THE FLORIDA STATE UNIVERSITY

COLLEGE OF ARTS AND SCIENCE

A MODERNIZED VERSION OF VISUAL CRYPTOGRAPHY

By

MAHESH KUMAR PATEL

A thesis submitted to the
Department of Computer Science
in partial fulfillment of the
requirements for the degree of
Master of Science

Degree Awarded:
Spring Semester, 2003

The members of the Committee approve the thesis of Mahesh Kumar Patel defended on February 21 2003.

Yvo Desmedt
Professor Directing Thesis

Lois Hawkes
Committee Member

Mike Burmester
Committee Member

Approved:

Sudhir Aggarwal, Chair
Department of Computer Science

The Office of Graduate Studies has verified and approved the above named committee members

To Mom, Dad, Mitul, Ashish and Jivantika…

ACKNOWLEDGEMENTS

My deepest thanks to my Major Professor, Dr Yvo Desmedt in whose guidance I learnt about the principles of cryptography. Special thanks also goes to my committee members, Dr. Lois Hawkes and Dr. Mike Burmester. Their help in writing of this Thesis is highly appreciated. Finally I appreciate Ms. Elenor McNealy's help in arranging the projectors and the room whenever I needed them. This work was supported in part by the US Army Research Office, grant numer DAAD19-01-1-0502.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

In this thesis we adapt the concept of visual cryptography to digital projectors as opposed to over-head projectors. Digital projectors are used to project the images from the computer monitor, whereas over-head projectors display the image from the transparencies placed on them. The schemes developed in this thesis guarantee perfect secrecy and also provide the best possible contrast. By using two projectors, there is no need for any computational device or a complex approach to decrypt the message. Decryption is done by the human visual system and the laws of Physics.

CHAPTER 1

INTRODUCTION

The concept of visual cryptography was first proposed in the open literature by Naor and Shamir [2] in 1994. In this novel idea, an image consisting of text, drawings etc., is encrypted into two images. These images reveal nothing about the original image (plaintext). These images are given to two different parties as shares. Decryption is not possible without having both of them together. These shares are stored on transparencies and the process of decryption begins with stacking these two transparencies together on the over-head projector. Decryption is then done by the human visual system because the schemes are based on how we perceive and differentiate different gray levels and the laws of Physics. This idea of having the original image (plaintext) encrypted into two shares and the requirement of having both for decryption is called 2-out-of-2 secret sharing. Similarly, having m shares for an original image (plaintext) with the requirement for at least s shares for decryption would be s-out-of-m secret sharing. While overhead projectors were used almost exclusively in 1994 when Naor and Shamir invented visual cryptography, today these are being replaced by digital computer projectors. So, we extend visual cryptography for the use with digital projectors. Note that we are not interested in steganographic use of visual cryptography as was done in [1]. The application of visual cryptography is described in Figure 1.1.

In Figure 1.1 we need to transfer an image to the destination realiably without the information being leaked. Using visual cryptography, we at the source encrypt the original image using a computer into two shares, “Share 1” and “Share 2”. These

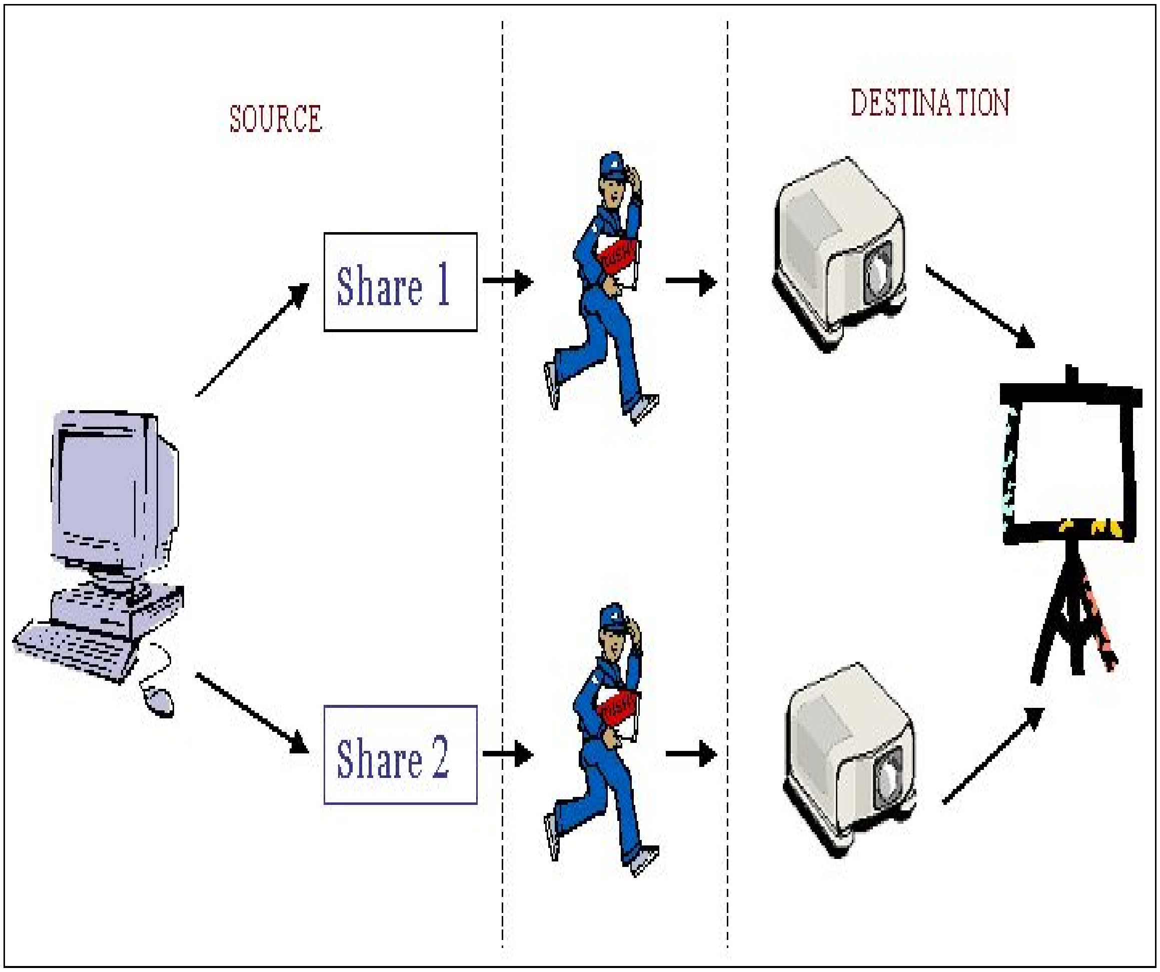

Figure 1.1. The application of visual cryptography

shares do not reveal anything about the actual image and are independent of one another. So by looking at either of these shares, nothing is revealed about the original image. These shares are then given to two separate reliable couriers. These couriers follow different paths in reaching the destination. The probability that both of them are intruded upon is thus halved. By having two separate couriers follow different routes and each sharing a secret we decrease the chance that the secret would be leaked while it is in transition from the source to the destination. Even if either one of the couriers is compromised or intruded we ensure that original image is not revealed. Once the shares have reached the destination they are projected on the screen using two projectors and the shares are decrypted by the human eye.

The remainder of this document is organized as follows. In the next chapter we discuss the background knowledge required to understand visual cryptography. Here we will also describe the Naor and Shamir scheme. The third chapter deals with the main idea of our scheme. We then discuss the implementation issues regarding visual cryptography. After that in the fifth chapter, we present the various schemes.

CHAPTER 2

BACKGROUND

In this chapter, we start with the explanation of the one-time pad scheme. We will explain why it is totally secure and then we describe the Naor and Shamir scheme in detail.

2.1 One-time Pad

The one-time pad commonly known as Vernam's one-time pad [7] is a cryptography scheme which is perfectly secure. In this scheme a message string of symbols belonging to a finite alphabet set A, on which an operation "*" is defined. For example consider A to be 0, 1 and the operation be exor (exclusive or $\oplus$). Now during the encryption process, there is a key having length equal to that of the message. The important point to be noted here is that if we have $c = g \oplus k$, then $g = c \oplus k$. Here g is the message symbol, c the encrypted message and k the key. Using this fact, the message of string is encrypted using random order of string which forms the key. Assume c_i, g_i and k_i to be the i^th symbols of the ciphertext, message and the key respectively. Therefore according to the algorithm, $c = g \oplus k$ and $g = c \oplus k$. This scheme is perfectly secure because the message g is independent of the ciphertext c. Formally:

$$proablity(message = g|c = k \oplus g) = proablity(message = g)$$

2.2 Technical Survey of Naor and Shamir's paper

In their original paper [2] in 1994, the idea of visual cryptography was applied to transparencies for secret sharing. We present here a brief outline of this novel idea.

The simplest of the implementations assumed that the message (original image) consisted of a collection of black and white pixels. The original image was encrypted into different shares. Each of the share is part of the secret sharing scheme which is the underlining principle of visual cryptography. These shares are represented on transparencies hence decryption is done by stacking them up (proper alignment) to reveal the original image.

The black and white pixels from the original image are represented differently in shares by a set of subpixels. Hence each white pixel would be represented by a set of subpixels in the shares and similarly for the black pixel. A convention is followed such that '1' represents black and '0' represents white. Each pixel is represented by i subpixels which are a row of pixels. In the model each pixel is shared into m shares. The structure which is derived from the model is a $m \times i$ Boolean matrix $B = [b_{jk}]$. The original pixel is decrypted by stacking the transparencies together. The gray weight of the combined share is proportional to the Hamming weight $H(V)$ of the shares. The human eye interpreted as white if $H(V) < d - \alpha i$ for some threshold $1 \leq d \leq u$ and relative difference $\alpha > 0$ and black if $H(V) \geq d$.

In the framework, there are two matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. During the encryption process, the white pixel is shared from one of the matrices in $\mathcal{C}_0$ and the black is shared from one of the matrices in $\mathcal{C}_1$. In this framework a s-out-of-m visual cryptography scheme, contrast is ensured by:

1. For any share, the "or" V of any s of the m rows satisfies the condition that $H(V) \leq d - \alpha i$. This condition is true for a white pixel in the original image.

2. For any share, the "or" V of any s of the m rows satisfies the condition that $H(V) \geq d$. This condition applies for a black image.

To guarantee security we should insure that if there are less than s shares, no information is leaked. Assume that there are q shares available and $q < s$, and the rows from matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ occur with equal probability. When these cases are considered, the Hamming weight follows a uniform distribution $H(V) = f(q)$.

So essentially there are two criteria for visual cryptography to work, security and contrast. For better contrast, i should as small as possible and α should be as large as possible.

2.2.1 Encryption

In this section we will show a simple scheme which is 2-out-of-m scheme. Assuming that 1 represents a black pixel and 0 a white pixel throughout the text.

The set of matrices $\mathcal{C}_0$ is obtained by permutating the columns of the following matrix

$$\begin{bmatrix} 100...0 \\ 100...0 \\ ... \\ 100...0 \end{bmatrix}$$

The set of matrices $\mathcal{C}_1$ is obtained by permutating the columns of the following matrix

$$\begin{bmatrix} 100...0 \\ 010...0 \\ ... \\ 000...1 \end{bmatrix}$$

Shares are represented by rows in both the matrices. Each share hence has only one black subpixel but $i - 1$ white subpixels. Taking the Hamming weight for the "or" of any two shares in matrix C_0, we get 1 and for that of matrix $\mathcal{C}_1$ we have 2. Hence $\mathcal{C}_1$ looks darker when stacked together. Reducing the problem to a 2-out-of-2 visual cryptography scheme, it can be solved using two subpixels. Thus i in this case is equal to 2. Therefore all the matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ would look like:

$$\mathcal{C}_0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$$

$$\mathcal{C}_0 = \begin{bmatrix} 01 \\ 01 \end{bmatrix}$$

$$\mathcal{C}_1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$$

$$\mathcal{C}_1 = \begin{bmatrix} 01 \\ 10 \end{bmatrix}$$

Although the 2-out-of-2 visual secret sharing scheme could be solved using 2 pixels, the aspect ratio of the original image is distorted. In order to maintain this, the subpixel is a square block consisting of $i \times i$ subpixels. Lets assume that the original image has $r \times r$ pixels. Each of these pixels are represented by $i \times i$ subpixels. Hence the shares would be of size $ri \times ri$. These shares are to be arranged such that subpixels are properly aligned. The original individual pixel would be represented in the decrypted image by $ri \times ri$ subpixels too.

Applying this to the 2-out-of-2 scheme, the matrices are represented as follows:

$$\mathcal{C}_0 = \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix}$$

$$\mathcal{C}_1 = \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix}$$

Each row of the shares is 4 sub-pixels in length and is encrypted into 2×2 block. While encrypting a white pixel is represented into two identical shares from either the $\mathcal{C}_0$ or $\mathcal{C}_1$ matrices. A black pixel is represented into shares from complementary shares.

These shares thus obtained are printed on transparencies. In their paper Naor and Shamir generalized the solution to s-out-of-m scheme and showed how the matrices could be obtained.

2.2.2 Decryption

The decryption is done by stacking the transparencies together on the over-head projectors.

2.3 Advantages of visual cryptography

The advantages of visual cryptography are:

- **Perfect Secrecy:** The underlining principle of encrypting the original image (plaintext) into shares is similar to the one-time pad. Visual cryptography provides perfect privacy in a similar way as the one-time pad.

- **Secure Decryption:** Today's computers are inherently insecure. Hence having computers to decrypt the shares would make it possible that the plaintext is leaked and the purpose of a perfectly secure scheme is defeated. The decryption is done by the laws of physics and by the human visual system (eyes and brain), using the basic properties of contrast. Contrast plays an important role in determining whether the human visual system can differentiate gray levels.

CHAPTER 3

MAIN IDEA

After discussing the basics of visual cryptography from Naor and Shamirs view point, we will now discuss the modernized version. In this chapter we will discuss in details using first of the three schemes (described in Chapter 5). Encryption using our scheme and the decryption is described. All our schemes are 2-out-of-2 secret sharing schemes.

3.1 Original Image and Decrypted Image

It is assumed that the image required to be encrypted consists of black and white pixels. The decrypted image however has three gray levels, namely black, white and medium gray. Medium gray will be referred to gray throughout the document. The gray pixel which is an extra color during decryption is due to the fact that when a white pixel interacts with a black pixel resulting from the shares we get a gray pixel.Black corresponds to lack of photons. White corresponds to several photons. When a white pixel from one share is overlapped by a black share (from another share), at one common point, a pixel of medium gray level is observed at that point. The interaction of a white pixel with a black pixel is shown in Figure 3.1. The gray pixel reduces the resolution of the image during decryption known as the graying effect [8]. Figure 3.2 shows the original image we will be using for the encryption.

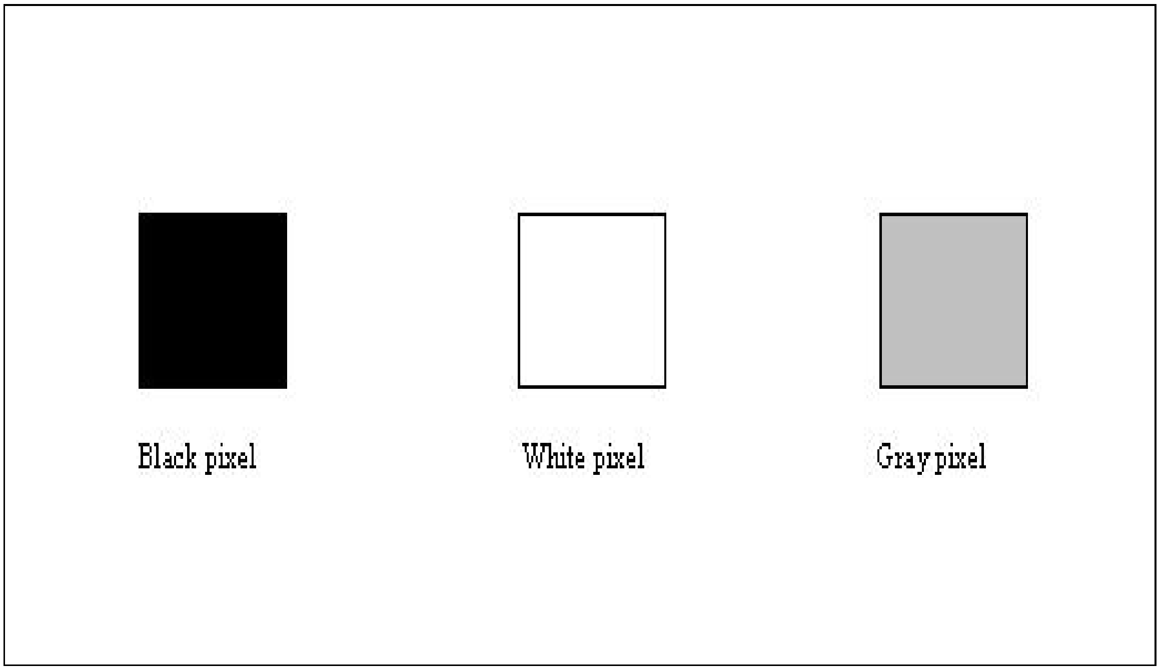

Figure 3.1. Black, White and Gray pixels

3.2 Encryption

Every pixel in the original image is mapped to blocks of subpixels as in Naor and Shamir's scheme. Let the number of subpixels in the block be n. The mapping of the original pixel into blocks of subpixels is governed by rules of encryption.

Assume that there are two blocks, Block A and Block B. These blocks are shown below in Figure 3.3.

In our schemes, we are using blocks of $n = 9$ subpixels. Hence they form a block of 3 x 3. It is to be noted that we maintain the number of subpixels to be a perfect square so that the aspect ratio of the original image is maintained during the decryption. While encrypting a pixel into two shares, we replace the pixel by blocks of subpixels in the shares. The blocks to be replaces are chosen as:

- The white pixel from the original image is replaced by two blocks in two shares in such a way that when they are decrypted they produce enough contrast that

Figure 3.2. Original image used for encryption. The image is a single word "CRYPT" with white background

they are distinguishable from the decryption of a black one. So the rules of encryption should follow this principle.

- The blocks should exist in equal probability so that looking at the blocks, it is not possible to determine whether the block originated due to black pixel or a white pixel.

The rules of encryption are shown in Table 3.1 The encryption process when we have a white pixel has two options with equal probability. It is possible to encrypt a white pixel by putting A in share 1 and B in share 2 or vice-versa. Similarly is the case for the black pixel.

Eventhough a formal proof regarding the security of the scheme is given in Chapter 5, we will show the security of the scheme. By observing the column of share 1, notice that it has blocks A and B once for each white and black pixel. Since the

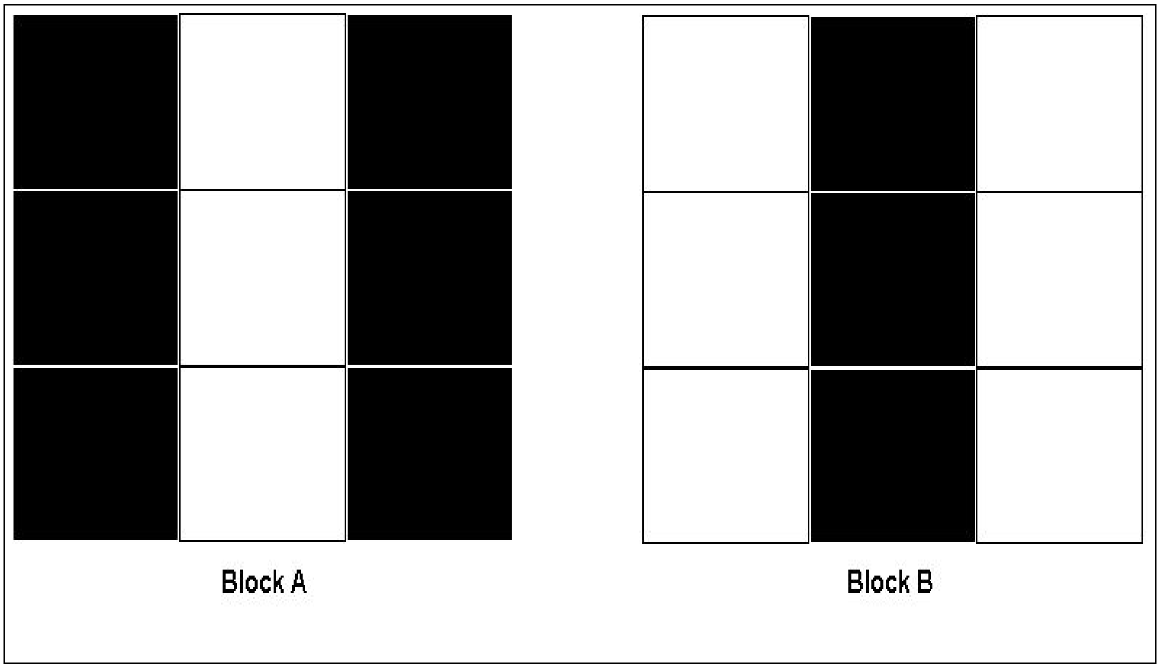

Figure 3.3. Block of subpixels

Table 3.1. Encryption rules for the first scheme

Original Pixel	Share 1	Share 2
White	Block A	Block B
	Block B	Block A
Black	Block A	Block A
	Block B	Block B

option of selecting the rules is with equal probability, we cannot determine which block originated from which block. This can be seen for the case of share 2 as well. The rules are shown diagrammatically in Figure 3.4 and Figure 3.5. Figures 3.6 and 3.7 shows the shares resulting from the encryption. As evident, none of the shares make the actual original image viewable.

It is observed from the figures that for a black pixel we selected the blocks and rules such that while decryption we get black and white subpixels. Similarly, the

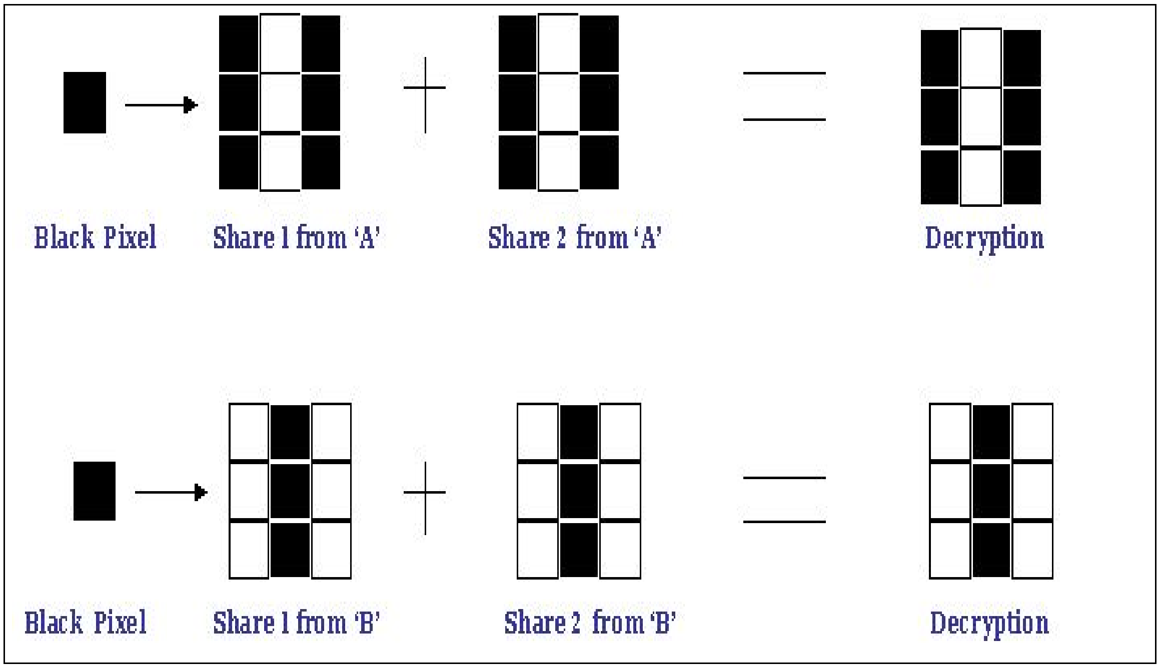

Figure 3.4. Encryption for black pixel

blocks and rules for the white pixel were selected to give gray block during decryption. This difference in color at the decryption is sufficient for the eye to distinguish color.

3.3 Decryption

Decryption in our schemes makes use of the laws of physics and the human visual system (eye and brain). The decryption process is simple, only two projectors and screen are required as necessary equipment. The image projected is decrypted by the human brain and the eye. For proper decryption the projectors should be arranged in the fashion shown in Figure 3.8. The projectors must focus on the screen so that the images overlap perfectly. Note that for best results the following points should be noted about the two projectors:

- They should be in the same plane orthogonal to the screen on which one projects.

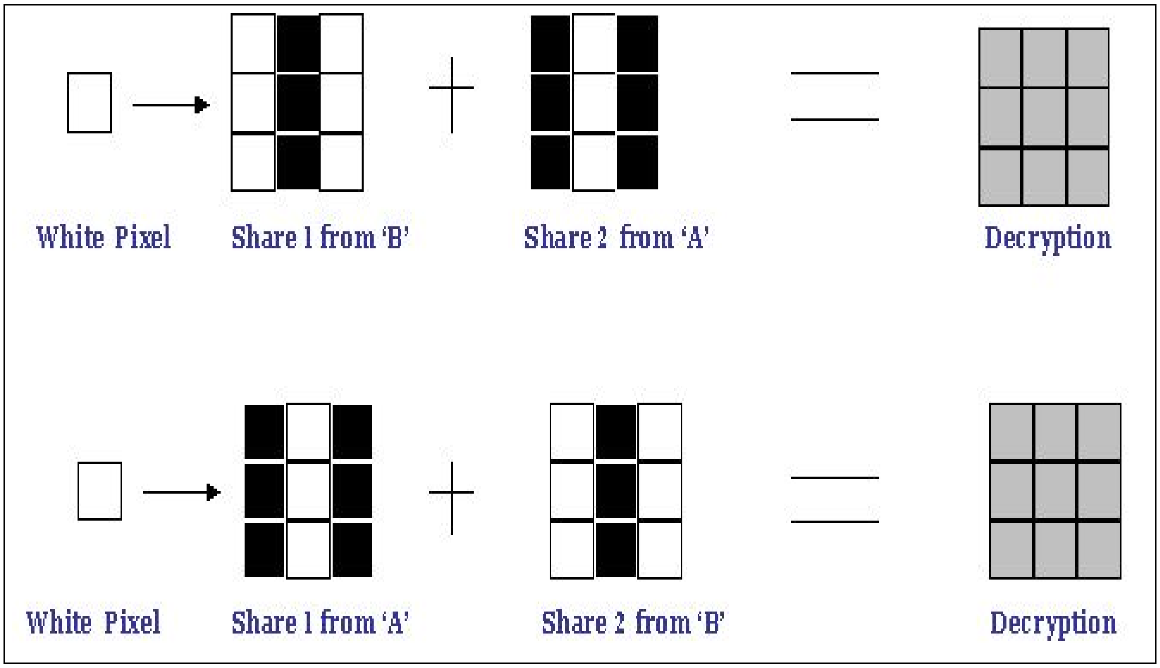

Figure 3.5. Encryption for white pixel

- They should be at equal distance from the screen.
- They should have equal properties for color representation, contrast and image dimensions.

A simulated decryption of the original image is shown in Figure 3.9. As expected the white from the original is now gray and the black from the original image is now black and white in the decrypted image.

The gray level depends on whether both projectors have the same luminance and phase differences between the photons also play a role in determining the gray level. For pixels with the same gray level from two shares at one common point, the resulting gray level remains the same. This means that a black pixel from both of the shares incident at one point would produce a black pixel, and similarly for white.

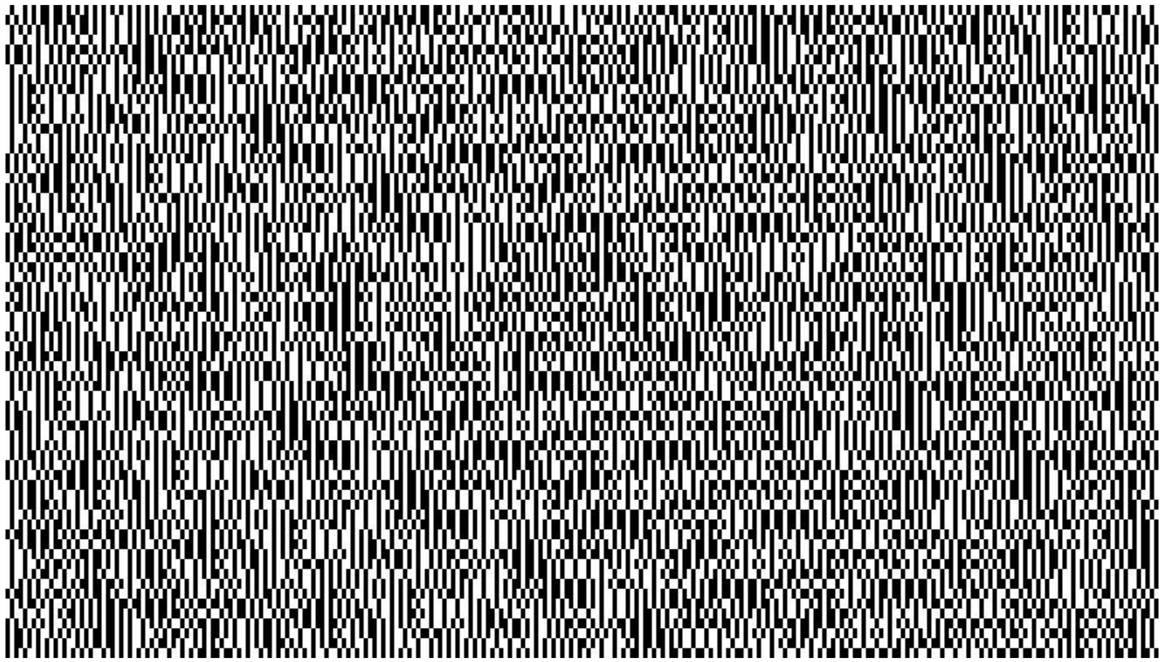

Figure 3.6. Share 1 resulting from the original image

We now describe the impact of the human visual system. The human visual system does the decryption based on the relative contrast levels of the three gray levels. Depending on the actual encoding used to produce the shares different contrast levels are obtained which are discussed in more detail in Chapter 4.

In the next chapter we discuss the implementation issues and their solutions.

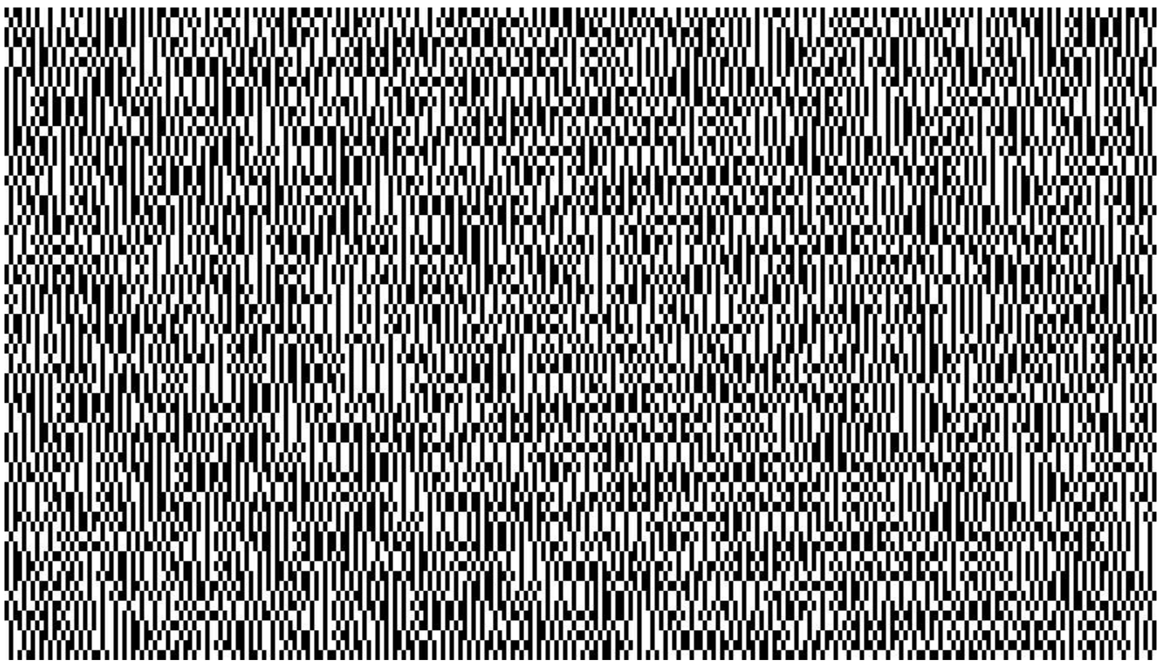

Figure 3.7. Share 2 resulting from the original image

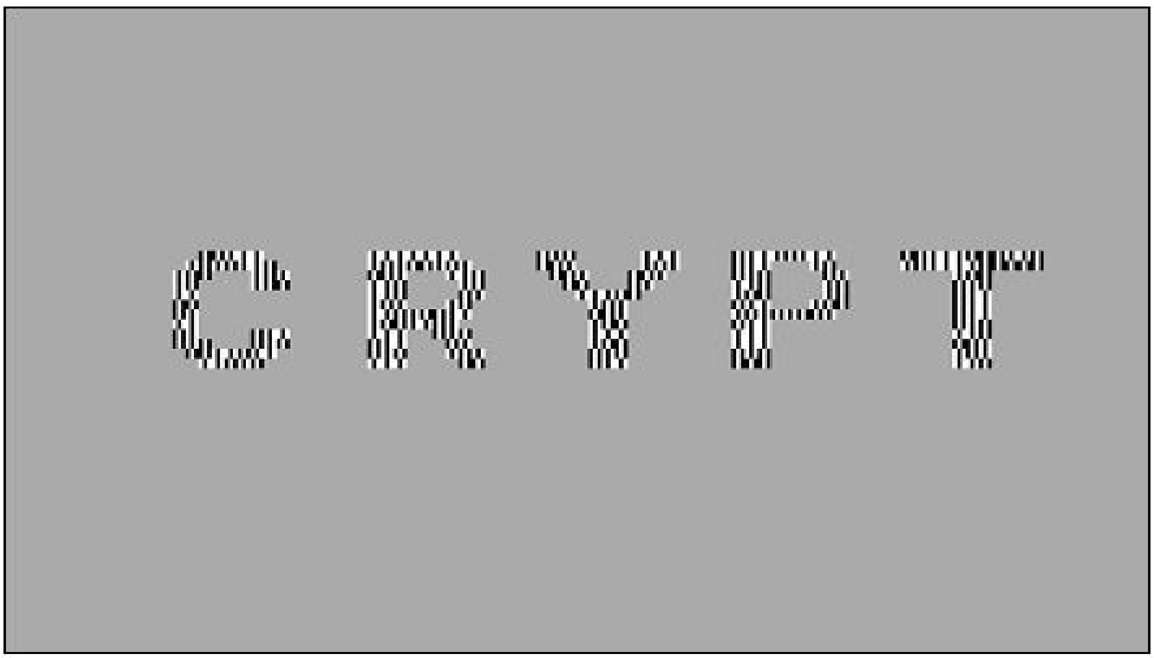

Figure 3.8. Decrypted Image

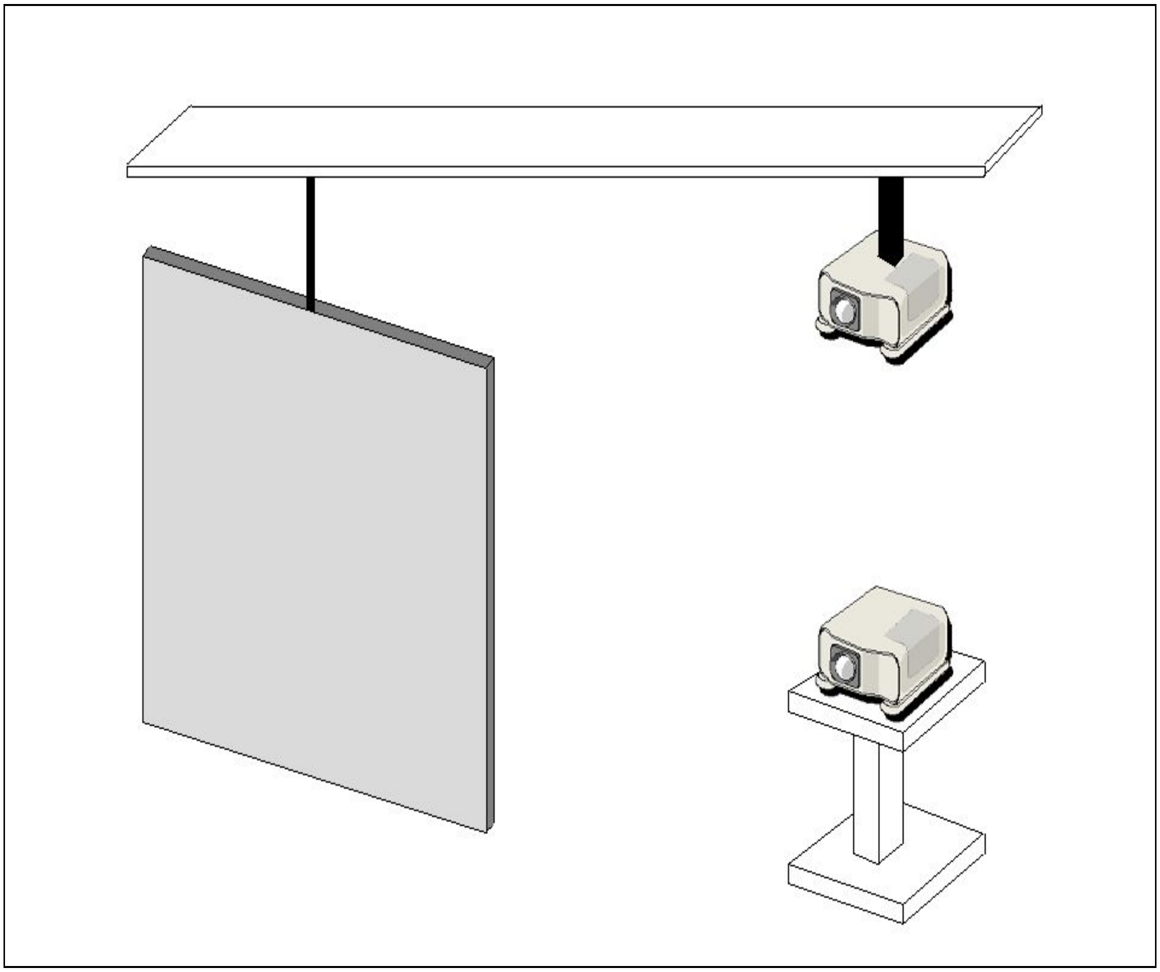

Figure 3.9. Arrangement of projectors for decryption. The projectors are focussed on a single screen so the images exactly overlap.

CHAPTER 4

IMPLEMENTATION ISSUES AND SOLUTIONS

In this chapter we present the various implementation issues where by visual cryptography can be applied effectively for practical use. The first issue has to do with synchronization of the shares which governs the visibility of the ordinal image during decryption. The second issue is contrast. Contrast is the ability to distinguish the colors by the human visual system. A practical solution to these problems are provided which circumvent these problems. Implementing the solutions increases the practicality of visual cryptography.

4.1 Implementation Issues

4.1.1 Synchronization

This is a typical problem, which Naor and Shamir's scheme also suffered from. Aligning the shares from the projectors is difficult, as each pixel from one share should overlap with the corresponding pixel from the other share to get the desired image. Figure 4.1 shows simulations of misaligning the shares. As observed when images are misaligned by one pixel each in the x and y coordinate, the white of the original image (Figure 3.2) which was represented by medium gray is not totally gray. The black of the original image is distorted to a large extent and is not very clear as the one without misalignment.

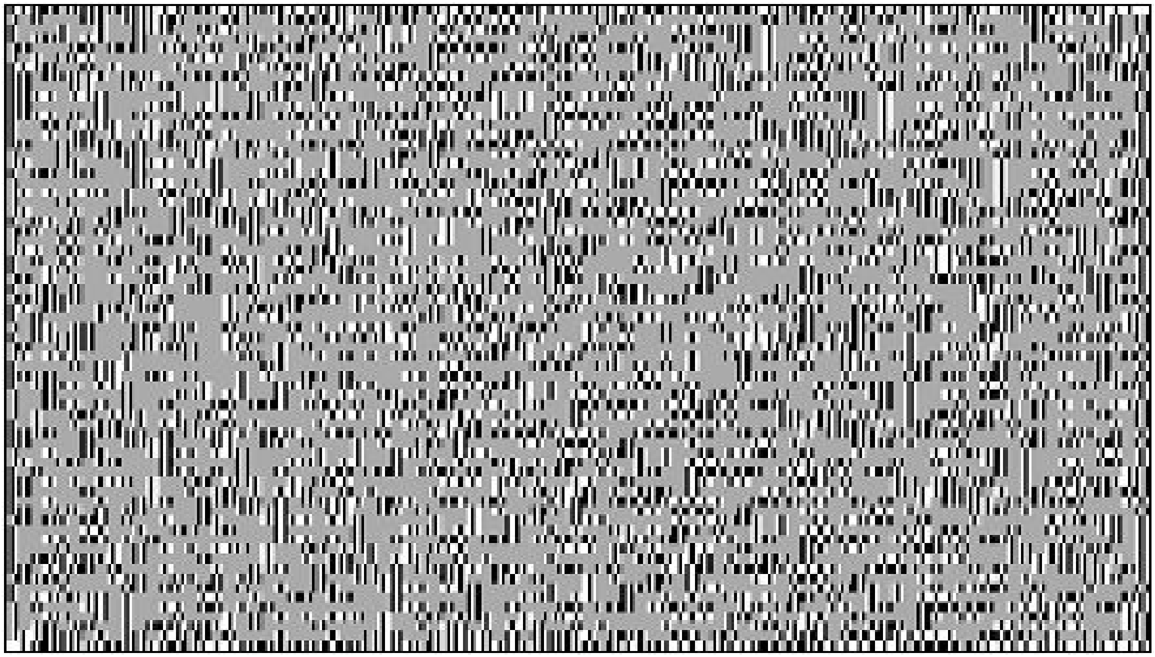

Figure 4.1. Decrypted image with misaligning the shares by one pixel, both horizontally and vertically. As observed the image is not very clear and is as bad as the shares.

4.1.2 Contrast

A second issue is related to the decryption done by the visual system. The nature of the combined shares by the projectors should be such that the black from the original images (plaintext), which is represented by a set of pixels, should stand out from the set of pixels representing white. The contrast in images is dependent on "Simultaneous Color Contrast". The phenomenon is explained by the Figure 4.2. This is an illusion in which the human vision system perceives different color for the same color depending on the background. In Figure 4.2, the ring in the middle is medium gray in color. But the human eye is clearly able to distinguish it in blocks A and D rather than in blocks B and C. Using this fact, we try to distinguish white and black pixels from the original image. So while selecting the blocks and rules for

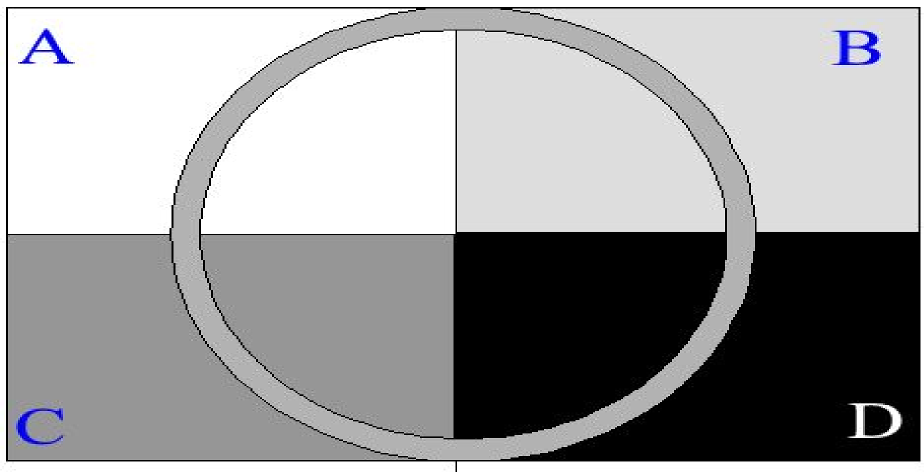

Figure 4.2. Showing the illusion called "Simultaneous Color Contrast". Notice the ring is of uniform density throughout. However it appears brightest is block A, lightest in block D and intermediate in blocks B and C

encryption, we try to make white decrypted to gray and black decrypted to black and white. It is generally required to avoid gray pixels where the original pixel is black. Whenever the original pixel was white, it is required to have it as gray without any black or white. This approach would produce the best contrast based on simultaneous color contrast.

4.2 Solutions

4.2.1 Solution for Synchronization

The task of aligning the shares can be mitigated by the two following methods:

Increasing the pixel size: The original image is assumed to be of size r x r. The shares are of size ri x ri. Now for proper decryption each of the pixels of all the shares should be properly aligned. As this is not easy, we have included a method

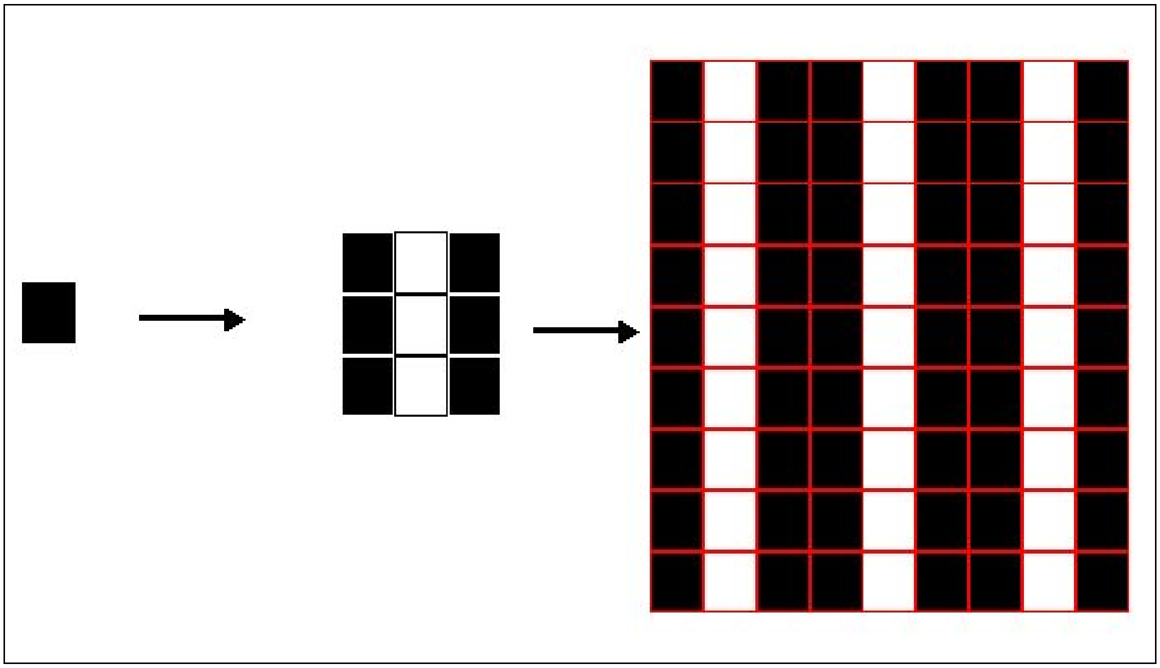

Figure 4.3. The mapping of a single pixel into a set of 9 subpixels and further mapping it to 81 subpixels, as a solution to problem of synchronization.

which allows tolerance so that even if the pixels are misaligned by a couple of pixels, decryption is relatively clear. To achieve this, each pixel from the share is blown by b x b pixels. With this, a white pixel in the share which was originally represented by a single pixel would now be represented by b^2 white pixels.This would increase the size of shares to rib x rib. This solution is illustrated in Figure 4.3. In the first scheme we showed in Chapter 3, we mapped a single pixel into 9 subpixels. In the solution here will map into block of 9 x 9 subpixels. The positive result is shown in Figure 4.4. Comparing this with Figure 4.1, the solution shows marked improvement.

Marking out colored borders: Another method that helps with the alignment is having colored borders on the periphery of the shares. In this way, aligning the shares would not require aligning the pixels but the colored borders, which turns out to be a lot easier. Tests have demonstrated that this last method helps, but is insufficient

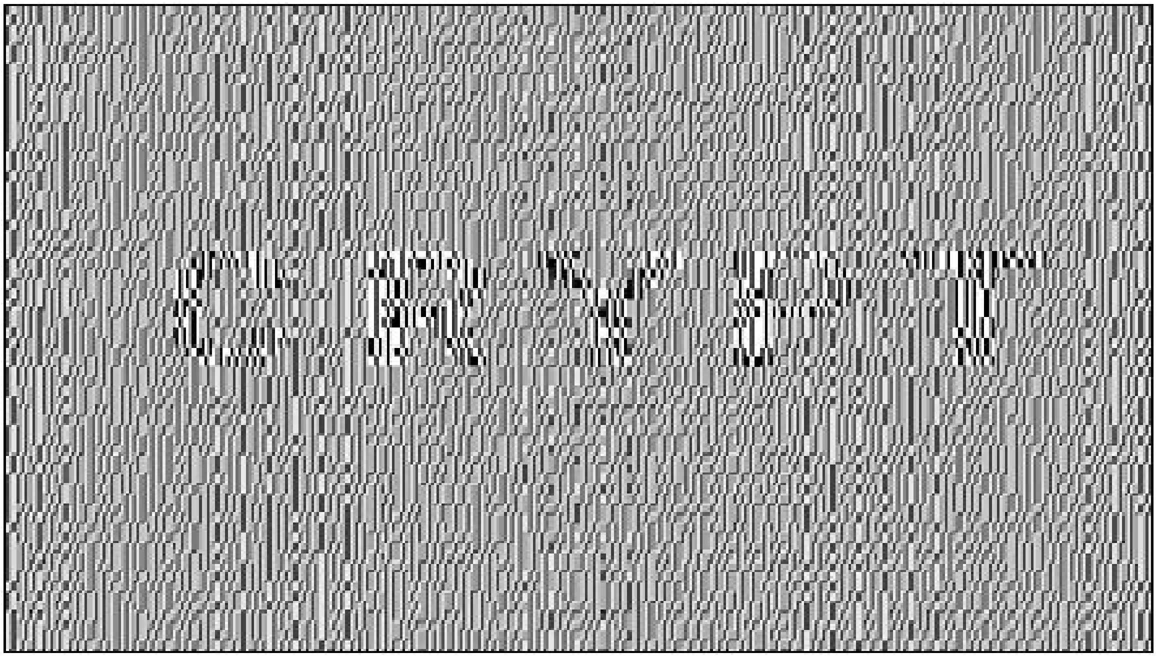

Figure 4.4. Decrypted image with misaligning the shares by one pixel, both horizontally and vertically. As observed the image although not very clear is still viewable to the human eye

on itself to deal with the synchronization problem. Reducing the resolution is the main solution.

4.2.2 Solution for Contrast

To effectively decrypt the image from the shares and to take care of “graying effect” of the decrypted image, it is required that the white pixel from the original image decrypts to all gray pixels. The black pixel from the original image decrypts to white and black pixels only. This done so that the contrast provided from using this method is better as described by the simultaneous color contrast.

We surveyed models that have a metric for contrast. In [3] (Chapter 4) each gray level, white, black and medium gray is given a reflective index. The value for black in [3] is 0.05, white is 0.9 and for medium gray it is 0.5.

As explained in Section 3.2.1, each virtual pixel corresponds to i x i subpixels pixels.Using these values and the coding used for the creation of the shares results gives the effective value for reflective index. We illustrate this for our variant schemes in Section 4. Let ρ_b and ρ_w be respectively the average reflective index of a decrypted black and white plaintext. ρ_b is calculated by summing up the reflective indices for all the pixels in the decrypted black pixel based on thier values. Similarly ρ_w is calculated for white. For our model, there are three more variables used to calculate contrast, n_b, n_w and n_g.

n_b is the number of rules which result in black pixels in the decrypted image corresponding to the white pixel from the original image. n_w is also the number of rules which result in white pixels in the decrypted image corresponding to the white pixel from the original image. n_g is the number of rules which result in gray pixels in the decrypted image corresponding to the black pixel from the original image. The contrast as explained above is proportional to the difference of average reflective indices of the decrypted image. Contrast is however inversely proportional to the sum of n_b + n_g +n_w. Using our first scheme, looking at Figure 3.4 $n_g = 0$. From Figure 3.5, $n_w = 0$ and $n_b = 0$.

The equation for contrast

$$C_t = \frac{|\rho_b - \rho_w|}{1 + n_b + n_w + n_g}. \tag{4.1}$$

Thus C_t is 0.225 for the first scheme. It is observed that C_t is directly proportional to the difference of ρ_w and ρ_b, and in inversely proportional to the sum of $1 + n_b + n_w + n_g$. Hence, larger the value C_t, the better the contrast. In the next chapter we will describe the maximum the value of C_t with the optimum scheme and give a formal proof for unconditional security that our scheme provides.

CHAPTER 5

SCHEMES

We begin this chapter by marking out the differences between our scheme and Naor and Shamir's scheme.Then we describe two more schemes to illustrate the optimum scheme and prove that the schemes are secure.

5.1 Differences with Naor and Shamir schemes

The main difference between Naor and Shamir's [2] schemes when used for overhead projectors and our computer projectors scheme is the following. The decrypted image in our scheme has three gray levels as opposed to two gray levels in the case of overhead projectors.

Although Naor-Shamir's schemes were originally designed for overhead projectors one can attempt to use these for overhead projectors. We now discuss this aspect.

5.2 Towards an optimal scheme

5.2.1 Second Scheme

For our second scheme we use 4 blocks of pixels we call A, B, C, and D. The structure of the different blocks in terms of subpixels is shown in Figure 5.1. The rules for our second scheme is given in Table 5.1.

The pixel assignment of sets A, B, C and D are shown in Figure 4.4 and are listed below. Note that 1 corresponds to black and 0 corresponds to white.

1. A = [1 1 1 1 1 0 0 0 0]

Table 5.1. Encryption rules for the second scheme

Original	Share 1	Share 2
White	A	B
	B	A
	C	D
	D	C
Black	A	D
	D	A
	C	B
	B	C

2. B = [0 0 0 0 0 1 1 1 1]

3. C = [0 0 0 0 1 1 1 1 1]

4. D = [1 1 1 1 0 0 0 0 0]

From Section 3.2.2, $\rho_b = 4.3$, $\rho_w = 4.5$, $n_b = 0$, $n_w = 0$ and $n_g = 2$. Using Eq. 4.1, we obtain a contrast of 0.067. However for $n = 9$, this does not give the best contrast. We discuss an optimal solution in Section 5.2.3. Figure 5.2 shows the simulation for the decrypted image using second scheme. It is to be noted that there are gray pixels where there should be either black or white pixels which reduce the contrast.

5.2.2 Proof of security

Theorem 1 The scheme gives perfect privacy.

Proof The probability that the 2nd block is B and the pixel is white is:

P(block in 2nd share = B, pixel is white)

$= \sum_{i=1}^{1} P(block\ in\ 2nd\ share = B, pixel \text{ is } white, block \text{ in } 1st\ share = i)$

$=\sum P(block\ in\ \ 2nd\ share = B|block\ in\ 1st\ share = i, pixel\ is\ White)$

$*P(pixel\ is\ white, 1st \text{ block } = i)$

Now, B can be the second share from Rule (1) of white iff 1st share is A. Therefore if i = A

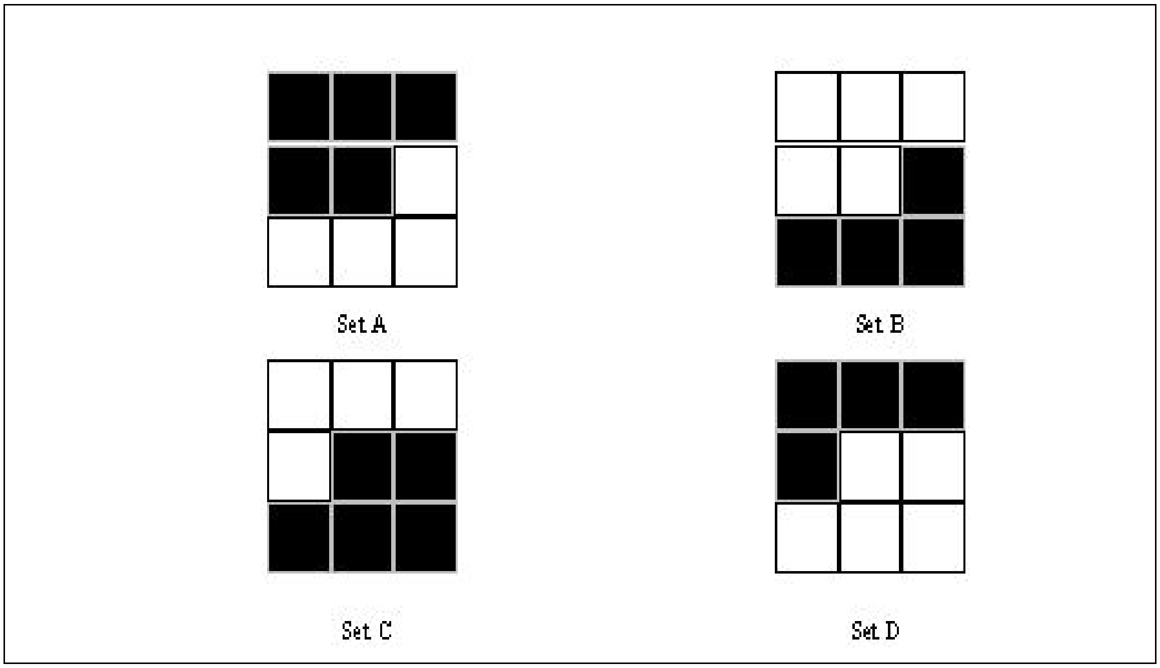

Figure 5.1. Blocks A,B,C and D in terms of pixels

$= \sum P(block\ in\ 2nd\ share = B|block\ in\ 1st\ share = A, pixel\ is\ White)$

$*P(pixeliswhite, 1st$ block $= A)$ ....Eq(1)

Since each of the block is selected with equal probability and

P(2nd block=B| 1stblock =A, Pixel is White) = 1 Therefore Eq(1) becomes:

= 1 * P(Pixel is White, 1st block = A)

= 1 * P(1st set = A) * P(White)

= 1 * (1/4) * P(White)

= (1/4) * P(White)

Similarly, P(2nd block = B, pixel is black) = (1/4) * P(black)

Since, the probability that the second block is B, given pixel is white is (1/4) times the probability the pixel being white, and the probability that second share is

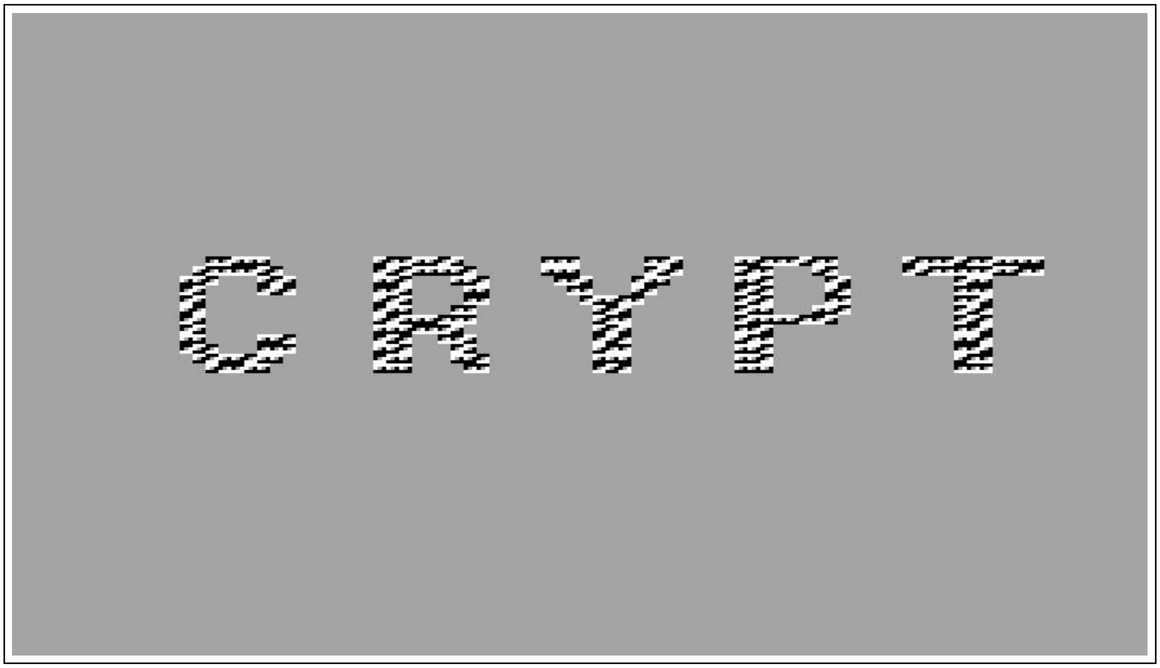

Figure 5.2. Simulated decryption of second scheme

B, given pixel is black is (1/4) times the probability the pixel is black, the scheme is secure and does not leak for B.

It can be easily proved for sets A, C and D as well. Hence the above scheme is secure.

5.2.3 Scheme for Best Contrast

We present a scheme which according to Eq.4.1 produces the best contrast for n = 9. We use two blocks A and B with the following pixels:

1. A = [1 1 1 1 1 0 0 0 0]

2. B = [0 0 0 0 0 1 1 1 1]

The encryption is based on the following rules given in Table 5.2.

Table 5.2. Encryption rules for an optimal contrast scheme

Original	Share 1	Share 2
White	A	B
	B	A
Black	A	A
	B	B

From our model, ρ_w = 4.5, and ρ_b= 4.7 if rule (2) is applied, and ρ_b= 3.85 if rule (1) is applied. So on average ρ_b= 4.275. n_b= 0, n_w = 0 and n_g = 0. Hence C_t = 0.225. This is the maximum value possible for C_t when n = 9 as shown by the following proof.

Theorem 2 For n = 9 the maximum value possible is 0.225.

Proof Considering the denominator, the least value is 1 when n_w, n_g and n_b are all zero. Now consider the numerator. Assuming n_g is zero the number of total count white pixel and black pixel would be 9 each. Hence the difference between ρ_b and ρ_w is always 0.225 under the assumptions that n_g is zero. hence the maximum value is 0.225 The simulated decryption is shown in Figure 5.3 for the scheme with the optimum contrast.

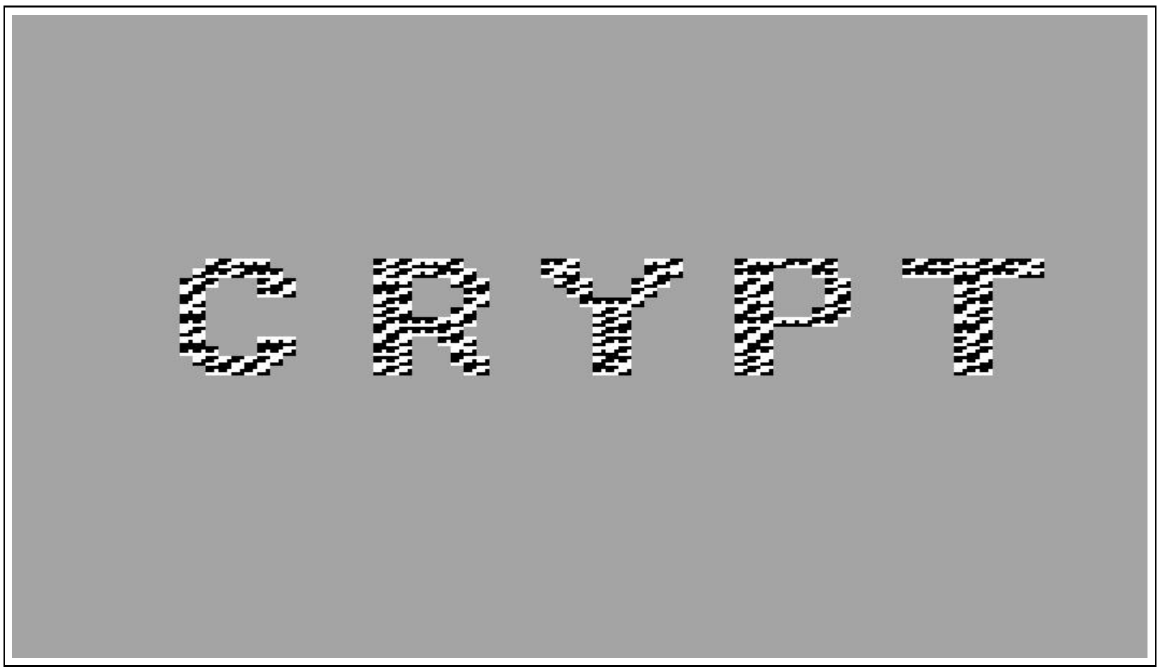

Figure 5.3. Simulated decryption for the scheme with the best contrast

CHAPTER 6

CONCLUSIONS

Our scheme uses projectors as opposed to transparencies described by Naor and Shamir's scheme. The modernized version described is totally secure as the one-time pad scheme. Although there are inherent problems on alignment of the shares, we have described methods to make the task easier. We have also shown a metric to calculate the contrast and created one with the best contrast.

Our scheme deals only with black and white pixels, so further development in this area would address pixels of more than two gray levels or color.

REFERENCES

[1] Y. G. Desmedt and Tri Van Le. *Moire Cryptography*. 7th ACM Conference on Computer and Communications Security, Athens, Greece, 2000.

[2] M. Naor and A. Shamir. *Visual Cryptography*, *Advances in cryptology - Eurocrypt - 1994*.

[3] Theodore Fuchs. *Stage Lighting*. Benjamin Blom, Inc, New York.

[4] Joseph B. Murdoch. *Illumination Engineering - From Edison's Lamp to the LASER*. MacMillan Publishing Company, New York.

[5] Douglas R. Stinson *Cryptography - Theory and Practice*. CRC Press LLC, Boca Raton, Florida.

[6] Stephen E. Palmer *Vision Science* . Cambridge, Mass, MIT Press, 1999.

[7] M. Atallah, editor *Handbook of Algorithms and Theory of Computation* . CRC Press LLC, Boca Raton, 1998.

[8] Douglas R. Stinson *An introduction to visual cryptography* Available at http://bibd.unl.edu/stinson/VCS-PKS.ps.

[9] Bruce Schneier *Applied Cryptography: Protocols, Algorithms, and Source Code in C* . John Wiley Sons, 1995.

[10] A. Menezes, P. van Oorschot, S. Vanstone *Handbook of Applied Cryptography* . CRC Press LLC, Boca Raton, 1996.

BIOGRAPHICAL SKETCH

Mahesh Kumar Patel

Mahesh Kumar Patel was born in Gujarat, India. He passed High School 12th grade from Our Own English High School (OOEHS) Dubai. He obtained his undergradute degree in Computer Engineering from Mumbai Unversity, India. He was the Joint Secretary of Computer Society of India (CSI), VESIT Chapter between 1995-96. After the completion of his Masters degree from Florida State University (FSU), he intends to pursue a doctoral degree at FSU.