCS construction will have small memory requirements (it only keeps the basis matrices) and high efficiency [to choose a matrix in C_0(resp. C_1), it only needs to generate a permutation of the basis matrix]. In this paper, we denote $P(M_i)$ as a random column permutation of M_i.

2.3 Definition of EVCS:

In general, a (k,n)-EVCS takes a secret image and *n* original share images as inputs, and outputs *n* shares that satisfy the following three conditions: first, any *k* out of *n* shares can recover the secret image; secondly, any less than *k* shares cannot obtain any information about the secret image other than the size of the secret image; and thirdly, all the shares are meaningful images. Besides, a colour (k,n)-EVCS should fulfil the condition that the secret image, the original share images, the shares and the recovered secret image are all colourful.

Because all the constructions of colour EVCS of this study take their corresponding black and white EVCS as building blocks, in this section, we will give some definitions about the black and white EVCS. Note that, for the black and white EVCS, the colour of a pixel only has two possible values black and white. We denote $C_c^{c_1,\ldots\ldots,c_n}$ as the collections of matrices from which the dealer chooses a matrix to encrypt, where $c\ \ ,c_1,\ldots\ldots.,\ c_n \in \{1,0\}$ For $i = 1,\ldots..n,$ c_i is the colour of the pixel on the i_{th} original share image, and *c* is the colour of the secret image. Hence, to realise a black and white (k,n)-EVCS, we have to construct 2_n pairs of such collections $(c_0^{c_1\ldots.c_n}, c_1^{c_1\ldots\ldots\ldots c_n})$, one for each possible combination of white and black pixels in the *n* original share images. A black and white (k,n)-EVCS is defined as follows.

Definition 1: A family of *2n* pairs of collections of $n \times m'$ binary matrices *{* $(c_0^{c_1....c_n}, c_1^{c_1.........c_n})$ *}c1,...,cn ∈ {1,0},* constitute a black and white (k,n)-EVCS if there exist values $\alpha_F(>0), \alpha_S(>0)$ and *h* satisfying:

1. (Contrast) for any $M \in C_0^{c_1,....,c_n}$ the $\bullet$ operation of any *k* out of *n* rows of *M* is a vector *v* that satisfies $w(v) \leq (h - \alpha_F m')$, and for any $M \in C_1^{c_1,....,c_n}$, we have $w(v) \geq h$.

2. (Security) for any $i_1 < i_2 < \cdots\cdots < i_t$ in $\{1,2,....,n\}$ with *t* , *k,* the two collections of $t \times m'$ matrices $D_j^{c_1,...,c_n}, j = 0,1,$ obtained by restricting each $n \times m'$ matrix in $C_j^{c_1,...,c_n}$ to rows $i_1, i_2, \cdots\cdots, i_t$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

3. (Contrast) after the original share images are encrypted, the shares are still meaningful. Formally, for any $i \in \{1,2,....,n\}$ and any $c, c_1, ..., c_{i-1}, c_{i+1}, ..., c_n \in \{0,1\}$, with the *ith* row of *M* denoted as *M[i],* we have

$$\min_{M \in M_1} w(M[i]) - \max_{M \in M_0} w(M[i]) \geq \alpha_S m'$$

Where

$$M_1 = \bigcup_{c, c_1, ..., c_n \in \{0,1\}} C_c^{c_1,....,c_{(i-1)} 1 c_{(i+1)},....,c_n} \qquad \text{and}$$

$$M_0 = \bigcup_{c, c_1, ..., c_n \in \{0,1\}} C_c^{c_1,....,c_{(i-1)} 0 c_{(i+1)},....,c_n}$$

In the above Definition 2, m' is the pixel expansion of the black and white (k,n)-EVCS. α_F and α_S are the contrast of the recovered secret image and that of the shares, respectively. We consider EVCS where $S_c^{c_1,....,c_n}$ are constructed from the $n \times m'$ basis matrices $S_c^{c_1,....,c_n}$. The set $C_{cc1,...,cn}$ consists of the m_0! matrices obtained by applying all permutations to the columns of $S_c^{c_1,....,c_n}$. Denote $P(S_c^{c_1,....,c_n})$ as a random column permutation of $S_c^{c_1,....,c_n}$.

In Definition 1, the first and second conditions correspond to the contrast and security conditions of Definition 1, and the third condition implies that the original share images are not 'modified', that is, after we encrypt the *n* original images by using the *2n* pairs of collections$\{\left(C_0^{c_1,....,c_n},C_1^{c_1,....,c_n}\right)\}$,where $c_1,....., c_n \in \{0,1\}$, the encrypted shares are still meaningful.Naor and Shamir first mentioned a simple example of black and white EVCS in, that is, each share carries a meaningful image rather than a noise image. Droste proposed a new black and white EVCS that not only encrypts the shares with meaningful images but also decrypts different secret images by stacking different combinations of shares. Ateniese have formalised the framework of black and white EVCS for general access structures. All of the above schemes are under the visual cryptography model of Naor and Shamir that is, under the operation OR. However, for the general black andwhite (k,n)-EVCS under the visual cryptography model of Tuyls, that is, under the operation XOR, there are no such constructions. We propose a black and white (k,n)-EVCS under the XOR operation that is under the visual cryptography model of Tuyls. Also, based on the black and white (k,n)-EVCS, we propose a colour (k,n)-EVCS under the visual cryptography model of Tuyls.

Definition 2:

Denote *b* as the number of the black pixels in a block of *m* pixels. Denote e_b as the number of blocks, with *b* black pixels, which have already been encrypted. The multi-pixel encryption method of encrypts a block of m pixels and can be described as follows.

Algorithm 2:

Input: The secret image and the basis matrices for a black and white (k,n)-VCS, M_0 and M_1, which have pixel expansion *m*.

Output: The shares S_i for $i=1,\ldots,n$.

Step 1: Set $e_b \leftarrow 0$ for $b=1,2,\ldots,m$;

Step 2: Pick up a block of *m* pixels, $p_1, p_2,....., p_m$, in the secret image, and denote *b* as the number of black pixels among them;

Step 3: Put the *m* sub-pixels in the *ith* row of $p(M)$to the corresponding positions of $p_1, p_2,....., p_m$ in the ith share for $i = 1,\ldots,n$, where $p(M)$ is a random column permutation of M and the basis matrix *M* is decided as follows

If $e_b \bmod m < b$ then $M \leftarrow M_1$

else $M \leftarrow M_0$

Step 4: Set $e_b \leftarrow e_b + 1$;

Step 5: Repeat the Steps 2, 3 and 4 until all the pixels of the secret image are encrypted and output the *n* shares S_i for $i = 1,\ldots,n$.

For a block of m pixels that have *b* black pixels, Algorithm 1 shows a method to encrypt these *m* pixels with the basis matrices M_0 and M_1, where M_0 contributes with a probability of *b/m* and M_1 contributes with a probability of *(m-b)/m* exactly.By such a method, the recovered secret image has a better visual effect.

An example of Algorithm 1 can be found in Example 1. The security of the multi-pixel encryption method has been proved by Hou and Tu ; we refer to their result by the following theorem:

Theorem 1: Algorithm 1 generates *n* shares S_i for $i = 1,\ldots,n$, where less than *k* out of these *n* shares cannot obtain any information about the secret image other than the size of the secret image.

Proof: According to Algorithm 1, each block of *m* pixels in the secret image is encrypted by either $p(M_0)$ or $p(M_1)$ and because M_0 and M_1 are the basis matrices of a black and white (k,n)-VCS, which satisfies the security condition of Definition 1, i.e. given any less than *k* shares, then it cannot tell whether a block of *m* pixels in the secret image is encrypted by $p(M_0)$ or $p(M_1)$, as both are equally likely. Hence the conclusion of the theorem follows: Note that the multi-pixel encryption is a method to reduce the pixel expansion while maintaining better visual effect. However, for the encryption of a single pixel, the generated shares do not satisfy the contrast conditions of Definition 1 since a white pixel may occasionally be wrongly represented by a black pixel and vice versa.

2.3.1. Black and White (k,n)-VCS under the model of Tuyls:

Droste proposed an algorithm to construct (k,n)-VCS under the OR operation, that is, under the visual cryptography model of Naor and Shamir. In this section, we will prove that the basis matrices constructed by that algorithm is also a (k,n)-VCS under the XOR operation that is under the visual cryptography model of Tuyls. Droste's algorithm can be described as follows. First, we give a sub-routine ADD (*p*, *M*) which is used to add each restriction of *k* rows of a matrix *M* every column with *p* 1's by adding columns to the entire matrix *M*, where a matrix is considered as a collection of columns.

***ADD (p,M)*:**

1**:** If $p \le k - p$, add all the columns with $q = p$ 1's to *M*, that is, the number of columns of *M* is increased by $\binom{n}{q}$.

2: If $p \ge k - p$, add all the columns with $q = p + n - k$ 1's to *M*, that is, the number of columns of *M* is increased by $\binom{n}{q}$.

The sub-routine ADD (*p, M*) makes it easy to construct basis matrices *M₀*(resp. *M₁*) whose restrictions to *k* rows always contain every even (resp. odd) column (an even column is a one that contains even number of 1's; an odd column is one that contains odd number of 1's). When every even (resp. odd) column is removed once from every restriction of M_0 (resp. M_1), the remaining columns maintain the same, i.e., those remaining columns are unchanged regardless which *k* rows are restricted, and whether they are from M_0 or M_1. Hence, the remaining columns of every restriction of M_0, which are no remaining columns of every restriction of M_1, called the rest of M_0, have to be added to every restriction of M_1 and vice versa. In most cases, these added columns will create new rests which cause new columns to be added. The algorithm has the following form:

Algorithm 3:

Input: The parameters *k* and *n*, and two empty basis matrices M_0 and M_1, where the basis matrices M_0 and M_1 are considered as collections of columns;

Output: The basis matrices M_0 and M_1 for a (k,n)-VCS;

Step 1: For all even $p \in \{0,\ldots,k\}$, call ADD(*p*, M_0);

Step 2: For all odd $p \in \{0,\ldots,k\}$, call ADD(*p*, M_1);

Step 3: While the rests of M_0 and M_1 are not empty:

(a) Add to M_0 all columns adjusting the rest of M_1 by calling ADD.

(b) Add to M_1 all columns adjusting the rest of $\boldsymbol{M_0}$ by calling ADD.

Execute the Step 3 until the rests of M_0 and M_1 are empty.

Then, we show that Algorithm 2 also generates a (k,n)- VCS under the XOR operation.That is under the visual cryptography model of Tuyls.

Theorem 3: Algorithm 2 generates the basis matrices of a (k,n)-VCS, M_0 and M_1, under the XOR operation.

Proof: We need to prove that the basis matrices M_0 and M_1 satisfy the contrast and security conditions of Definition 1.

First, for the contrast condition, we need to prove that the Hamming weight of the stacking (XOR operation) of any *k* out of *n* rows of M_0 is less than that of M_1.

Denote M_0^k (resp. M_1^k) as the sub-matrix generated by restricting to arbitrary *k* rows of M_0(resp. M_1). According to the Steps 1 and 2 in Algorithm 2, it is clear that all the even (resp. m the even (resp. odd) columns of length *k*. Because Algorithm 2 terminates when the rests of M_0 and M_1 are empty, at implies that the remaining columns of M_0 and M_1 are the same, that is, $M_0^k \setminus I_0^k = M_1^k \setminus I_1^k$.Denote R as the remaining columns of M_0 and M_1, we have $M_0^k = I_0^k \cup R$ and $M_1^k = I_1^k \cup R$. Because the XOR (operation) of the entries of an even (resp. odd) column is 0 (resp. 1), we have that the Hamming weight of the stacking (XOR operation) of the rows of M_0^k is less than that of M_1^k. Hence, the contrast condition is satisfied.

Secondly, for the security condition, we need to prove that the sub-matrices of any less than *k* rows of *M0* and *M1* have the same columns, and only in such a case, all the column permutations of the two sub-matrices will generate the same collection, that is, the security condition is satisfied. Denote M_0^t(resp. M_1^t) as the sub-matrix generated by restricting to arbitrary *t* rows of *M0*(resp. *M1*), where $t < k$. Denote M_0^k (resp. M_1^k) as the sub-matrix generated by concatenating M_0^t (resp. M_1^t) and arbitrary *k* - *t* rows chosen from the remaining rows of *M0*(resp. *M1*) (other than the rows in M_0^t and M_1^t). As discussed above we have $M_0^k = I_0^k \cup R$ and $M_1^k = I_1^k \cup R$ where I_0^k(resp- I_1^k) is the matrix that contains all the even(resp.odd) columns of length *k*. Note that I_0^k and I_1^k are the basis matrices of a (k,k)-VCS proposed . We have that the sub-matrices generated by restricting to any *t* rows of I_0^k and I_1^k have the same columns.

Hence, the sub-matrices generated by restricting to any t rows of M_0^k and M_1^k have the same columns, that is, the security condition is satisfied.

2.3.2. Black and White (k,n)-EVCS under the model of Tuyls:

In this section, we propose a black and white (k,n)-EVCS under the visual cryptography model of Tuyls that is under the XOR operation, as follows:

Algorithm 3: Denote $S_c^{c_1,\ldots,c_n}$ as the basis matrix for that the *n* original share images have colour $c_1,\ldots., c_n$ and the secret image has colour *c* for $c_1,\ldots., c_n, c \in \{0,1\}$. Denote the binary matrices *M0* and *M1* as the basis matrices of a black and white (k,n)-VCS under the operation XOR, where all the rows of *M0* (resp. *M1*) have the same Hamming weight. Denote a as its contrast and m as its pixel expansion.

Step 1: Construct an $n \times l$ matrix *D* as follows (*l* is an integer satisfying $1 \le l < \alpha m$):

For $i = 1$ to *n* do

```
{
        If $c_i = 1$ then setall the entries of row $i$ in $D$ to 1.
            Else setall the entries of row $i$ in $D$ to 0.
}
```

Step 2: The basis matrices $S_c^{c_1,\ldots,c_n}$ are obtained by concatenating the matrix *D* with *M0* and *M1* that is

$$S_c^{c_1,\ldots,c_n} = [M_0, D], \text{ if } c = 0$$

$$= [M_1, D], \text{ if } c = 1$$

where the notation *[M, D]* means the concatenation of the two matrices *M* and *D*.

It is easy to verify that the above construction generates a general black and white (k,n)-EVCS under the operation XOR, and the basis matrices *M0* and *M1* can be the basis matrices constructed. If $\alpha \cdot m = 1$ holds, then, we can replace *M0* and *M1* by the matrices [*M0*, *M0*] and [*M1*, *M1*], respectively. Note that, the basis matrices generated always satisfy $\alpha m > 1$ hence, we can let $l = 1$for any access structure. In fact, Algorithm 3 is not restricted to threshold EVCS only; it can be applied to the general access structure EVCS given that *M0* and *M1* are the basis matrices of the general access structure VCS. Because of the lack of VCS for the general access structure, this paper only considers the threshold access structure for the case of EVCS. However, if such a VCS of the general access structure exists, then our approach can be applied to generate the corresponding EVCS under the operation XOR directly.

Formally, we have the following theorem:

Theorem 4: Algorithm 3 generates the basis matrices $S_c^{c_1,\ldots,c_n}$ for a black and white (k,n)-EVCS under the operation XOR, where c, c1, . . . , cn ∈ {0, 1}.

Proof: We need to prove that the basis matrices S satisfy the three conditions of Definition 2.

For the condition 1 of Definition 2: according to Algorithm 3, the pixel expansion of $S_c^{c_1,....c_n}$ is $m' = m + l$. Because *M0* and *M1* are basis matrices of the corresponding VCS, we have that the Hamming weight of the stacking results of any *k* out of *n* rows of $S_c^{c_1,....c_n} = [M_0, D]$ is at most $h - \alpha m + l$ and that of $S_c^{c_1,....c_n} = [M_1, D]$ is at least *h*. Hence

$$\begin{aligned}\alpha_F &= \frac{(h) - (h - \alpha m + l)}{m + l} \\ &= \frac{(\alpha m - l)}{m + l} > 0\end{aligned}$$

For the condition 2 of Definition 2: because *M0* and *M1* are basis matrices of the corresponding (k, n)-VCS, and $S_0^{c_1,....c_n}$ and $S_1^{c_1,....c_n}$ are generated by concatenating the same matrix *D* to *M0* and *M1*, and noting that $C_0^{c_1,....c_n}$ and $C_1^{c_1,....c_n}$ are the collections of all the permutations of $S_0^{c_1,....c_n}$ and $S_1^{c_1,....c_n}$, respectively, $C_0^{c_1,....c_n}$ and $C_1^{c_1,....c_n}$ satisfy the security condition 2 of Definition 2.

For the condition 3 of Definition 2: because all the rows of *M0*(resp. *M1*) have the same Hamming weight, by concatenating the matrix *D*, the difference between a white pixel and a black pixel in the share image is l and, hence,

$$\alpha_F = \frac{l}{m + l} > 0$$

In light of the above discussion, the theorem is proved. Two examples of black and white EVCS for the (2, 2) access structure are as follows (for operations XOR and OR, respectively):

Example 2: The first example is a black and white (2, 2)-EVCS under the visual cryptography model of Tuyls, that is under the operation XOR

$$S_0^{10} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \qquad S_1^{10} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$S_0^{11} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \qquad S_1^{11} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$S_0^{00} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \qquad S_1^{00} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$S_0^{01} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \qquad S_0^{01} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

The second example is a black and white (2, 2)-EVCS under the visual cryptography model of Naor and Shamir that is under the OR operation.

$$S_0^{10} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad S_1^{10} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S_0^{11} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \qquad S_1^{11} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

$$S_0^{00} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad S_1^{00} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

$$S_0^{01} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \qquad S_1^{01} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Comparisons:

In this section, we compare our constructions of colour (k,n)- VCS and colour (k,n)-EVCS with known results in the literature. In the comparisons are on the following criteria:

C1 : The pixel expansion of colour (k,n)-VCS under the visual cryptography model of Naor and Shamir;

C2 : The pixel expansion of colour (k,n)-EVCS under the visual cryptography model of Naor andShamir;

C3: The pixel expansion of colour (k,n)-VCS under the visual cryptography model of Tuyls;

C4: The pixel expansion of colour (k,n)-EVCS under the visual cryptography model of Tuyls;

C5: Whether or not the construction is based on the halftone technique;

C6: Whether or not the increase in the number of colours of the recovered secret image will increase the pixel expansion;

C7: Whether or not the colour model of the construction considers the colour darkening phenomenon during stacking of pixels with the same colour;

C8: Whether or not the recovering of the secret image requires the assistance of computing devices.

Chapter 3

Proposed Method

3.1. The model:

Let $p = \{1,\ldots\ldots n\}$ be a set of elements called participants, and let 2^P denote all the subsets of p .Let $\Gamma_{Qual} \subseteq 2^P$ and $\Gamma_{forb} \subseteq 2^p$, where $\Gamma_{Qual} \bigcap \Gamma_{forb} = \phi$ We refer to members of Γ_{Qual} as qualified sets and we call the members of Γ_{Forb} as forbidden sets. The pair ($\Gamma_{Qual}, \Gamma_{Forb}$) is called the access structure of the scheme.

Define Γ_0 to consist of all the minimal qualified sets:

$$\Gamma_0 = \{ A \in \Gamma_{Qual} : A' \notin \Gamma_{Qual} \text{ for all } A' \subseteq A,\ A' \neq A \}$$

We will refer to a participant $x \in p$ as an essential participant if there exists a set $X \subseteq P$ such that $X \cup \{P\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. If a participant *P* is not essential then we can construct a visual cryptography scheme giving him nothing as share. In fact, a nonessential participant does not participate “actively” in the reconstruction of the image, that is the information he has is not needed by any set in *P* in order to recover the shared image. Therefore, any VCS handling nonessential participants can give to these participants nothing as share.

We assume that the message 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 subpixels. The resulting structure can be described by an n × m Boolean matrix S = $[s_{ij}]$ where $s_{ij} = 1$ iff the j_{th} sub pixel in the i_{th} transparency is black. Therefore the gray level of the combined share, obtained by stacking the transparencies i_1,......, i_s, is proportional to the Hamming weight $w(V)$ of the m-vector V = OR (r_{i1},....., r_{is}), where r_{i1},....., r_{is}, are the rows of S associated with the transparencies we stack. This gray level is interpreted by the visual system of the users as black or as white in according with some rule of contrast.

Definition 3.1 Let ($\Gamma_{Qual}, \Gamma_{Forb}$) be an access structure on a set of n participants. Two collections (multisets) of n × m boolean matrices C_0 and C_1 constitute a visual cryptography scheme ($\Gamma_{Qual}, \Gamma_{Forb}, m$) VCS if there exist values $\alpha(m)$ and $\{t_x\}_{X \in \Gamma_{Qual}}$ satisfying:

1. Any qualified set X = { $i_1, i_2, \ldots\ldots, i_p$ } $\in \Gamma_{Qual}$ can recover the shared image by stacking their transparencies.

Formally, for any M $\in C_0$, the "or" V of rows $i_1, i_2, \ldots\ldots, i_p$ satisfies $w(v) \le t_x - \alpha(m) \cdot m$; whereas, for any M $\in$ C_1 it results that $w(V) \ge$ t_X .

2. Any nonqualified set X = $\{i_1, i_2, \ldots\ldots, i_p\} \in$ Γ_{Forb} has no information on the shared image. .

Formally, the two collections of $p \times m$ matrices D_t, with $t \in$ {0, 1}, obtained by restricting each $n \times m$ matrix in C_t to rows $i_1, i_2, \ldots\ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Each pixel of the original image will be encoded into n pixels each one consisting of m subpixels. To share a white/black pixel the dealer randomly chooses one of the matrices in C_0 / C_1 and distributes row i to participant i. The chosen matrix defines the color of the m subpixels in each one of the n transparencies. Observe that the size of the collections C_0 and C_1 does not need to be the same.

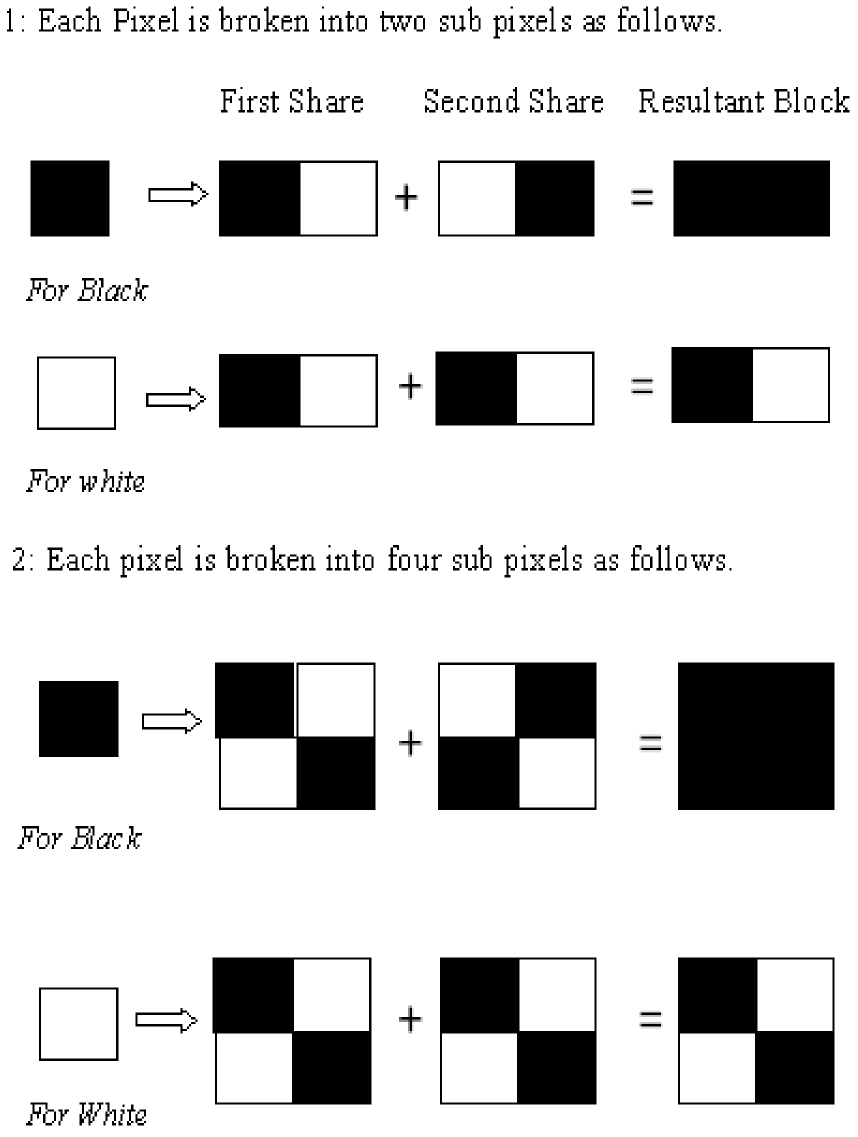
The first condition is related to the contrast of the image. It states that a qualified set of users, belonging to the basis of the access structure, stacking their transparencies can correctly recover the image shared by the dealer. The value $\alpha(m)$ is called relative difference, the number $\alpha(m) \cdot m$ is referred to as the contrast of the image, and the set $\{t_x\}_{X \in \Gamma_{Qual}}$ is called the set of thresholds. We want the contrast to be as large as possible and at least 1 subpixel over the m subpixels, that is, $\alpha(m) \ge 1/m$

The second condition is called security, it implies that by inspecting the shares of a nonqualified subset of participants one cannot gain any advantage in deciding whether the shared pixel was white or black.

3.2 Basic approach:

Basic visual cryptography is based on breaking of pixels into some sub pixels or we can say expansion of pixels. Figure shows two approaches for (2, 2) – Threshold VCS.

In this particular figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=BT or TB+TB=TB.



1: Each Pixel is broken into two sub pixels as follows.

2: Each pixel is broken into four sub pixels as follows.

Figure 3: Visual Cryptography

Chapter 4
Simulation Results

4.1 General Access Structure:

In this section we have implemented a general access structure using the scheme proposed by A. Adhikari in [1].It is based on the idea that the col lection of all the solutions of a system of linear homogeneous equations over the binary field forms a vector space over the base field.The basis matrix S^0 is constructed whose columns are all the possible solutions of a system of linear homogeneous equations. Another basis matrix S^1 is constructed by considering all solutions of a system of non-homogeneous linear equations.

In this project we have implemented a general access structure where we have a boss B, 2 managers $M_1 \& M_2$ and 2 users $U_1 \& U_2$.The qualified sets include $\{B, M_1, U_1\}$ and $\{B, M_2, U_2\}$.The basis matrices $S^0$and S^1 in this case can be obtained by solving the following system of linear equations:

$$\begin{aligned} b + m_1 + u_1 &= 0 \\ b + m_2 + u_2 &= 0 \rightarrow (1) \end{aligned}$$

$$\begin{aligned} b + m_1 + u_1 &= 1 \\ b + m_2 + u_2 &= 1 \rightarrow (2) \end{aligned}$$

The solution of the these linear equations gives us the Basis Matrices.
The solution of the equations of set (1) gives us the matrix S^0 and that of set (2) gives us the matrix S^1.

The Matrices are :

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

If we take "OR" of rows of any allowed set of parcipants, (namely 1st, 2nd, 4th or 1st, 3rd, 5th) the weight in S^1 is greater than that in S^0. For any other combination the weight is same in both the basis matrices. Thus, any set other the qualified one cannot obtain the secret on stacking their respective shares. The pixel expansion in this case is 8. The weight on doing the "OR" operation in case of is 8, while it is 6 in the case of S^0 thereby producing a relative contrast of 1/4.

4.2 (3,n)-VTS using BCH Codes:

4.2.1. Construction of (k,k)-VTS:

The construction of (k,n)-VTS requires the use of initial matrices used in (k,k)-VTS. The (k,k)-VTS was first proposed by Naor and Shamir .

Consider a ground set $w = \{1,2,.......,k\}$ of k elements and let $\pi_1, \pi_2, ..., \pi_{2^{k-1}}$ be a list of all subsets of w of even cardinality and let $\alpha_1, \alpha_2, ..., \alpha_{2^{k-1}}$ be a list of all subsets of w of odd cardinality. Each list defines the following $k \times\ 2^{k-1}$Boolean matrices S^0 and S^1 : For$1 \le i \le k$ and $1 \le\ j \le\ 2^{k-1}$ let $S^0[i, j] = 1$ iff $i \in\ \pi_j$ and $S^1[i, j] = 1$ iff $i \in \alpha_j$ These two matrices satisfy the definition of basis matrices for k out of k schemes.

In our case we have constructed the basis matrices for the (3,3)-VTS. The subsets of odd cardinality of the set {1,2,3} in this case include {1}, {2}, {3}, {1,2,3} and the sets of even cardinality are φ, {1,2}, {2,3}, {1,3}.

Therefore the matrices S^0 and S^1 are given by

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

4.2.2 Initial Matrix:

For the construction of $(k,n)-$VTS described in [3] we need an initial matrix which is defined as follows.

Definition 4.1 Let n,l,k be integers such that k/n. An initial matrix $IM(n,l,k)$ is an $n \times l$ matrix whose entries are elements of a ground set A = {a_1, a_2,......, a_k} in which the set of columns is equal to the set of vectors in which each element of A appears n/k times.

The number of columns, l, of an initial matrix $IM(n,l,k)$ is equal to the number of ”anagrams” of the word

$a_1 .....a_1$ (n/k times) …. $a_i ,....a_i$ (n/k times) …. $a_k ,....a_k$ (n/k times)

that is ,

$$l = \frac{n!}{((n/k)!)^k}$$

Given an initial matrix $IM(n,l,k)$ we can construct a (k,n) thresholdVCS as follows:

The n × $(l \cdot 2^{k-1})$ basis matrices S^0 and S^1 are constructed by replacing the symbols a_1, a_2,......, a_k respectively, with the $1_{st}, 2_{nd}$,......, k_{th} rows of the corresponding basis matrices T_k^0 and T_k^1 of the (k,k) threshold VCS .

The pixel expansion and Relative Contrast in this case are

$$m = \frac{n!}{((n/k)!)^k} \cdot 2^{k-1} \quad \text{and} \quad \alpha(m) = \frac{(n/k)^k}{\begin{pmatrix} n_0 \\ k \end{pmatrix} \cdot 2^{k-1}}$$

4.2.3. Orthogonal arrays and BCH codes

In this section we describe how we can use the orthogonal arrays to minimize the pixel expansion. The orthogonal arrays are created using the BCH codes.

Definition 4.2 A cyclic code of length n over GF(q) is a BCH code of designed distance δ ,if for some integer b ≥ 0,

$$g(x) = l.c.m.\{M^{(b)}(x), M^{(b+1)}(x), ..., \ M^{(b+\delta-2)}(x)\}$$

i.e $g(x)$ is the lowest degree monic polynomial over GF(q) having $\alpha^b, \alpha^{b+1}, ..., \ \alpha^{b+\delta-2}$ as zeroes.

Definition 4.3 An orthogonal array $OA_\lambda(t,k,v)$ is a $\lambda v^{t\backslash} \times k$ array, say A, of elements from a set X of cardinality v, with the property that within any t columns of A every possible t-tuple of elements from X occurs in exacty λ rows.

The next theorem establishes the relationship between orthogonal arrays and (k,n)-VTS.

Theorem 1: Suppose there exists an $OA_\lambda(t,k,v)$. Then there exists a strong (k,n)-threshold VCS with $m = \lambda k^k 2^{k-1}$ and

$$\alpha(m) = \frac{(k-1)!}{(2k)^{k-1}}$$

Proof: The construction is the same as before, except that the initial matrix is replaced by the transpose A^T of an $OA_\lambda(t,k,k)$. Note that A^T has n rows and λ ・ k^k columns.

We compute the contrast in the resulting (k,n) threshold VCS. Fix any *k* rows of *AT* . Here also α(m) ・ m equals the number of columns of A^T in which *k* distinct symbols occur in the *k* given rows. Since A is an orthogonal array, there are λ such columns for every permutation of the *k* symbols. Hence,

$$\alpha(m) \cdot m = \lambda \cdot k!$$

Since $$m = \lambda k^k 2^{k-1}$$

It fallows that

$$\alpha(m) = \frac{(k-1)!}{(2k)^{k-1}} \qquad \text{as desired.}$$

Lemma 4.1: If there exists an $[n,l,d]_q$ code, then there exists an $OA_\lambda(d-1,n,q)$ where $\lambda = q^{n-l-d+1}$.

Proof: Let C be the hypothesized $[n,l,d]_q$ code, and let $C^\perp$ be the dual code to C (i.e., the orthogonal complement of C in (GF(q))^n). If we construct the q^{n-1} × n array A whose rows are the codewords in $C^\perp$, then it can be shown that A is an $OA_\lambda(d-1,n,q)$.

Corollary 4.1: If there exists an $[n,l,d]_q$ code, then there exists a (q, n)-threshold VCS with $m = q^{n-1}2^{q-1}$ and

$$\alpha(m) = \frac{(q-1)!}{(2q)^{q-1}}.$$

4.3 Details Of the Construction:

In this section we describe how did we actually generate the BCH codes and used them for the construction of (3,8)-VTS. For a (3,8)-VTS, we need a $[8,4,4]_3$ BCH code by the theorem in the previous section.We first construct the finite field GF(3^2) using the polynomial $x^2 + x + 2$ which is irreducible over GF(3). Let α be the root of this polynomial in the extension field. Therefore the field is given by

$$\begin{array}{lll}
00 = 0 & & = \alpha^{-\infty} \\
10 = 1 & & = \alpha^{0} \\
01 = \alpha & & = \alpha^{1} \\
12 = 1 + 2\alpha & & = \alpha^{2} \\
22 = 2 + 2\alpha & & = \alpha^{3} \\
20 = 2 & & = \alpha^{4} \\
02 = 2\alpha & & = \alpha^{5} \\
21 = 2 + \alpha & & = \alpha^{6} \\
11 = 1 + \alpha & & = \alpha^{7}
\end{array}$$

Associated with each element of the field is an irreducible polynomial called its minimal polynomial.

Definition 4.3 The minimal polynomial over GF(p) of β is the lowest degree monic polynomial M(x) with coefficients from GF(p) such that

$$M(\beta) = 0$$

In case of GF(3^2) the minimal polynomial for α and α^3 is $x^2 + x + 2$ while for α^2 it is $x^2 + 1$. The generator polynomial g(x) for $[8,4,4]_3$ BCH code is therefore given by the l.c.m. of the minimal polynomial of α ,α^2,and, α^3.

$$g(x) = l.c.m.\{M^{(1)}(x), M^{(2)}(x), M^{(3)}(x)\}$$

$$= l.c.m.\{ x^2 + x + 2 , x^2 + 1\}$$

$$= x^4 + x^3 + x + 2$$

The codewords thus, are given by all polynomials of degree less than 8 over GF(3) which are the multiples of this generator polynomial ,i.e. all the polynomials of the form

$$r(x) = g(x) \cdot q(x)$$

4.4 (3,n)-VTS using Canonical Matrices:

4.4.1. Canonical Matrices:

In this section we consider basis matrices containing all the columns of a given weight each occurring with the same frequency . Such matrices are called canonical.

Definition .1 Let (S^0, S^1), be the basis matrices of a (k,n) - threshold VCS. They are in canonical form if , for i = 0, 1, the following two properties are satisfied.

1. For any two columns c and c′ such that w(c) = w(c′) it results that $f_{c,i} = f_{c',i}$, where $f_{c,i}$ denotes the multiplicity of the column c in S^i .

2. For any column c it results that

$$f_{c,i} = f_{c',i} \qquad \text{if k is even}$$

$$= f_{c',1-i} \qquad \text{if k is odd .}$$

Theorem 2: S(h_0) and S(h_1) are basis matrices of a (k,n)-threshold VCS with pixel expansion *m* and contrast *a* if the following properties are satisfied:

1. $\sum_{j=0}^{n}\binom{n}{j}h_{j,0} = \sum_{j=0}^{n}\binom{n}{j}h_{j,1} = m.$
2. $\sum_{j=l'}^{n-l+l'}\binom{n-l}{j-l'}h_{j,0} = \sum_{j=l'}^{n-l+l'}\binom{n-l}{j-l'}h_{j,1}$, for $1 \le l \le k-1$ and $0 \le l' \le l$
3. $\sum_{j=0}^{n-k}\binom{n-k}{j}(h_{j,0} - h_{j,1}) = \alpha m.$

where $h_{j,i}$ is the multiplicity of a column of weight j in S^i , i.e., $h_{j,i}$ = $f_{c,i}$ if w(c) = j.

Proof. Suppose that S(h_0) and S(h_1) are basis matrices for a VCS with the stated parameters. The number of columns in S(h_i) (i = 0, 1) is

$$\sum_{j=0}^{n}\binom{n}{j}h_{j,i} \qquad \text{Therefore property 1 holds.}$$

Next, let c be a binary column l-tuple, where $0 \le l \le k-1$. Suppose that the weight of *c* is l' (note that $l' \le$ *l*). Fix *l* rows of S(h_0) and S(h_1), say the first *l* rows. The number of occurences of *c* as a column of S(h_i)[{1,…….*l* }] is

$$\sum_{j=0}^{n-1}\binom{n-l}{j-l'}h_{j,i},$$

for i = 0,1. Therefore property 2 holds.

Finally, we look at the weight of the OR of *k* rows of S(h_0) and S(h_1) , say the first *k* rows. If we let X = {1, . . . , k} then

$$w(s(h_1)_x) - w(s(h_0)_x) \ge \alpha m .$$

Let $\in_i$ denote the number of occurences of $(0, . . . ,)^T$ as a column of S(h_i)[X], for i = 0,1.

It is easy to see that

$$w(S(h_i)_X) = m - \in_i$$

for i = 0,1. Hence,

$$w(S(h_i)_X) = -\sum_{j=0}^{n-k} \binom{n-k}{j} h_{j,i},$$

for i = 0,1. Therefore property 3 holds.Conversely, if properties 1-3 hold, it is easy to see that S(h_0) and S(h_1) are basis matrices for a VCS with the stated parameters.

4.4.2. Details of the Construction:

In this section we provide, a construction for (3,8)-VTS using canonical matrices describe in [4] using Canonical matrices.

For any $n \geq 4$ and any integer $1 \leq g \leq n/2$, consider the visual cryptography scheme whose basis matrices are in canonical form, denoted by S(3, n, g), described by the following $h_{j,i}s$.

$$h_{0,0} = h_{n,1} = \binom{n-1}{g} - \binom{n-1}{g-1} \quad \text{and} \quad h_{n-g,0} = h_{g,1} = 1$$

where as all the remaining $h'_{j,i}s$ are equal to zero.This is a strong $(3,n)$-threshold VCS as shown by the following theorem.

Theorem 3: For any n ≥ 4 and any integer$1 \leq g \leq n/2$, the scheme S(3, n, g) described earlier is a strong (3, n)-threshold VCS having pixel expansion and contrast equal to

$$m = 2\binom{n-1}{g} \quad \text{and} \quad \alpha = \frac{g(n-2g)}{2(n-1)(n-2)},$$

respectively.

In this project, for implementing the (3,8)-VTS, we have used the value of g as above.

2. Thus according to the formula given above h $_{j,i}$ is equal to

$$h_{0,0} = h_{n,1} = \begin{pmatrix} n-1 \\ g \end{pmatrix} - \begin{pmatrix} n-1 \\ g-1 \end{pmatrix} \quad \text{and} \quad h_{n-g,0} = h_{g,1} = 1$$

$$= \begin{pmatrix} 7 \\ 2 \end{pmatrix} - \begin{pmatrix} 7 \\ 1 \end{pmatrix}$$

$$=14$$

Thus in S^0 we have 14 columns of 0′s and 28 columns of weight 6. S^1 has 14 columns of weight 8 and 28 columns of weight 2.

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

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

Chapter 5

Colour visual cryptography

5.1. Basic principles of colour models:

The additive and subtractive colour models are widely used to describe the constitutions of colours. In the additive colour model, the three primary colours are red, green and blue (RGB), with desired colours being obtained by mixing different RGB channels. By controlling the intensity of red (resp. green or blue) channel, we can modulate the amount of red (resp. green or blue) in compound light. The more the mixed-coloured light, the more is the brightness of the light. Mixing the red, green and blue channels of equal intensities, results in white colour light. The computer screen is a good example of the additive colour model. In the subtractive colour model, the colour is represented by applying the combinations of coloured light reflected from the surface of an object (because most objects do not radiate by themselves). For example take an apple under natural light; the surface of the apple absorbs the green and blue parts of the natural light and reflects the red light to human eyes and, thus, it becomes a red apple.The more the pigment added, the lower is the intensity of the light is, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colours of pigment, which cannot be composed from other colours. In the computer, a natural colour image can be divided into three colour channels: red, green and blue (or equivalently cyan, magenta and yellow), and each channel will constitute a grey-level image, where each pixel can be represented by a binary value of 8 bits. Denote $x_{(p,q)} = [x_{(p,q)1}, x_{(p,q)2}, x_{(p,q)3}]$ as the colour of a pixel located at the position (p,q) of a colour image of size $k_1 \times k_2$ for p = 1, 2, . . . , K_1 and q = 1, 2, . . . , K_2. Let t describe the colour channel (e.g. t = 1 for red, t = 2 for green and t = 3 for blue) and the colour component $x_{(p,q)t}$ is coded with a binary value of 8-bits allowing $x_{(p,q)t}$ to be an integer value between 0 and 28 - 1 = 255 and, hence, the colour of the pixel $x_{(p,q)}$ can be expressed in a binary form as follows.

$$x_{(p,q)} = \sum_{i=1}^{8} x_{(p,q)}^{i} 2^{(8-i)}$$

Where $x_{(p,q)}^{i} = [x_{(p,q)1}^{i}, x_{(p,q)2}^{i}, x_{(p,q)3}^{i}] \in \{0,1\}^3$ denote the binary vector at the ith bit-level, with i =1 denoting the most significant bit and i = 2 denoting the second most significant bit. In such a way, a natural colour image is divided into 24 binary images. By the grey level of a pixel, we mean the darkness of the pixel appears for each colour channel. In this study, we divide the distance between a black and a white pixel, for each colour channel, into 256 grey levels. Define the grey level 0 for a complete white pixel, and the grey level 255 for a complete black pixel. Note that this definition of black and white pixels is just the opposite to their traditional definitions on computer. Under this definition, the 1's and 0's in the binary representation of the grey level correspond to black and white bits, which is consistent with their definitions in visual cryptography.

Because we divide 256 grey levels for each colour channel, each colour channel can be expressed by a binary vector of 8 bits. bit-levels should be assigned with different For example, we can print a pixel with a grey level a1 for the most significant bit, and a2 for the second most significant bit under the visual cryptography model of Naor and Shamir. For the VCS under the visual cryptography model of Tuyls, we rotate through an angle (a1/256 . π/2) for the most significant bit, and through (a2/256 . π/2) for the second most significant bit and so on, where $a_i \in [0,255]$, for $i \in \{1,.......,8\}$ Then, we show the principles of the colour superimposition for the visual cryptography model of Naor and Shamir and those of Tuyls, respectively. To simplify the discussion, we take one colour channel as an example. First, for the visual cryptography model of Naor and Shamir, the basic principle of the colour by superimposing two pixels is defined as follows: for a pixel with a grey level a_i and a pixel with a grey level a_j, the grey level of the result pixel by stacking the two pixels will be $(255-((255-a_i)(255-a_j)/255))$. This definition of colour superimposition is widely accepted. We define the grey level 255 as the black pixel and grey level 0 as the white pixel. Secondly, for the visual cryptography model of Tuyls, the basic principle of the colour by superimposing the shares is defined as follows: for a pixel with a grey level a_i and a pixel with a grey level a_j , which are realised by rotating the angles $(a_i / 256 \cdot \Pi / 2)$ and $(a_j / 256 \cdot \Pi / 2)$ for the first and the second LC layers, respectively, the grey level of the super imposition of the two pixels will be a_i + a_j, which is realised by rotating through an angle $(a_i + a_j) / 256 \cdot \Pi / 2$.

5.2. Multi-pixel encryption method:

In most cases, the encryption of the VCS causes the expansion of the shares, which will lower the resolution of the recovered secret image and enlarge the storage of the shares. Ito and Yang propose a method that encrypts a pixel by randomly choosing a column in the basis matrix; this method results in no pixel expansion. Unfortunately, the recovered secret image appears to be a clutter; many noise-like pixels appear in the recovered secret image. To mitigate this phenomenon, Hou and TU proposed a new method in, which encrypts a block of *m* pixels at a time. This method results in no pixel expansion. In this paper, we make use of the multi-pixel encryption method to reduce the pixel expansion of our colour VCS. Denote M_0 andM_1 as the $n \times m$ basis matrices for a black and white (k, n) -VCS, which satisfy the colour visual cryptography scheme (VCS) under the visual cryptography model of Naor and Shamir.

5.3 Constructions of the (k, n) -VCS and the (k, n) -EVCS :

. The first approach to realise colour VCS is to print the colours in the secret image on the transparencies directly. This approach has the following disadvantages. First, this approach often generates colour VCS with large pixel expansion. Secondly, this approach can only represent a small number of colours, the reason being that the pixel expansion of the colour VCS generated by this approach is related to the number of colours in the recovered secret image, and the pixel expansion grows rapidly when the number of colours in the recovered secret image increases. Hence, given a reasonable pixel expansion in the practical sense (which cannot be too large), the recovered secret image can only represent a small number of colours. Thirdly, the colour model of this approach assumes that the stacking of pixels with the same colour will result in a pixel that has the same colour (such an assumption is used to simplify the constructions). However, it is not true. The stacking of some lighter pixels will result in a darker pixel. For example, the stacking of two red pixels will result in a wine pixel different from the original red pixel. This is the colour darkening phenomenon because of stacking the pixels with the same colour.

The second approach to realise colour visual cryptography is to convert a colour image into black and white images on the three colour channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the colour channels. This method can obtain smaller pixel expansion, but requires the halftone process, which decreases the quality of the secret image and which often results in the expansion of the input images. Halftoning is a process of converting a gray scale image into a binary image. The halftoning technique is required in many present applications such as facsimile (FAX), electronic scanning and copying, and laser printing etc.

The third approach to realise colour visual cryptography is proposed by Lukac and Plataniotis. Their method can recover the secret image perfectly and requires only little computation. Their method utilises the binary representation of the colour of a pixel and encrypts the representation of the colour of a pixel and encrypts the secret image at the bit-level. However, the method has pixel expansion m and needs the assistance of computing devices for decrypting, and can only be applied under the visual cryptography model of Naor and Shamir.

The colour VCS under the visual cryptography model of Tuyls is attractive since it has good colour, resolution and contrast properties. For example, the (n,n)-VCS under the visual cryptography model can recover the secret image perfectly. However, the colour VCS for general (k,n) access structure has not been studied, not to mention the colour EVCS. This paper tries to construct a general colour (k,n)-VCS and a colour (k,n)-EVCS under the visual cryptography model of Tuyls.

The main idea of our construction of colour (k,n)-VCS and colour (k,n) EVCS is that, for each pixel in the secret image, we first represent its colour by binary bits with several bit-levels. Then, we encrypt the bits at each bit-level by applying the corresponding black and white VCS and EVCS, where a corresponding VCS (resp. EVCS) is the VCS (resp. EVCS) that has the same access structure and under the same visual cryptography model. Compared with the known results in the literature, the advantages of our constructions are as follows. First, compared with the first approach of realizing colour VCS, the pixel expansion of our constructions is small, and our constructions have the ability to represent all colours. Our colour model also considers the colour darkening phenomenon when stacking the pixels with the same colour, which makes our constructions more practical. Second, compared with the second approach of realising colour VCS, our constructions do not need the halftone process while maintaining small pixel expansion. Third, compared with the third approach of realising colour VCS, our constructions do not need the assistances of computing devices

Input: Denote the $n \times m$ matrices *M₀* and *M₁* as the basis matrices of a corresponding black and white (k,n)-VCS under the visual cryptography model of Naor and Shamir. Denote the $n \times m'$ matrices $M_{C}^{C_1......C_n}$. as the basis matrices of a corresponding black and white (k,n)-EVCS under the visual cryptography model of Naor and Shamir, where $c_1,.......c_n \in \{0,1\}$, Denote a_j as the grey level of 1's at bit-level j, $j \in \{1,2,\ldots.8\}$

Output: The shares S_i for $i = 1\ldots.n$.

Step 1: Represent the grey levels of each colour channel (*C*,*M* and *Y*, respectively) of all the pixels in the secret image by vectors of 8 bits, that is, the secret image is divided into 8 bit-levels and each bit-level forms a binary image.

Step 1': Represent the grey levels of each colour channel (*C*,*M* and *Y*, respectively) of all the pixels in the secret image (resp. the *n* original share images) by vectors of 8 bits, that is, the secret image (resp. the *n* original share images) is divided into 8 bit-levels and each bit-level forms a binary image.

Step 2: For each bit-level *j* and each colour channel, choose a block of *m* pixels in the binary secret image, and encrypt the *m* bits by applying Algorithm1 for the colour channels *C,M* and *Y* and bit-levels $j \in \{1,2,\ldots.8\}$ respectively, in which replace the 1's in *M*0 or *M*1 by the grey level *a*j and leave the 0's intact.

Step 2': For each bit-level *j* and each colour channel, encrypt a bit by $p(M_c^{c_1,\ldots\ldots,c_n})$ for the colour channels *C,M* and *Y* and bitlevels $j \in \{1,2,\ldots.8\}$ respectively, in which $p(M_c^{c_1,\ldots\ldots,c_n})$ is a random column permutation of $M_c^{c_1,\ldots\ldots,c_n}$ and replace the 1's in $p(M_c^{c_1,\ldots\ldots,c_n})$ by the grey level *aj* and leave the 0's intact.

Step 3: Repeat the steps 1 and 2 (resp. 1' and 2') until all the pixels in the secret image have been encrypted. Then, we obtain the shares $s_1^{i,t}, s_2^{i,t}, \ldots\ldots\ldots s_8^{i,t}$ where $i \in \{1,\ldots\ldots,n\}, t \in \{C,M,Y\}$ and the share $s_j^{i,t}$ is denoted as the share for the participant *i* at the bit-level *j* for the colour channel *t*.

Step 4: Each participant i is distributed with a share Si, where Si is generated by stacking the shares at the different bit-levels and of the different colour channels $s_1^{i,c}, s_2^{i,c}, \ldots\ldots\ldots s_8^{i,c}$, $s_1^{i,M}, s_2^{i,M}, \ldots\ldots\ldots s_8^{i,M}$, $s_1^{i,Y}, s_2^{i,Y}, \ldots\ldots\ldots s_8^{i,Y}$ for $i \in \{1,2,\ldots.n\}$.

In Construction 1, Steps 1 and 1' divides the secret image (resp. the n original shares images) into 8 bit-levels and three colour channels. In fact, the colour images stored in the computer, such as the bitmap image file, are of this format.

Then, in Steps 2, 2' and 3, we encrypt each bit-level and colour channel, respectively. More specifically, when we encrypt the binary secret image at bit-level *j* by applying the corresponding black and white (k,n)-VCS, for the bitlevel *j,* we print pixels with grey level *aj* for the 1's of *M0, M1* and $M_c^{c_1\ldots\ldots\ldots c_n}$, and leave the pixel intact for the 0's of *M0, M1* and $M_c^{c_1\ldots\ldots\ldots c_n}$.Then, we construct 24 shares in total for each participant, that is, the shares $s_{i,c}^1, s_{i,c}^2, \ldots. s_{i,c}^8$ $s_{i,M}^1, s_{i,M}^2, \ldots. s_{i,M}^8$, $s_{i,Y}^1, s_{i,Y}^2, \ldots. s_{i,Y}^8$. The final shares for the participants are constructed by superimposing the 24 shares in Step 4. One can easily observe that shares at the bit-level *j* can recover the *j*th binary image (bit-level) of the secret image visually. Thus, by superimposing the shares of all the bit-levels, the original secret image appears visually with all the bit-levels. We need to point out that, taking the characteristic of the human visual system into consideration, the dealer does not need to generate all the shares for all the bit-levels, since the information about a higher bit-level is not as important as that of a lower bit-level for the human visual system, that is, the dealer only generates the shares for several lower bit-levels in the practical sense. In Examples 1 and 3, we only generated the shares for the most and second most significant bit-levels. In Step 2, Algorithm 1 encrypts a block of *m* pixels at a time by using the *m* columns of the basis matrices, which results in no pixel expansion. For general colour (k,n)- VCS, one can make use of the basis matrices of the corresponding black and white (k,n)-VCS. In Step 2', because the encryption uses the $n \times m_0$ basis matrix $M_c^{c_1.........c_n}$, this later scheme results in the pixel expansion *m0*, that is, the same as that of the corresponding black and white EVCS. For general colour (k,n)-EVCS, one can make use of the basis matrices of the corresponding black and white (k,n)-EVCS.As for the security of Construction 1, according to Definitions 1 and 2, and Theorem 1, we have the following theorem:

Theorem 1: Construction 1 generates *n* shares S*i* for $i = 1....n.$ where less than *k* out of *n* shares cannot get any information about the secret image other than the size of the secret image.

Proof: In Construction 1, the corresponding black and white (k,n) -VCS and (k,n)-EVCS are used to encrypt the secret bits at each bit-level and each colour channel, respectively, that is, for a particular bit-level j $(1 \leq j \leq 8)$ and a colour channel *X (X = C, M, Y),* the shares $s^{j_{1,X}}, s^{j_{2,X}}, ...\,.., s^{J_{n,X}}$ constitute a black and white (k,n)-VCS. Because of the security conditions of Definitions 1 and 2 and Theorem 1, any less than *k* out of *n* shares cannot obtain any information about the secret image other than the size of the secret image on the bit-level *j* and colour channel *X*, and they cannot get any information about the secret image for other bit-levels and colour channels either, since the construction of the shares $s^{j_{1,X}}, s^{j_{2,X}}, ...\,.., s^{J_{n,X}}$ is irrelevant to the information about the secret image on those bit-levels and colour channels. By applying the above discussions to all the bit-levels and colour channels, we have that any less than *k* out of *n* shares cannot get any information about the secret image other than the size of the secret image. For the colour VCS under the visual cryptography model of Naor and Shamir, the 0's in the transparencies for all bit-levels are intact (i.e. with grey level 0), and the 1's for the bit-level *j* is assigned with grey level *aj*. Hence, the distance between the 0's and 1's for bit-level *j* is *aj*. The larger the value of *aj*, the more apparent is the difference between black and white pixels at bit-level *j*.

For two bit levels *i* and *j*, where $i < j$, they should satisfy $a_i > a_j$. For example, the grey levels of the most and second most significant bits a_1 and a_2 should satisfy a_1 . a_2, and the larger the value of $(a_1 > a_2)$, the more apparent the most significant bits appear in the recovered secret image, and vice versa. Hence, for different types of secret images, the dealer should choose the grey levels carefully for different applications.

Example 1: For the construction of a colour $(2,2)$-VCS by Construction 1: let the basis matrices used in Algorithm 1 of the corresponding black and white $(2,2)$-VCS be where the pixel expansion is m = 2. $M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ and $M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. To simplify the example, we take a secret image with only two bit-levels as example, that is, each pixel only has the most and second most significant bits for each colour channel. In such case, the grey levels of each colour channel only have the four values 192, 128, 64 and 0. Let the parameters of Algorithm 1 be e_0 = 0, e_1 = 0 and e_2 = 0 for the most significant bit-level and e_0’ = 0, e_1’ = 0 and e_2’ = 0 for the second most significant bit-level. We take the encryption of a block of 2 pixels with the grey levels 192 and 128 as example. We come to know that the most significant bits of the two pixels are 1, 1. Because (e_2 mod m) = (0 mod 2) = 0 < 2, we encrypt the two bits by $P(M_1)$, where we replace the 1’s in M_1 by the grey level a_1 and leave the 0’in $P(M_1)$ intact; then, we set e_2 = 1. Then, the second most significant bits are 1, 0. Because (e_1’ mod m) = (0 mod 1) = 0 < 1, we encrypt the two bits by $P(M_1)$, where we replace the 1’s in M_1 by the grey level a_2 and leave the 0’s in $P(M_1)$ intact; then, we set e_1’ = 1. By encrypting all the blocks in the secret image, we obtain six shares for each participant *i* as $s^1_{i,C}, s^2_{i,C}, s^1_{i,M}\ s^2_{i,M}, s^1_{i,Y}, s^2_{i,Y}$ By stacking the six shares, we obtain the final share S_i for participant *i*. shows the experimental results of the colour $(2,2)$-VCS, where we set the grey levels a_1 = 128 and a_2 = 64.

Similarly, for the construction of colour $(2,2)$-EVCS by Construction 1: let the basis matrices of the corresponding black and white $(2,2)$-EVCS be the second example in Example 2 where the pixel expansion is 4. Also, let the secret image and the original share images only have two bit-levels for each colour channel. For the encryption of a pixel where the grey levels of the secret image and the two original share images are 192, 128 and 64, the most significant bits of the pixel in the three images are 1, 1, 0. Hence, we encrypt the most significant bit of this pixel by $p(s_1^{10})$. Similarly, we encrypt the second most significant bits of this pixel by $p(s_1^{10})$, where we replace the 1's in $p(s_1^{10})$ and $p(s_1^{01})$ by the grey levels *a1* and *a2,* respectively.By encrypting all the pixels in the secret image, we obtain six shares for each participant *i* as $s_{i,C}^1, s_{i,C}^2, s_{i,M}^1\ s_{i,M}^2, s_{i,Y}^1, s_{i,Y}^2$. By stacking the six shares, we obtain the final share *Si* for participant *i*.

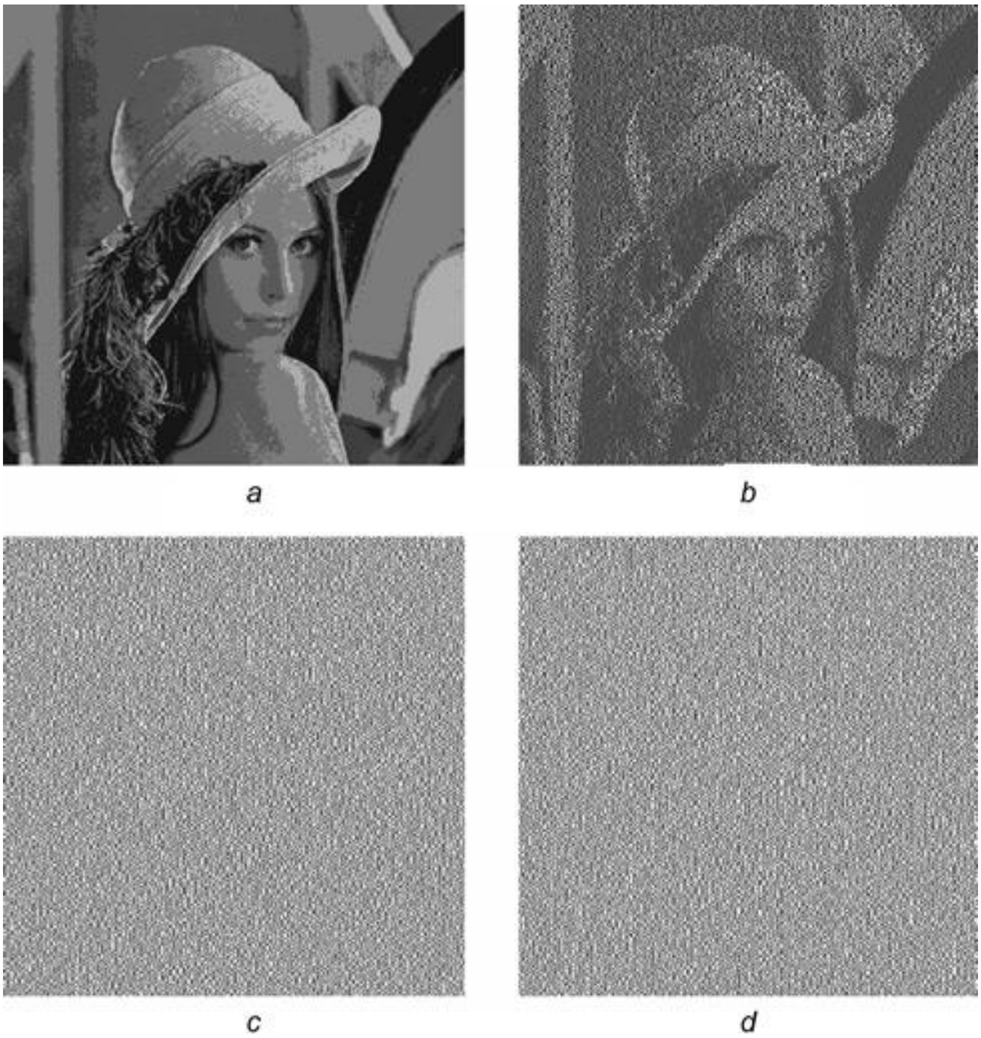


Figure 4: Experimental results of the colour (2,2)-VCS with no pixel expansion under the visual cryptography model of Naor and Shamir

a Original secret image

b Resulting image by superimposing fig 1c and 1d

c Encrypted shares

d Encrypted shares

Size of the secret image is 256 _ 256

Under the ideal subtractive colour model, the stacking of the qualified colour shares can recover the secret image visually. However, such an ideal subtractive colour mixture is impractical because of the properties of the ink.

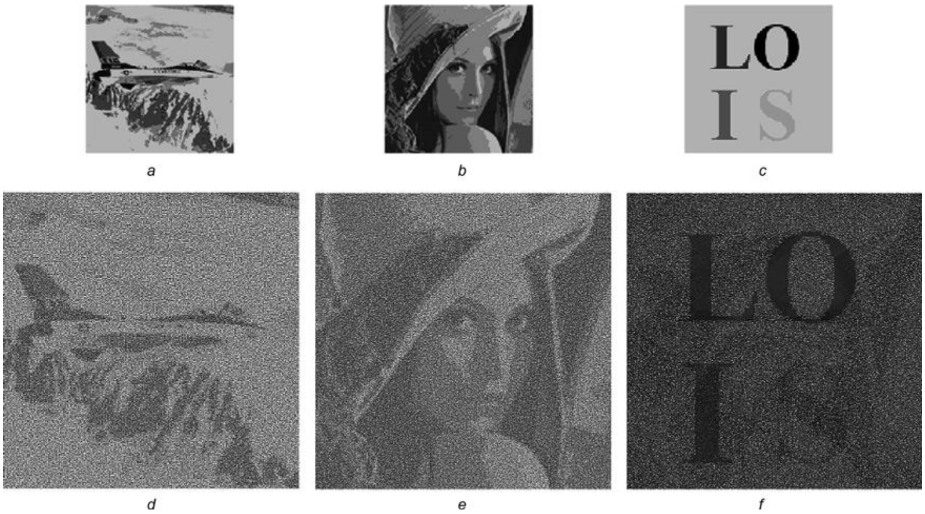


Figure 5: Experimental results of the colour (2,2) -EVCS with pixel expansion of 4 under the visual cryptography model of Naor and Shamir

a. Original two share image

b. Original two share image

c. Original secret image

d. Encrypted shares

e. Encrypted shares

f. Resulting image by superimposing the shares fig 5.d and 5.e

Size of the secret image is 200 _ 200

To alleviate this phenomenon, we propose to divide the colour into three channels *C*, *M* and *Y*, and print each channel of the colour on adjacent pixels, respectively. Superimposition of the same colour channel results in better visual effect. However, this method will expand the output images three times.

5.4. Colour VCS and colour EVCS under the model of Tuyls:

The visual cryptography model of Tuyls is interesting for the reasons of good resolution, contrast and colour properties. The colour (n,n)-VCS on this visual cryptography model can recover the secret image perfectly. However, there is no known colour VCS for general (k,n)-VCS, not to mention the colour EVCS under this visual cryptography model. In this section, we propose the constructions of colour VCS and colour EVCS under the visual cryptography model of Tuyls.

The following construction constructs the colour (k,n)- VCS by Steps 1, 2, 3 and 4, and constructs the colour (k,n)-EVCS by Steps 1′, 2′, 3′ and 4′:

Construction: Constructions of the colour (k,n)-VCS and the colour (k,n)-EVCS under the visual cryptography model of Tuyls:

Setup: Denote the $n \times m$ matrices *M0* and *M1* as the basis matrices of a corresponding black and white (k,n)-VCS under the visual cryptography model of Tuyls, and denote the $n \times m$ matrices $M_c^{c_1 \ldots\ldots\ldots c_n}$ as the basis matrices of a corresponding black and white (k,n)-EVCS under the visual cryptography model of Tuyls, where $c, c_1, \ldots\ldots., c_n \in \{0,1\}$. Denote *aj* as the grey level of 1’s and *bj* as the grey level of 0’s at bit-level *j*.

Output: The shares *Si* for $i \in 1,2,\ldots.n$.

Step 1: Represent the grey levels of each colour channel (*R*, *G* and *B*, respectively) of all the pixels in the secret image by vectors of 8 bits, that is, the secret image is divided into 8 bit-levels, and each bit-level forms a binary image.

Step 1′: Represent the grey levels of each colour channel (*R*, *G* and *B*, respectively) of all the pixels in the secret image (resp. the *n* original share images) by vectors of 8 bits, that is, the secret image (resp. the *n* original share images) is divided into 8 bit-levels, and each bit-level forms a binary image.

Step 2: For each bit-level *j* and each colour channel, encrypt a bit by $p(M_0)$ and $p(M_1)$ for the colour channels R, G and B and bit-levels $j \in \{1,2.....8\}$, respectively, where $p(M_0)$, $p(M_1)$ are the random column permutations of M_0, M_1, and replace the 1's in $p(M_0)$, $p(M_1)$ by the grey level a_j and the 0's by the grey level b_j.

Step 2′: For each bit-level *j* and each colour channel, encrypt a bit by $p(M_c^{c_1,\ldots\ldots,c_n})$ for the colour channels *R, G* and *B* and bitlevels $j \in \{1,2.....8\}$ respectively, where $p(M_c^{c_1,\ldots\ldots,c_n})$ is a random column permutation of $M_c^{c_1\ldots\ldots c_n}$, and replace the 1's in $p(M_c^{c_1,\ldots\ldots,c_n})$ by the grey level a_j and the 0's by the grey level b_j.

Step 3: Repeat the steps 1 and 2 (resp. **1′** and **2′**) until all the pixels in the secret image have been encrypted. Then, w obtain the shares $s^1_{i,t}, s^2_{i,t}, ...s^8_{i,t}$ where $i \in \{1,2.....n\}$, *t* ∈ *{R, G, B}*, and the share $s^j_{i,t}$,is denoted as the share for the participant *i* at the bit-level *j* for the colour channel *t*.

Step 4: Each participant i is distributed with a share S_i, where S_i is generated by stacking the shares at the different bit-levels and of the different colour channels $S_{1i,R}$, $S_{2i,R}$, . . . , $S_{8i,R}$, $S_{1i,G}$, $S_{2i,G}$, . . . , $S_{8i,G}$, $S_{1i,B}$, $S_{2i,B}$, . . . , $S_{8i,B}$ for $i \in \{1,2.....n\}$.

The two construction looks similar, except the differe nces in the colour channels and the basis matrices M_0, M_1 and $M_c^{c_1\ldots\ldots c_n}$. However, Construction 1 cannot be applied properly under the visual cryptography model of Tuyls, because of the differences on choosing the values of the grey levels, which is caused by the different colour model. For the case of the construction of the colour VCS under the visual cryptography model of Naor and Shamir, we only need to choose the grey levels for the 1's of each bitlevel, and leave the pixel of the 0's intact. However, for the case under the visual cryptography model of Tuyls, we have to choose the grey levels for both the 1's and 0's of each bit-level *j* that is the values of a_j and b_j. We notice that, by choosing different grey levels for the bit-levels, we will obtain the quite different visual effects. However, finding a formula to determine the proper values for a_j and b_j is rather complicated for the general (k,n)-VCS, which heavily depends on the contents of the secret image, the observer's experiences, the access structure and the intensity function of the visual cryptography model of Tuyls (i.e. the function

$I_r(\alpha) = \cos 2(\alpha_1 + \alpha_2)$ and so on. However, some basic rules should be satisfied, for example as follows. First, the distance between *aj* and *bj* should be larger than the distance between *aj+1* and *bj+1*, that is$|a_j - b_j| > |a_j + 1 - b_j + 1|$, which means that the information about bit-level *j* should be more apparent than that of bit-level *j + 1*. Secondly, the average intensity of a white pixel, which contains *m (m')* sub-pixels, should be larger than that of a black pixel that is, a white pixel should be lighter than a black pixel.

The values of *aj* and *bj* in example satisfy the above rules.In Step 2, because the encryption uses the $n \times m$ basis matrices *M0* and *M1*, this scheme results in the pixel expansion of *m* that is, the same as that of its corresponding black and white VCS.

In Step 2', because the encryption uses the $n \times m'$ basis matrix $M_c^{c_1 \ldots\ldots\ldots c_n}$, this later scheme results in a pixel expansion of m' that is, the same as that of its corresponding black and white EVCS. With regard to the security of Construction 2, we give the following theorem about the security of the proposed colour VCS and colour EVCS.

Theorem 2: Construction 2 generates *n* shares *Si* for $i \in 1,2,\ldots.n$, where less than *k* out of these *n* shares cannot get any information about the secret image other that the size of the secret image.

Proof: In Construction 2, the corresponding black and white (k,n)-VCS and (k,n) - EVCS are applied to encrypt the secret bits at each bit-level and each colour channel, respectively, that is, for a particular bit-level *j (1≤ j ≤ 8)* and a colour channel *X (X = R, G, B)*, the shares $s_{1,X}^j, s_{2,X}^j, \ldots\ldots. s_{n,X}^j$ constitute a black and white (k,n)-VCS. Because of the security conditions of Definitions 1 and 2, any less than *k* out of *n* shares cannot obtain any information about the secret image other than the size of the secret image on the bit-level *j* and colour channel *X*, and they cannot obtain any information about the secret image for other bit-levels and colour channels either, since the construction of the shares $s_{1,X}^j, s_{2,X}^j, \ldots\ldots. s_{n,X}^j$ is irrelevant to the information about the secret image on those bit-levels and colour channels. By applying the above discussions for all the bitlevels and colour channels, we have that any less than *k* out of *n* shares cannot obtain any information about the secret image other than the size of the secret image. An example of Construction 2 is as follows.

Example 2: For the construction of colour *(2, 3)*-VCS by Construction 2: let the basis matrices of the corresponding black and white *(2, 3)*-VCS be

$$\mathbf{M}_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

where the pixel expansion is 3. To simplify the example, we let the secret image only have two bitlevels for each colour channel. Take the encryption of a pixel with a grey level 128 as example. The most and second most significant bits of the pixel are 1 and 0. Hence, we encrypt them by $p(M_1)$ and $p(M_0)$, where we replace the 1's and 0's of $p(M_1)$ by *a*1 and *b*1, and replace the 1's and 0's of $p(M_0)$ by *a*2 and *b*2, respectively. By encrypting all the pixels in the secret image, we obtain six shares for each participant i as $s^1_{i,C}, s^2_{i,C}, s^1_{i,M}, s^2_{i,M}, s^1_{i,Y}, s^2_{i,Y}$.By stacking the six shares, we obtain the final share *Si* for participant *i*. Similarly, for the construction of colour *(2, 2)*-EVCS by Construction 2: let the basis matrices of the corresponding black and white *(2, 2)*-EVCS be the first example.

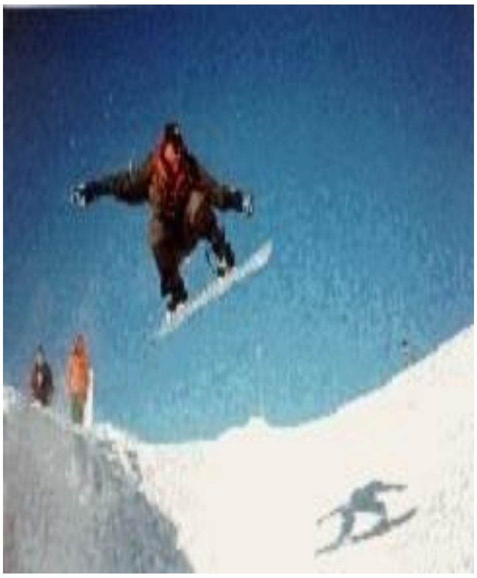


Figure 6.a: Original image

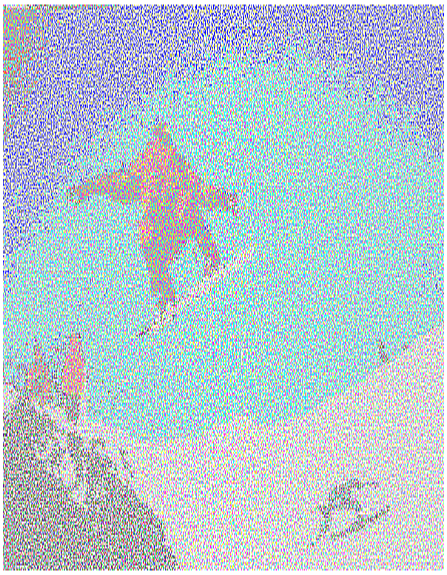


Figure 6.b: Stacking the shares

Example 2: where the pixel expansion is 3. Let the secret image only have two bit-levels for each colour channel. For the encrypting of a pixel where the grey levels of the secret image, the first and second original share images are 192,128 and 64, the most significant bits of the pixel in the three images are 1, 1, 0. Hence, we encrypt the most significant bit of this pixel by $p(s_1^{10})$. Similarly, we encrypt the second most significant bits of this pixel by $p(s_1^{01})$, where we replace the 1's and 0's in $p(s_1^{10})$ by the grey levels *a1* and *b1* and replace the 1's and 0's in $p(s_1^{10})$ by the grey levels *a2* and *b2*, respectively. By encrypting all the pixels in the secret image, we obtain six shares for each participant I as $s_{i,C}^1, s_{i,C}^2, s_{i,M}^1\ s_{i,M}^2, s_{i,Y}^1, s_{i,Y}^2$. By staking the six shares, we obtain the final share *Si*.

Chapter 6

Conclusions

6. 1. Improvements in the Schemes:

The relative contrast and the pixel expansion obtained from the above two schemes are so large that it is practically impossible to “see” the image after recombination. We have used the following two improvement schemes to lower the aspect ratio and tune the image after recombination.

6.1. 1. Aspect Ratio Maintenance:

Till now we used to take a single row of the basis matrix as the subpixels corresponding to a single pixel of the original image. This led to the distortion in the aspect ratio of the image after recovery. Instead of doing this we can replace the single row by blocks the product of whose dimensions is equal to the length of the row in the basis matrix. For eg. if the pixel expansion is 36 we can have blocks of size 6×6. This maintains the aspect ration of the
image.

6.1.2. Tuning of the image:

Tuning is used to improve the visual quality of the recovered image.In this we take each block of sub-pixels corresponding to a pixel of the original image and we replace it with the pixel value occurring greater number of times, i.e. if black(white) pixel occurs more than the whiteblack pixel then we replace the block with the blackwhite pixel. This drastically improves the quality of the image. A similar model of visual cryptography has been proposed. This new visual cryptography model utilised the polarisation of the light, which could realise the XOR operation, and had good colour, resolution and contrast properties.

\

6.2 Applications:

1. Bank customer identification
    - Bank sends customer a set of transparencies (key) in advance
    - Bank web site displays cipher
    - Customer applies overlay, reads transaction key
    - Customer enters transaction key
2. Verifiable Receipts in Electronic Voting
3. Anti spam-bot measure.

Chapter 7

Annexure-1

Source code

7.1 (2,2)-VTS MATLAB code and output

```
img = imread('cameraman.tif');
bin_img = im2bw(img);
[rows , cols] = size(bin_img);
s0 = [ 1 0 ; 1 0 ];
s0p= [ 0 1 ; 0 1 ];
s1 = [ 1 0 ; 0 1 ];
s1p =[ 0 1 ; 1 0 ];
share1= zeros(rows,2*cols);
share2=share1;
pos = 1;
for r=1:1:rows
        pos=1;
        for c=1:1:cols
                if(bin_img(r,c)==1)
                        ran = randint;
                if(ran==1)
                        share1(r,pos)=s0(1,1);
                        share2(r,pos)=s0(2,1);
                        pos=pos+1;
                        share1(r,pos)=s0(1,2);
                        share2(r,pos)=s0(2,2);
                        pos=pos+1;
                else
                        share1(r,pos)=s0p(1,1);
                        share2(r,pos)=s0p(2,1);
                        pos=pos+1;
                        share1(r,pos)=s0p(1,2);
                        share2(r,pos)=s0p(2,2);
```

```
            pos=pos+1;
        end
    else
        ran=randint;
        if(ran==0)
            share1(r,pos)=s1(1,1);
            share2(r,pos)=s1(2,1);
            pos=pos+1;
            share1(r,pos)=s1(1,2);
            share2(r,pos)=s1(2,2);
            pos=pos+1;
        else
            share1(r,pos)=s1p(1,1);
            share2(r,pos)=s1p(2,1);
            pos=pos+1;
            share1(r,pos)=s1p(1,2);
            share2(r,pos)=s1p(2,2);
            pos=pos+1;
            end
        end
    end
end
imwrite(share1,'D:\shares1.jpg','jpg');
imwrite(share2,'D:\shares2.jpg','jpg');
```

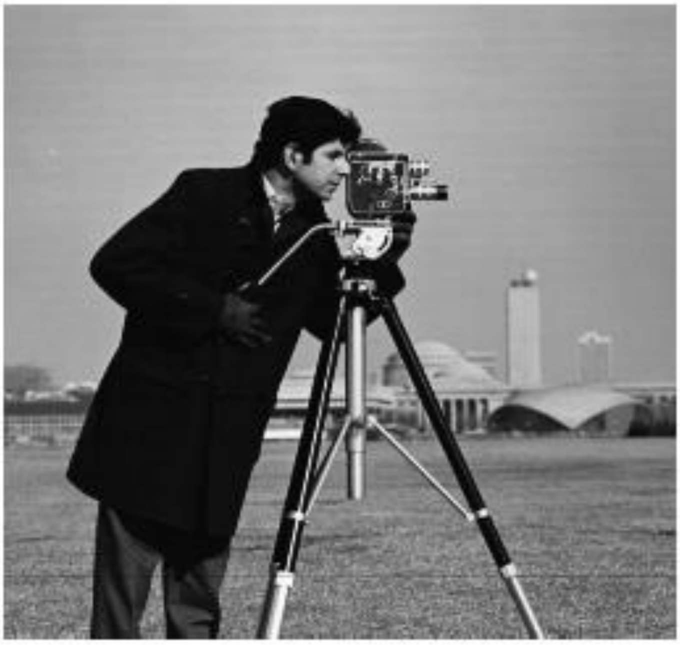


Figure 7: (2,2) secret image

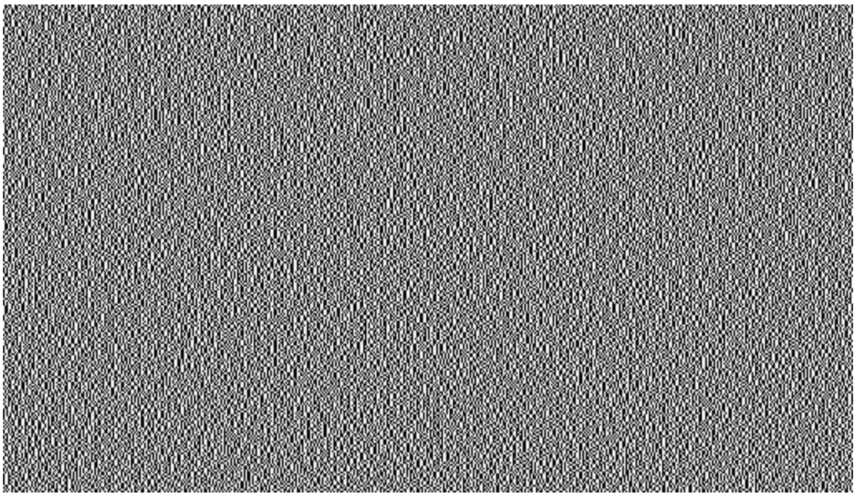


Figure 8: (2,2) Share 1

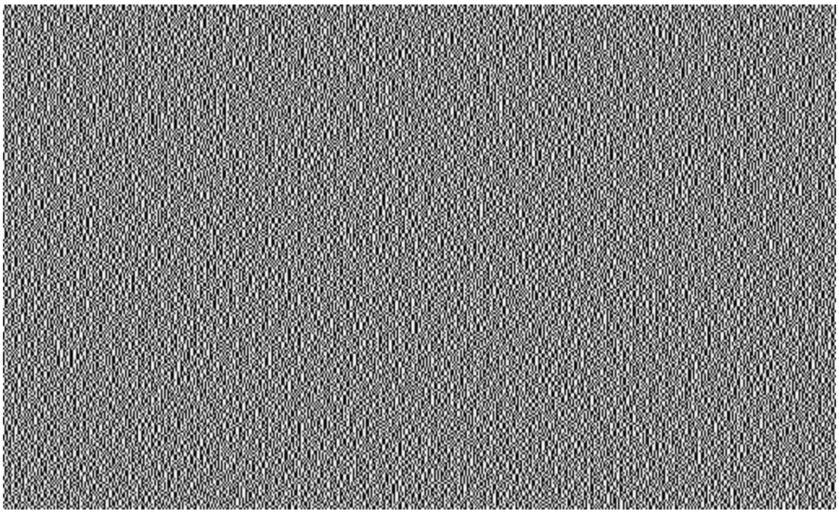


Figure 9: (2,2) Share 2

```
a=imread('D:\shares1.jpg');

b=imread('D:\shares2.jpg');
c=a+b;
imwrite(c,'D:\c.jpg','jpg')
```

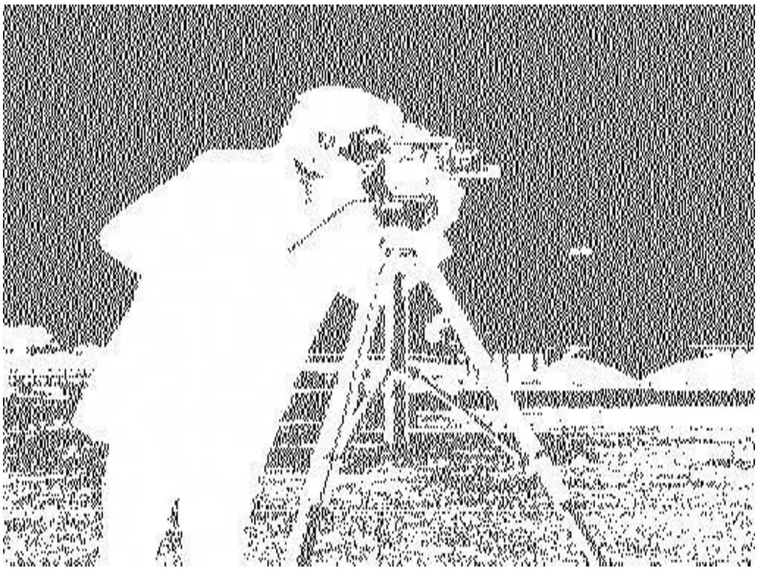


Figure 10: (2,2) Image is recovered on stacking the 2 shares

7.2 General Access Structure MATLAB code and output

Main program

```
img = imread('cameraman.tif');
bin_img = im2bw(img);
I = [ 1 2 3 4 5];
[rows , cols] = size(bin_img);
[s0,s1]=matrices(I);
pos=1;
shares = zeros(rows,8*cols,5);
for r = 1:rows
        pos=1;
        for c = 1:cols
                if(bin_img(r,c)==1)
                        temp=S0;
                                for z = 1:5
                                        post=pos;
                                        for cl=1:8
                                                shares(r,post,I(z))=temp(z,cl);
                                                post=post+1;
                                        end
                                end
                        pos=pos+8;
                else
        temp=S1;
                for z = 1:5
                        post=pos;
                        for cl=1:8
                                shares(r,post,I(z))=temp(z,cl);
                                post=post+1;
                        end
                end
                        pos=pos+8;
        end
end
end
imwrite(shares(:,:,1),'D:\sharesBOSS.jpg','jpg');
imwrite(shares(:,:,2),'D:\sharesMAN1.jpg','jpg');
imwrite(shares(:,:,3),'D:\sharesMAN2.jpg','jpg');
imwrite(shares(:,:,4),'D:\sharesUSER1.jpg','jpg');
imwrite(shares(:,:,5),'D:\sharesUSER2.jpg','jpg');
```

function matrices:

```
function [s0,s1] = matrices(I)
[s0,s1]=gen_mat();
grp1= [ 1 2 4];
grp2= [ 1 3 5];

for i = 1:8
        s0(I(grp1(3)),i)= mod(s0(I(grp1(1)),i) + s0(I(grp1(2)),i),2);
        s1(I(grp1(3)),i)= mod((s1(I(grp1(1)),i) + s1(I(grp1(2)),i)+1),2);
        s0(I(grp2(3)),i)= mod(s0(I(grp2(1)),i) + s0(I(grp2(2)),i),2);
        s1(I(grp2(3)),i)= mod((s1(I(grp2(1)),i) + s1(I(grp2(2)),i)+1),2);
end
```

function gen_mat

```
function [s0,s1] = gen_mat()
s0 = zeros(5,8);
s1 = zeros(5,8);
for i=1:8
        n=i-1;
        r=3;
        while(n>0)
                s0(r,i)=mod(n,2);
                n=(n-s0(r,i))/2;
                r=r-1;
        end
end
s1=s0;
```

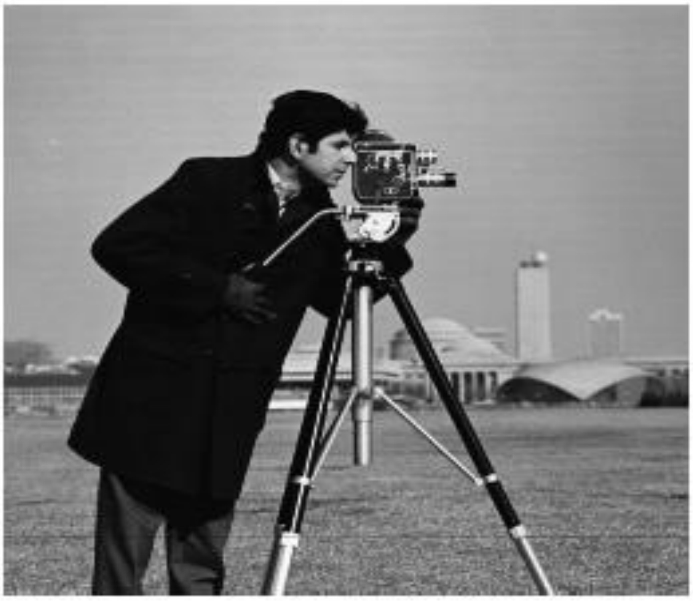


Figure 11:The Secret Image

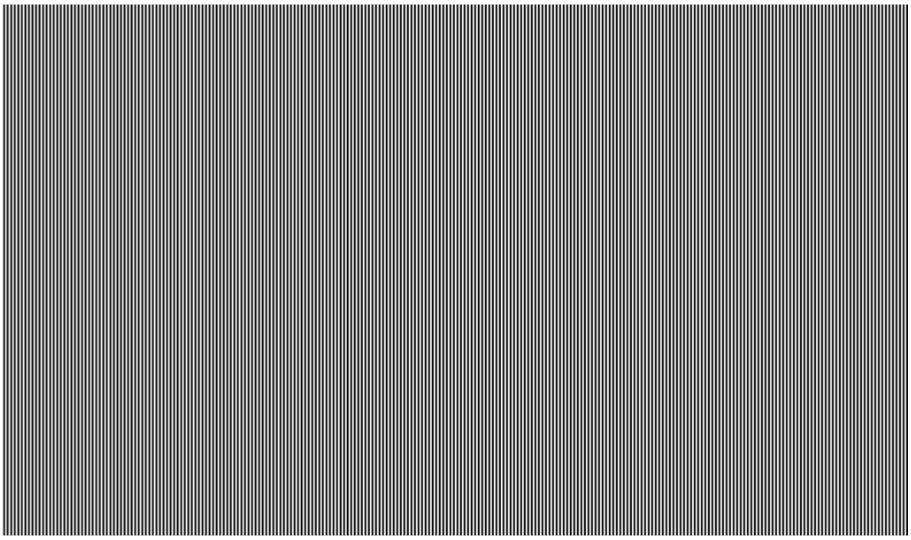


Figure 12: Share of BOSS

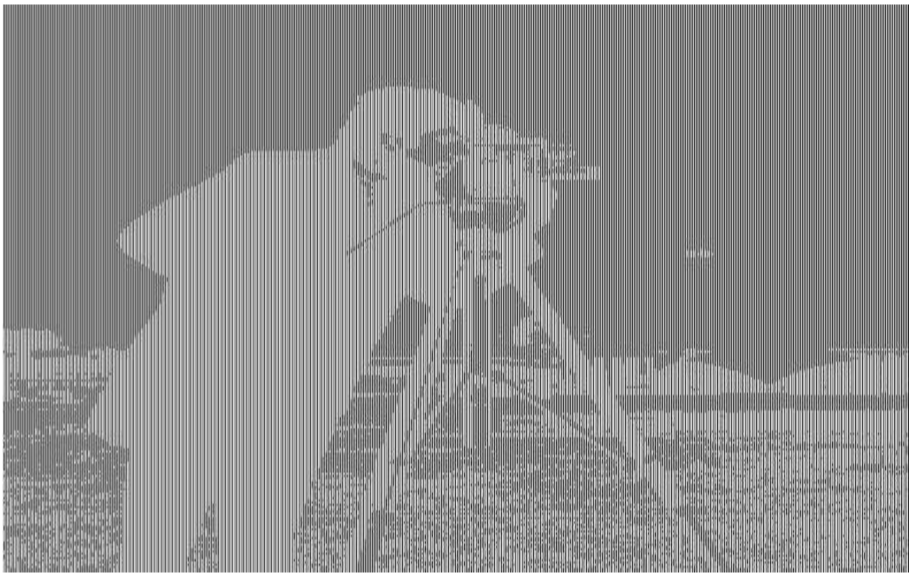


Figure 13: Share of Manager 1

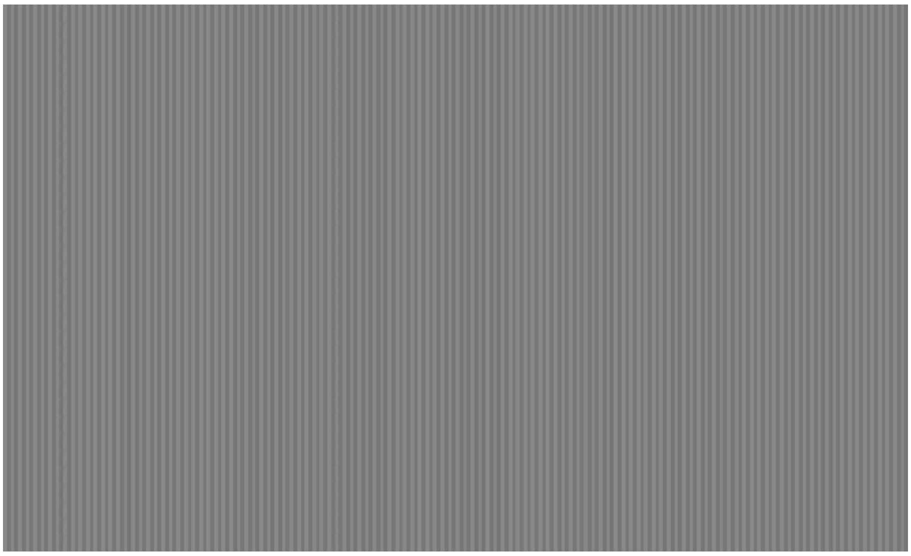


Figure 14: Share of Manager 2

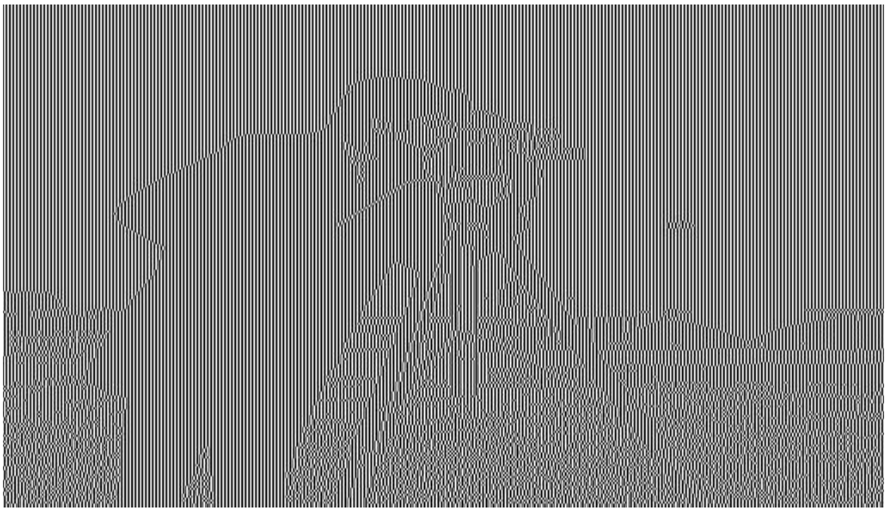


Figure 15: Share of User 1

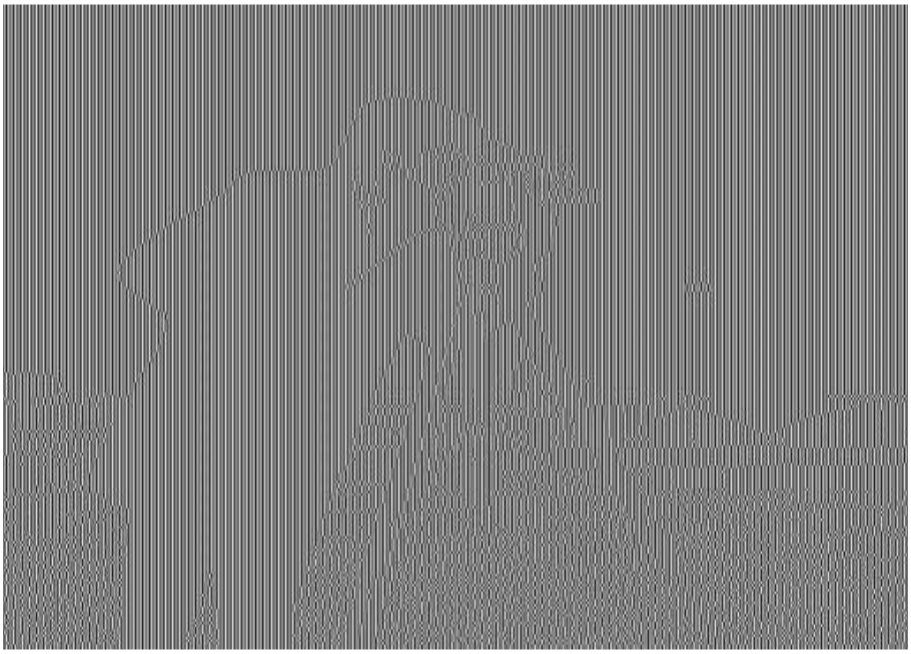


Figure 16:Share of User 2

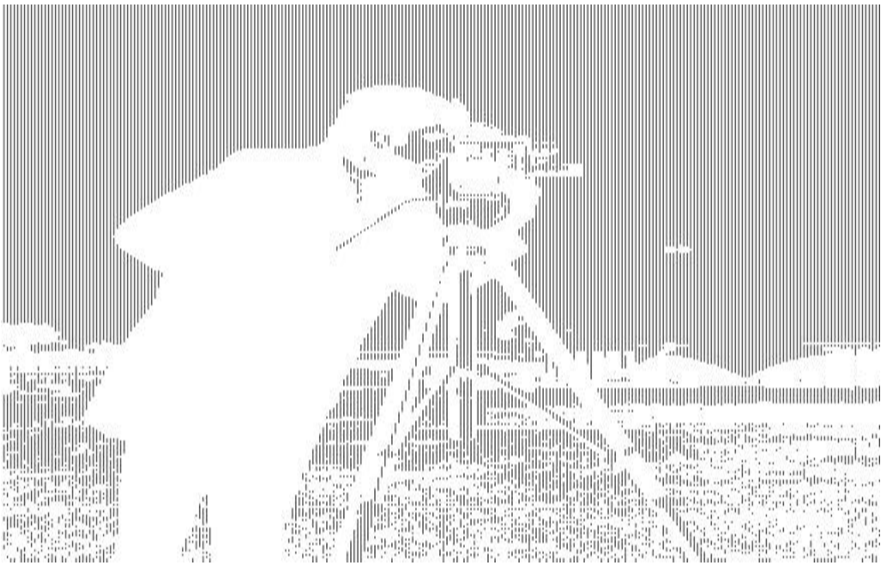


Figure 17: Recovery from group 1(Boss+Manager1+User1)

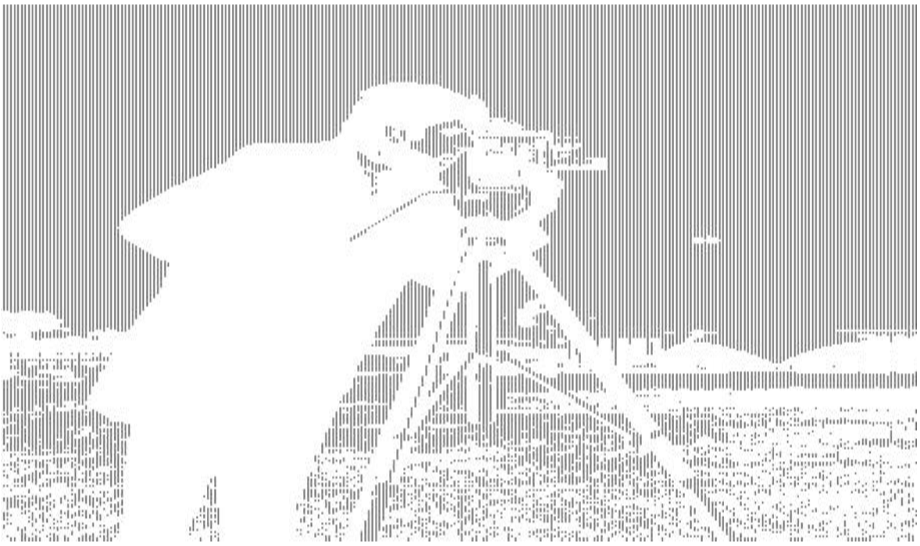


Figure 18: Recovery from group 2(Boss+Manager2+User2)

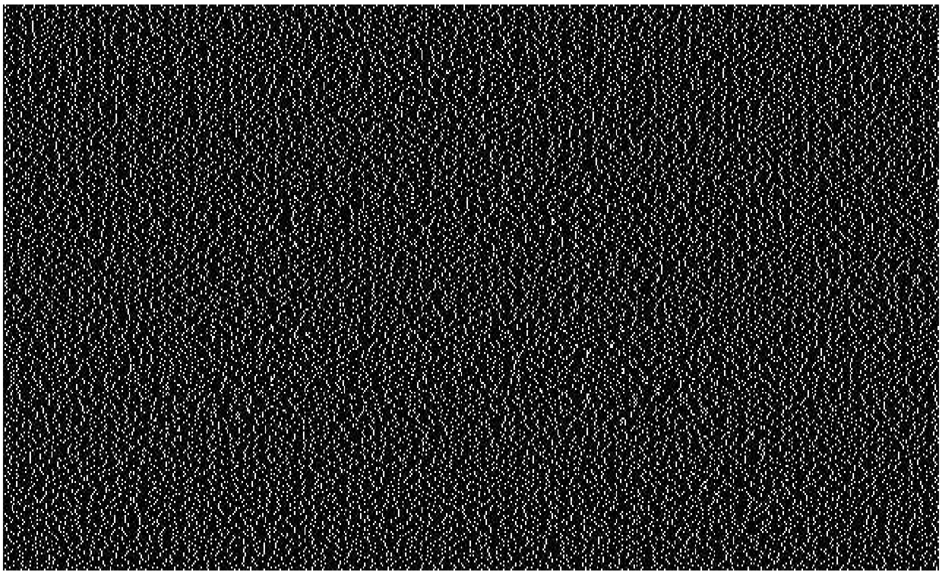


Figure 19: No inf is revealed from any forbidden group

7.3 Main Program:

```
[s0,s1]=gen_s0_s1;
img = imread('cameraman.tif');
bin_img = im2bw(img);
[rows , cols] = size(bin_img);
pos=1;
shares = zeros(6*rows,7*cols,8);
cr=1;
cc=-6;
for r = 1:rows
        cc=-6;
        for c = 1:cols
                if(bin_img(r,c)==1)
                temp=S1;
                cc=cc+7;
                        for z = 1:8
                                cr1=cr;
                                cl=1;
                                for r1 = 1:6
                                        cc1=cc;
                                        for c1=1:7
                                                shares(cr1,cc1,z)=temp(z,cl);
                                                cl=cl+1;
                                                cc1=cc1+1;
                                        end
                                        cr1=cr1+1;
                                end
                        end
                else
        temp=S0;
        cc=cc+7;
        for z = 1:8
                cl=1;
```

```
                    cr1=cr;
                    for r1 = 1:6
                              cc1=cc;
                              for c1=1:7
                                        shares(cr1,cc1,z)=temp(z,cl);
                                        cl=cl+1;
                                        cc1=cc1+1;
                              end
                              cr1=cr1+1;
                    end
          end
end
end
cr=cr+6;
end
imwrite(shares(:,:,1),'D:\share1b.jpg','jpg');
imwrite(shares(:,:,2),'D:\share2b.jpg','jpg');
imwrite(shares(:,:,3),'D:\share3b.jpg','jpg');
imwrite(shares(:,:,4),'D:\share4b.jpg','jpg');
imwrite(shares(:,:,5),'D:\share5b.jpg','jpg');
imwrite(shares(:,:,6),'D:\share6b.jpg','jpg');
imwrite(shares(:,:,7),'D:\share7b.jpg','jpg');
imwrite(shares(:,:,8),'D:\share8b.jpg','jpg');
```

Function gen_s0_s1:

```
function [s0,s1]= gen_s0_s1()
s0_1=zeros(8,14);
s1_1=ones(8,14);
s0_2=ones(8,28);
s1_2=zeros(8,28);
s0=cat(2,s0_1,s0_2);
s1=cat(2,s1_1,s1_2);
```

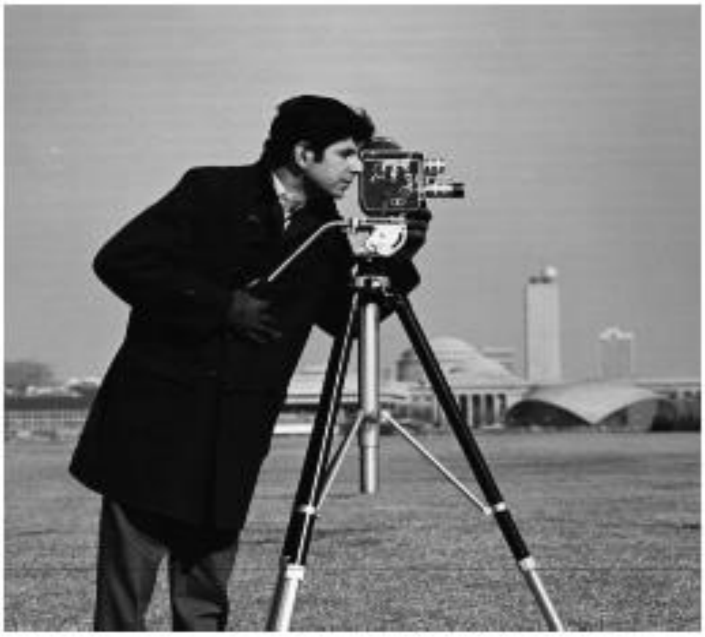


Figure 20: Original Secret

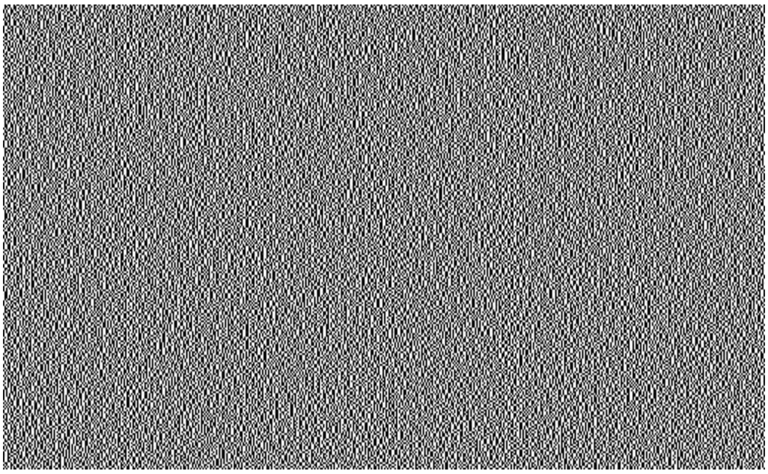


Figure 21: A Share of (3,8) Canonical VTS scheme

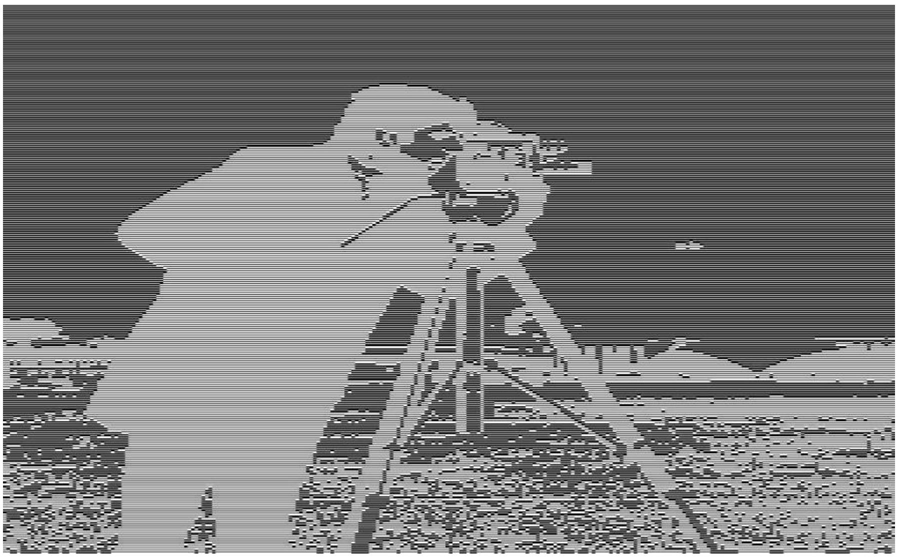


Figure 22: Recovery of secret from a set of three shares

References:

[1] A Adhikari, Applications of Combinatorial Structures in Secret Sharing and Visual Cryptography, Thesis submitted to Indian Statistical Institute in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy, August,2004.

[2] M. Naor and A. Shamir , Visual Cryptography, Eurocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer-Verlag, 1-12, 1994.,

[3] C. Blundo, A. De Santis and D. R. Stinson , On the contrast in visual cryptography schemes; Journal of Cryptology, Vol. 12, No. 4, 261-289, 1999.

[4] C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson, Contrast optimal threshold visual cryptography schemes, SIAM Journal of Discrete Mathematics, Vol. 16, No. 2, 224-261, 2003.

[5] F.J. MacWilliams and N.J.A Sloane, The Theory of Error-Correcting Codes, North Holland , Amsterdam , 1977.

[6] Rafael C. Gonzalez, Richard E. Woods , Steven L.Eddins, Digital Image Processing Using MATLAB r, PearsonEducation, 2004.

[7] NAOR M., SHAMIR A.: 'Visual cryptography'. EUROCRYPT '94, 1995, (LNCS, 950), pp. 1–12

[8] Patent with International Application No.: PCT/ IB2003/000261, 'Secure visual message communication method and device'. 2003

[9] CIMATO S., PRISCO R.D., DE SANTIS A.: 'Optimal colored threshold visual cryptography schemes', Des. Codes Cryptogr., 2005, 35, pp. 311–335

[10] NAKAJIMA M., YAMAGUCHI Y.: 'Extended visual cryptography for natural images'. WSCG Conf. 2002, 2002, pp. 303–412

[11] VERHEUL E., TILBORG H.V.: 'Constructions and properties of k out of n visual secret sharing schemes', Des. Codes Cryptogr., 1997, 11, (2), pp. 179–196

[12] DROSTE S.: 'New results on visual cryptography'. CRYPTO '96, 1996, (LNCS, 1109), pp. 401–415

[13] ATENIESE G., BLUNDO C., DE SANTIS A., STINSON D.R.: ‘Extended capabilities for visual cryptography’, ACM Theor. Comput. Sci., 2001, 250, (1–2), pp. 143–161

[14] ITO R., KUWAKADO H., TANAKA H.: ‘Image size invariant visual Cryp ography’, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 1999, E82-A, (10), pp. 2172–2177

[15] YANG C.N.: ‘New visual secret sharing schemes usingprobabilistic method’, Pattern Recognit. Lett., 2004, 25, pp. 481–494

[16] BLUNDO C., DE SANTIS A., STINSON D.R.: ‘On the contrast in visual cryptography schemes’, J. Cryptol., 1999, 12, (4), pp. 261–289

[17] TUYLS P., HOLLMANN H.D.L., VAN LINT J.H., TOLHUIZEN L.: ‘Xorbased visual cryptography schemes’, Des. Codes Cryptogr., 2005, 37, pp. 169–186

[18] Ming Sun Fu and Oscar C. Au “Data hiding in halftone images by conjugate error diffusion” D-7803-7761-3/03 © 2003 IEEE.

[19] Ming Sun Fu and Oscar C. Au “Joint Visual cryptography and watermarking”. 0-7803-8603-5/04 © 2004 IEEE.

[20] Zhongmin Wang and Gonzalo R. Arce “Halftone visual cryptography through error diffusion” ISBN 1-4244-0481- 9/06 © 2006 IEEE, pp.109-112.

[21] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo “Halftone Visual Cryptography” 0-7803-7750-8/03 © 2003 IEEE,

[22] Notes “Digital Image Processing Laboratory: Image Halftoning” April 30, 2006. Purdue University.

[23] Lingo Fang and Bin Yu “Research on pixel expansion of (2,n) Visual threshold scheme” 2006 1st International Symposium on Pervasive Computing and Applications.

[24] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129, No. 2, (1996), pp. 86-106.

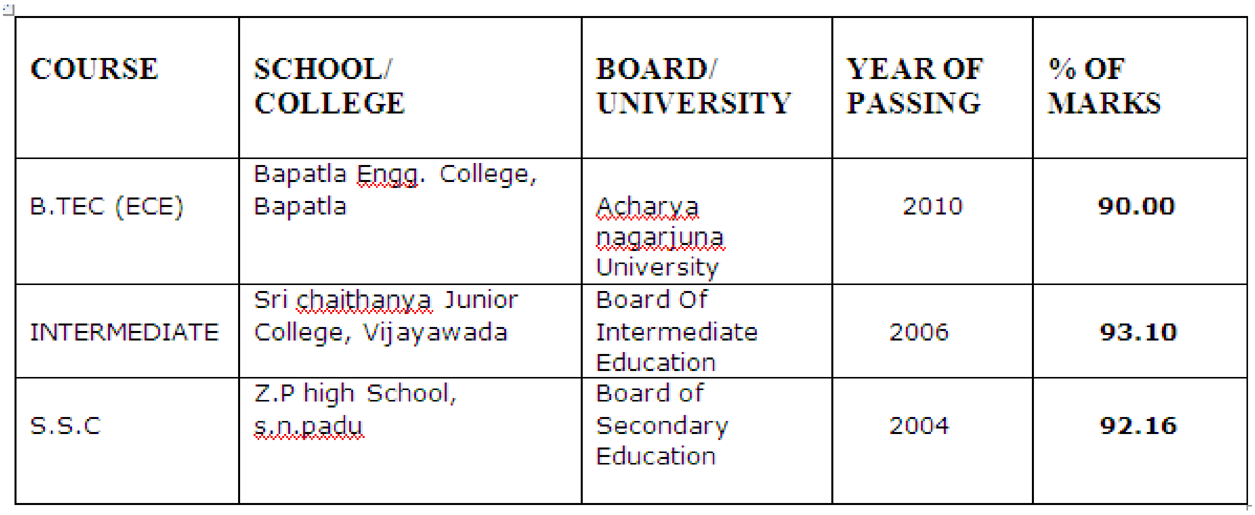
CURRICULUM VITAE

MANNAM VENKATA VARUNBABU
S/o M.Basavaiah,
D.no:40-12-1/6,
Kammapalem,
Ongole, Prakasam district
Phone:8977740962 **Email:pranav7223@gmail.com**

Career Objective:

Intend to build my career with leading corporate in Hi-tech environment with committed and dedicated people, which helps me to explore myself fully and realize my potential. Willing to work as a key player in challenging and creative environment.

Academic Profile:



COURSE	SCHOOL/ COLLEGE	BOARD/ UNIVERSITY	YEAR OF PASSING	% OF MARKS
B.TEC (ECE)	Bapatla Engg. College, Bapatla	Acharya nagarjuna University	2010	**90.00**
INTERMEDIATE	Sri chaithanya Junior College, Vijayawada	Board Of Intermediate Education	2006	**93.10**
S.S.C	Z.P high School, s.n.padu	Board of Secondary Education	2004	**92.16**

Soft skills:

C , DS using C, C++

Subjects of interest:

Analog communications

Digital electonics

ACADEMIC PROJECT:

Project name : Colour Visual Cryptography Schemes

Software Used : MATLAB 7.5.0.

Description:

Visual cryptography scheme is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n paricipants.In (k,n)-VCS,any k out of n shares can recover the secret image,but any less than k shares donot have any information about the secret image other than the size.

Awards and Accolades:

- Secured second place in technical paper presentation contest conducted by S.V.U,Tirupathi
- Stood in state second place in 35th maths Olympiad test
- Secured second place in mock GATE at VIGNAN MAHOTSAV,2008
- Got state level second rank in A.I.M.Ed talent search exam in class 9th

Personal Profile:

Name	:	M.V.VARUN BABU
Father’s Name	:	M.BASAVAIAH
Date of Birth	:	25-08-1989
Sex	:	Male
Nationality	:	Indian
Marital Status	:	Unmarried
Languages	:	English, Telugu
Permanent Address	:	D.no:40-12-1/6, Ist line,Kammapalem, Ongole, Prakasam district,A.P.523001
Hobbies	:	playing cricket

Strengths:

- Good communication skills with a positive attitude and an urge to take up challenging darer.
- Work sincerely to obtain the best results.
- Enthusiasm to learn new unknowns.

Extra-curricular activities:

- Take part in SKILL POOL, a student organizing committee in college
- Participated various competitions like quiz, debate, jam, floor crossing
- Organiser of alumni function held in 2008

CURRICULAM VITAE

CONTACT INFORMATION:

B.sarala kumari

Email:saralakumari15@gmail.com

Phone:9573160133

CAREER OBJECTIVE:

Intend to build a career in an enterprise swarming with committed and dedicated people which will help me to explore myself.

ACADAMIC PROFILE:

S.No.	Qualification	Name of the Institution	Aggregate	Year of duration
1.	B.Tech. (Electronics& Communication Engineering)	Bapatla Engineering. College, Bapatla.	80.0%	2006-10
2.	Intermediate	Smt.Doddapaneni Indira Mahila Kalasala,Tenali.	92.1%	2004-06
3.	S.S.C.	K S Munciple high School,Tenali.	89.6%	2003-04

SOFTWARE SKILLS:

C, basics of C++.

SUBJECTS OF INTEREST:

1. Linear Control Systems
2. Analog Communications

ACADEMIC PROJECT:

Project name : Colour Visual Cryptography Schemes

Implemented with : MATLAB 7.5.0.

Description:

Visual cryptography scheme is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n paricipants.In (k,n)-VCS,any k out of n shares can recover the secret image,but any less than k shares donot have any information about the secret image other than the size.

PERSONAL INFORMATION:

Father name	: B.Srinivasa Rao
Date of Birth	: 16th june 1989
Gender	: Female
Nationality	: Indian
Marital status	: Single
Mother tongue	: Telugu
Languages known	: Telugu,English
Strength	: Hardworking nature
Hobbies	: Listening to music
Address	: Dr.no:13-8-25, Imam khan street, Panduranga pet, Tenali, Guntur (Dt), Andra Pradesh. Pin no:522201.

CURRICULAM VITAE

KOTHA SILPA

CONTACT INFORMATION:

Email: silpaele@gmail.com

Phone: 9440273617

CAREER OBJECTIVE:

To work in a challenging organization where my skills are best utilized in the growth of the organization.

ACADAMIC PROFILE:

S.No.	Qualification	Name of the Institution	Aggregate	Year of duration
1.	B.Tech. (Electronics& Communication Engineering)	Bapatla Engineering. College, Bapatla.	85.67%	2006-10
2.	Intermediate	Sri chaithanya mahila kalasala,Thirupathi	96.8%	2004-06
3.	S.S.C.	Sudhaha little citizens high school	92.78%	2003-04

SOFTWARE SKILLS:

C, basics of C++.

SUBJECTS OF INTEREST:

1. Communications
2. Circuit theory

ACADEMIC PROJECT:

Project name : Colour Visual Cryptography Schemes

Implemented with: MATLAB 7.5.0.

Description:

Visual cryptography scheme is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n paricipants.In (k,n)-VCS,any k out of n shares can recover the secret image,but any less than k shares donot have any information about the secret image other than the size.

PERSONAL INFORMATION:

Father name	: K.CHENCHI REDDY
Date of Birth	: 20th march 1989
Gender	: Female
Nationality	: Indian
Marital status	: Single
Mother tongue	: Telugu
Languages known	: Telugu,English.
Strength	: positive thinking and quickness in learning.
Hobbies	: Listening to music,pencil sketching

Address : 8-88 royal nagar,
r.c.road,
Tirupathi,
Chithoor dst,
Andra Pradesh.
Pin no:517501.

CURRICULAM VITAE

SRUJANA VELAGA

CONTACT INFORMATION:

Email: velagasrujana146@gmail.com

Phone: 9492524898

CAREER OBJECTIVE:

To work in a professionally inspiring environment where I can ceaselessly improve my skillset and help in the growth of the company.

ACADAMIC PROFILE:

S.No.	Qualification	Name of the Institution	Aggregate	Year of duration
1.	B.Tech. (Electronics& Communication Engineering)	Bapatla Engineering. College, Bapatla.	70.2%	2006-10
2.	Intermediate	Nalanda girls junior college,Vijayawada	92.4%	2004-06
3.	S.S.C.	Sri Viswasanthi EM School, Vuyyuru.	92.83%	2003-04

SOFTWARE SKILLS:

C, basics of C++.

SUBJECTS OF INTEREST:

1. Digital Communications
2. Analog Communications

ACADEMIC PROJECT:

Project name : Colour Visual Cryptography Schemes

Implemented with : MATLAB 7.5.0.

Description:

Visual cryptography scheme is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n paricipants.In (k,n)-VCS,any k out of n shares can recover the secret image,but any less than k shares donot have any information about the secret image other than the size.

PERSONAL INFORMATION:

Father name	: V.Venkateswara Rao
Date of Birth	: 27th July 1989
Gender	: Female
Nationality	: Indian
Marital status	: Single
Mother tongue	: Telugu
Languages known	: Telugu,English,Hindi.
Strength	: Zeal and quickness in learning.
Hobbies	: Reading books and listening to music
Address	: 8-293,Sai Nilayam, Chowdary Pet, Vijayawada, Krishna dst, Andra Pradesh. Pin no:520007.

CURRICULAM VITAE

NARRA SOMA SEKHAR VARMA,
s/o N. venkateswarlu,
h/no:4-9-59/7,
patel nagar 3rd line,
bapatla,
guntur (d.t), e-mail:sekhar.483narra@gmail.com
pin: 522101. contact no: 08643 220588.

OBJECTIVE:

To obtain a nice position in an organization where I could get enough opportunity to prove my

potential and commitment and which will enhance my knowledge and skills and give me scope

in latest trends.

EDUCATIONAL QUALIFICATION:

- **B.Tech** (**E.C.E**) from **Bapatla Engineering College** , **Bapatla** with an aggregate of **65.00%** up to final year first semester.
- **Intermediate(M.P.C)** from **Sri Nalanda Junior College,Bapatla** with an aggregate of **88.00%** in **2006.**
- **S.S.C** from **Bapatla Public School,Bapatla** with an aggregate of **73.18%** in **2004.**

SOFTWARE SKILLS :

- **Languages** **:** Basics of **C, C++, DS,Matlab.**

STRENGTHS:

- Positive attitude.
- Self Confidence.
- Easily mingling with others.

HOBBIES:

- Listning Music.
- Singing Songs.

PROJECT:

Project	**: Visual Cryptography Schemes**.
Front end	**:** Monitor.
Back end	**:** Data base.
Software	**:** Mat lab.

PERSONAL PROFILE:

Father's name	**:** N. Venkateswarlu,
Date of Birth	**:** 28-05-1989.
Languages known	**:** English, Telugu, Hindi.
Gender	**:** Male.
Nationality	**:** Indian.