Visual Cryptography – Study and Implementation

Divij Wadhawan, Hemank Lamba, Rajat Vikram Singh

Introduction

Nowadays, in the Internet, besides text, multimedia information is also quite prevalent. Therefore the security of these secret and confidential images is a valid concern. To answer these concerns, in 1994, Shamir and Naor proposed a new domain of cryptography, known as visual cryptography (1). Visual cryptography is a unique kind of cryptography which is used to encrypt printed texts, handwritten notes and pictures such that the decryption can be done only by the human visual system. This unique property of visual cryptography makes decryption process unattainable even with the help of a brute force attack, as it requires a constant human intervention to check whether the decoded image is valid or not.

Visual cryptography, derived from the basic theory of secret sharing, extends the same sharing scheme to images in such a way that no single share reveals information about the original image. It finds its applications in sharing multimedia information secrets over the network, in thresholding the access to a bank account for example out of 6 participants only *n* such that $2<=n<=6$ can combine the share of the key given to them and access the bank account.

In this report, section 2 covers the background required for visual secret sharing, section 3 and 4 covers the model and the solutions, whereas section 5,6 and 7 deal with the various extensions that have been made to the basic algorithm of visual cryptography and the domains to which it has been extended to. Section 8 covers the details of the implementation of the project. Section 9 deals with the results of the project and discusses the open research directions available in this domain.

Background

As explained earlier, the motivation of sharing the multimedia information comes from the text secret sharing. The normal secret sharing algorithm works in the following way. We have **secret** as an *n-bit* binary string, and we want to split this key into two shares in such a way that no single share reveals information about the secret. We define the two shares in the following way

- Share 1 is *n-bit* randomly generated string.
- Share 2 is Share 1 *XOR* secret.

Now shares can be simply recomputed by Share 1 *XOR* Share 2. Let's consider the following case as an example.

n= 5

Secret= 10100

Share 1= 01101

Share 2= 11001

But in this scheme, there was no thresholding proposed. So, Shamir proposed that k points are sufficient to define a polynomial of degree k-1 and hence, based on this fact, he came up with the threshold scheme (2). It states that if a key is divided into n pieces and no t-1 pieces can be combined to reveal information about the key but knowledge of any t pieces makes computation of the key easier, then such a scheme is called *(t, n) threshold scheme.*

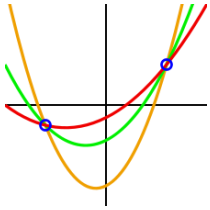


Fig 1: Shamir's Secret Sharing scheme Interpolation (3)

The Shamir's (t, w) threshold scheme works in the following manner

- Choose t-1 a_0, a_1, ...a_k coefficients in finite field F at random.
- Build the polynomial $f(x)=a_0+a_1x+a_2x^2+.....+ a_{k-1}x^{k-1}$
- Construct *n* points, in such a manner that (i,f(i)) is a point.
- We can recombine the secret by interpolation and the constant is the secret.

However, in images the algorithm for creating shares is a little different, but the threshold scheme is quite identical. The image is divided into n shares in such a manner that no t-1 shares can be combined (i.e superimposed on each other) to recompute the original image but any t images should give the original image back, when combined.

In addition to this, the visual cryptography model is advantageous in the following manners that it is simple to implement, no decryption algorithm is required and even infinite computing power can also not predict the message.

The Model

The simplest version of the visual cryptography model is on binary images where the message is nothing but a combination of black and white pixels, but advanced versions exists for gray scale images and color images, as well. From a cryptographic point of view, the user will be given a *key* which is one of the transparencies of the original image. Besides this, the *ciphertext* which is maintained by the validator is another transparency. The original *plaintext* image will be revealed by placing the key over the ciphertext.

This system is similar to *one-time pad scheme* and hence it is information –theoretically secure that is the encrypted message provides no information about the original message to a cryptanalyst. This gives another positive point of visual cryptography.

The important parameters for any (k,n) VCS are the following

- m - The number of subpixels into which each pixel is divided into. As m increases, it is expected that the resolution of the pixel is decreased.
- α - The relative difference is for the loss in contrast and hence should be as large as possible.
- k - The minimum shares required to recompute the image.
- n - The total number of shares into which image is going to be split into.

The original binary image is divided into *n* images for a n-share scheme, each image representing a share. Each share is again a collection of black and white subpixels. Number of subpixels per pixel is dependent on the *pixel expansion constant.* We can say that each pixel in the original image can be represented by a 2-D array of *n* x m. Now when the entire sets of shares are stacked over each other, then a valid solution to the scheme should follow the following two conditions

- For a white pixel, the hamming weight of "or"-ed m vector is < d – αm
- For a black pixel, the hamming weight of "or"-ed m vector is atleast d

Where d is some fixed threshold and α is the contrast relative difference, generally >0.

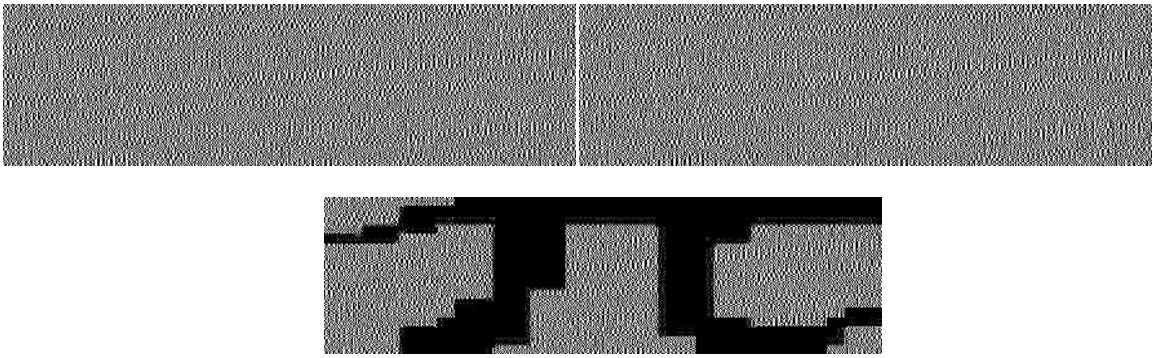


Fig 2: (L-R, Clockwise) Share 1 of (2,2) scheme, Share 2 of (2,2) Scheme and the recomputation.

According to (1), a solution to *k out of n* visual secret sharing scheme consists of two collections of *n x m* Boolean matrices in C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the permutations of the basic matrix in C_0 and if it is a black pixel, then from C_1. The solution will be called a valid one only if it meets the following three conditions

- For any S in C_0, the "or" of any k rows has a Hamming Weight which is less than or equal to d – αm
- For any S in C_1, the "or" of any k rows has a Hamming Weight which is of atleast d
- For any subset $\{i_1, i_2, ... i_q\}$ with q<k, the matrices hence obtained are indistinguishable and do not reveal any information about the original image.

The first two conditions are *contrast* as they make sure that the contrast for the decrypted image is identifiable by the human visual system. The third condition is called *security* because it makes sure that without the specified condition, no information about the original image can be revealed.

General Solutions

In the following section, we will be discussing two basic techniques as discussed by (1). The schemes that we will be discussing are as follows

- 2 out of N general scheme - This scheme means that if image is divided into N shares then atleast 2 shares are needed to recompute the image.
- 3 out of N general scheme – This scheme means that if image is divided into N shares then atleast 3 shares are needed to recompute the image.

Before discussing the two schemes, it is very vital to discuss about the basis matrices and the share distribution algorithm.

Basis Matrices – There are 2 matrices, which form the core of the visual cryptography scheme. One is to handle all the white pixels while the other is there to handle all the black pixels.

Share distribution Algorithm

In (1), the share distribution algorithm is defined as follows,

For each pixel, do the following

1. Generate a random permutation of the set – {1,2,3,....., m}
2. If P is a black pixel, then apply the permutation to columns of S^1.
3. Else if it is a white pixel, then apply the permutation to columns of S^0.
4. Now each row in the new matrix comprises the m sub pixels of the pixel P in the each share.

The above algorithm makes use of random permutations of the basis matrix. For each pixel a different permutation is used hence *confusion* is introduced. This *confusion* adds to the security of the algorithm.

2 out of N Visual Sharing Scheme

For a (2,n) VCS, the solution is obtained as follows for S^0 and S^1

- S^0 – It is the matrix which has all rows of column 1 set as 1 and all other cells as 0.
- S^1 – It is the identity matrix.

From these S^0 and S^1, the collection C^0 is obtained by all permutations of S^0 and C^1 is the collection of all permutations of S^1.

3 out of N Visual Sharing Scheme

For a (3,n) VCS, the solution is obtained by the following algorithm

- Generate a B matrix, which is of the dimension n x (n-2) containing only 1's
- Generate I as Identity matrix of n dimension
- Concatenate B and I to form the n x (2n-2) matrix
- C^0 – All matrices obtained by permuting c(BI)
- C^1- All matrices obtained by permuting BI

Other Extensions

There have been numerous extensions been proposed to the basic visual cryptography scheme as given by (1). We are keeping ourselves in scope of this report limited to the following

- Sharing multiple secrets
- Visual Cryptography for the coloured images

Sharing Multiple Secrets

The very first scheme designed to share multiple secrets was using circle shares (4). In this scheme, circular shares were used to hide two messages; each message can be decrypted by changing the angle of one of the circular shares.

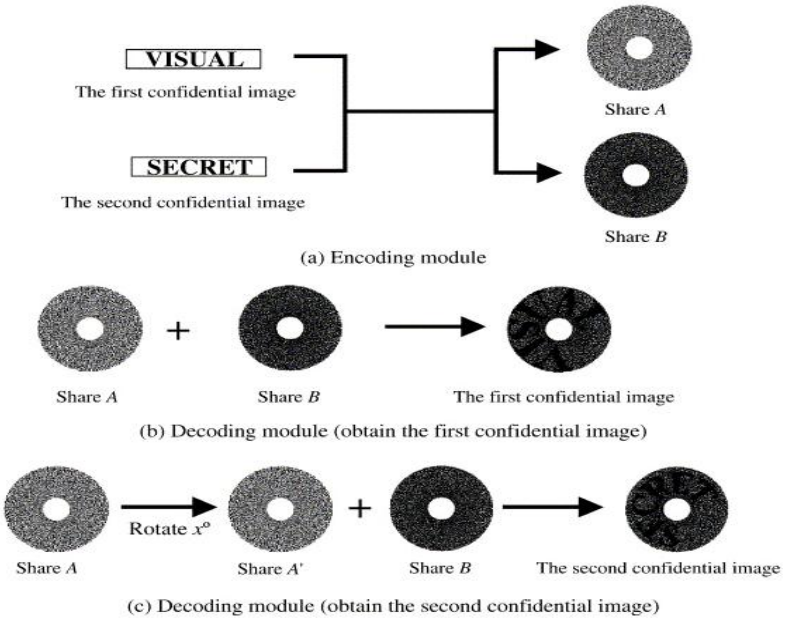


Fig 3: Multiple secrets sharing using circle sharing (5)

For a general (2,2) scheme, there are two shares created A and B. A can have the patterns shown in Fig 2 and B can have the patterns shown in Fig 3.

Fig 4: 4 possible patterns of A (5)

Fig 5: 4 possible patterns of B (5)

The secret 1 can be obtained by just overlapping the two circular shares whereas secret 2 can be obtained by overlapping share A rotated by some x degrees and share B without rotation.

Visual Cryptography for Colored Images

In (6), it was proposed for the very first time, the use of colored images in visual cryptography. The basic idea behind the colored image cryptography remained the same however. The paper proposed a *k out of n c- color* visual secret sharing system. It says that the matrix S is a collection of all collections of c-1 matrices.

$S = (C_0, C_1, \ldots\ldots\ldots\ldots, C_{c-1})$ where C is a collection of n x b q-ary matrix. To share a color i, randomly one matrix from C_i is chosen. The chosen matrix gives us the color of b *subp*ixels in each one of the shares.

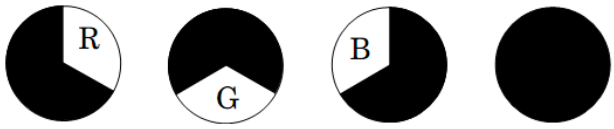


Fig 6: Representation of 3 colors

The image is visible only if all subpixels are of the same color, then the value of that pixel in the recomputed image is that color otherwise it is a mix color or black.

Project Results

In our project, we have implemented the visual cryptography scheme proposed by (1) for two basic solutions of '2 out of n' and '3 out of n' scheme.

The implementation has been done in C#. It as input can accept all binary image files. It does even accept color files and grayscale files but the program preprocesses the image and converts it to binary file.

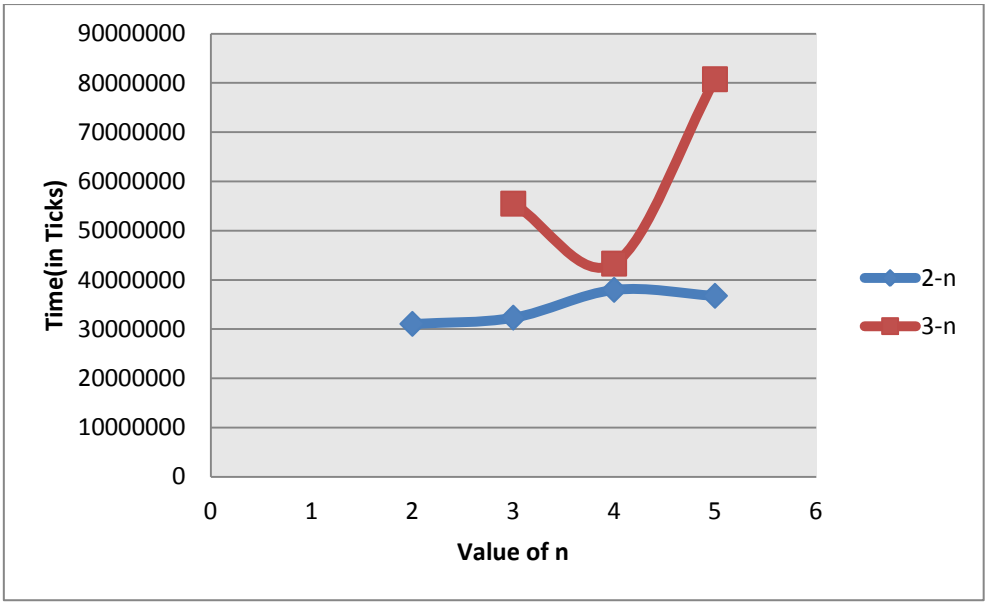
In our experiment, we tried to study the various threshold schemes along with the various parameters like the following

- Running Time
- Size of the image

Running Time – It is an important factor in any implementation. We observed the results shown in Table 1.

Min Shares	Total Shares	Running Time (in Ticks)
2	2	31061777
2	3	32331849
2	4	37972172
2	5	36762103
3	3	55483174
3	4	43302477
3	5	80754619

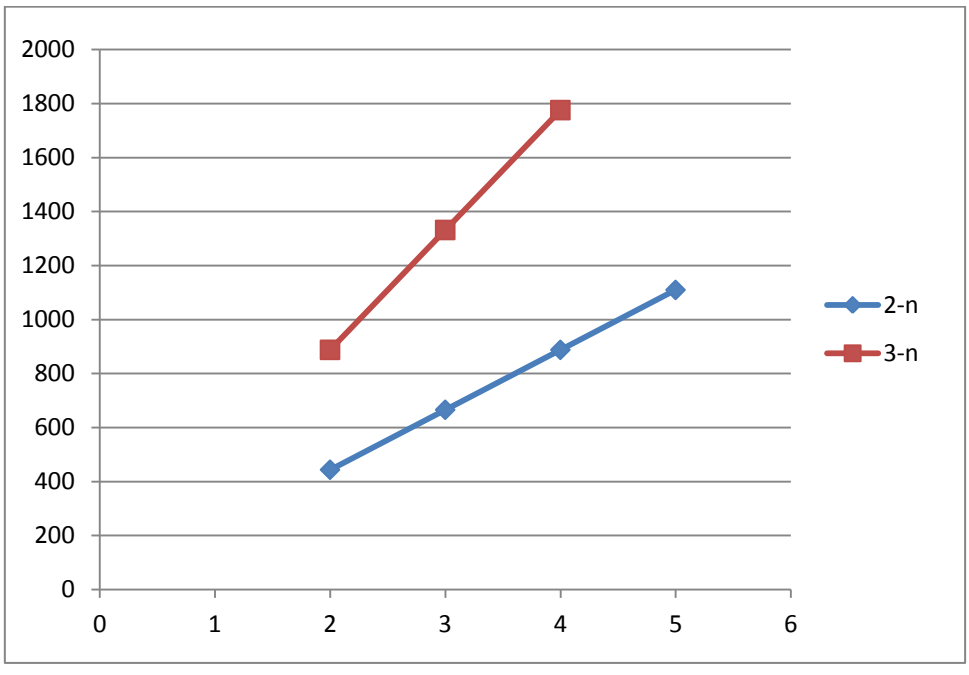
Table 1: Running Time of various threshold schemes



Graph 1: Computation Time for various threshold schemes

Image Size

Another important factor in visual cryptography schemes is image size and it plays a lot of role in the output image. Usually the output image gets enlarged in the width. Some work has been done in trying to restore the size of the image back to the original size without any loss in the resolution. A very increased size and hence a lesser resolution means that the human visual decryption system can even fail to identify the written text.



Graph 2: Image size vs number of shares graph

Future Work

A lot of work has already been done in the field of visual cryptography and technically the technique is sound enough and cryptanalysis is not so easy to do. Though seeing the immense vastness of the visual cryptography, it has not been implemented on a large scale. For example, these days top companies are using biometric sensors to take attendance. But, what they are mising is that most of low scale industries cannot afford the nusiances of a biometric sensor. Hence, using visual cryptography, a low cost solution can be established where multiple secrets are shared between users and the authenticator.

Besides this, a potential work lies in making visual cryptography size invariant, as increasing size of the output images lower the resolution of the images and hence making tougher for humans to decrypt them.

Bibliography

1. *Visual Cryptography.* **M. Naor, A.Shamir.** 1994. Eurocrypt 94.

2. *How to share a secret.* **Shamir, A.** s.l. : Communications of ACM Volume 22 Issue 11, Nov. 1979.

3. *http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing.* [Online]

4. *Sharing visual multi-secrets using circle shares.* **Hsien-Chu Wu, Chin-Chen Chang.** 2005.

5. **Shyong Jian Shyua, Shih-Yu Huanga,Yeuan-Kuen Leea, Ran-ZanWangb, Kun Chena.** http://www.ee.cgu.edu.tw/combrief/20071016/25E6/A1_Sharing_multiple_secrets/invisuacryptography/. [Online]

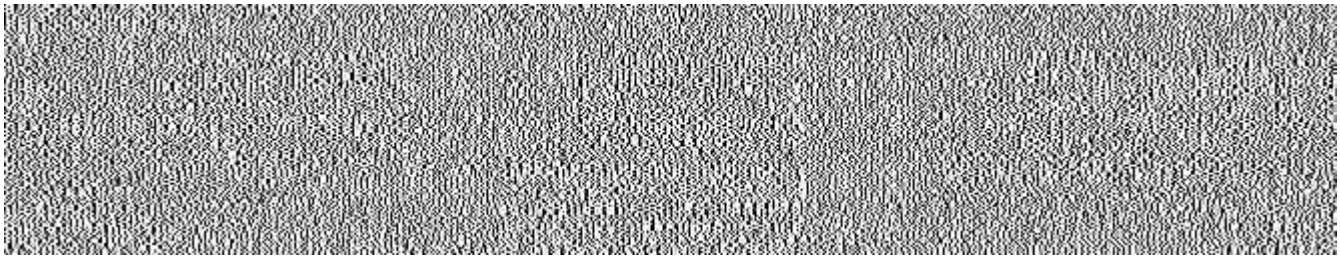
6. *Constructions and Properties of k out of n Visual Secret Sharing Schemes.* **Eric R. Verheul, Henk C. A. Van Tilborg.** s.l. : Journal Designs, Codes and Cryptography, 1997.

APPENDIX-I

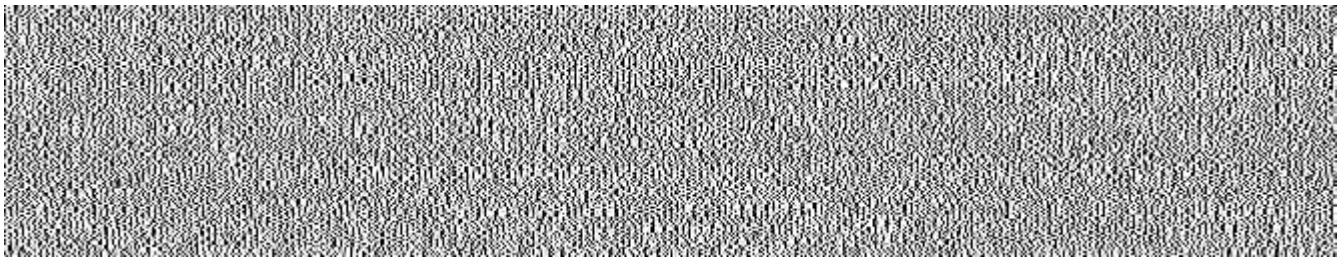
The secret and the corresponding shares generated by our implementation:-

Secret:

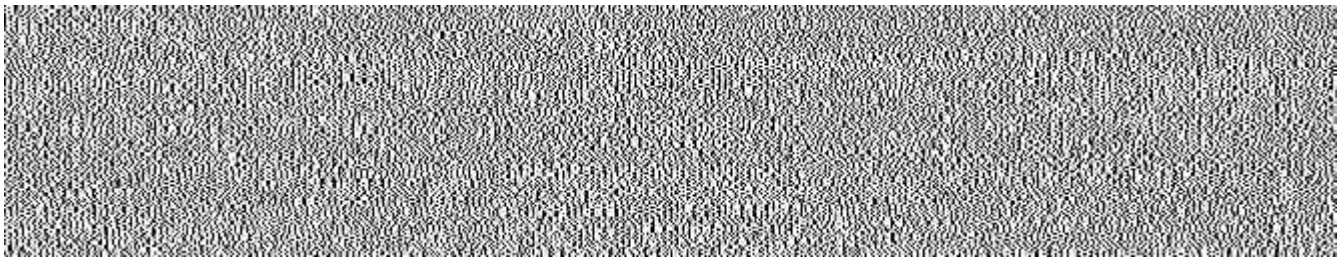
Share 1 (2-out of-3 scheme):



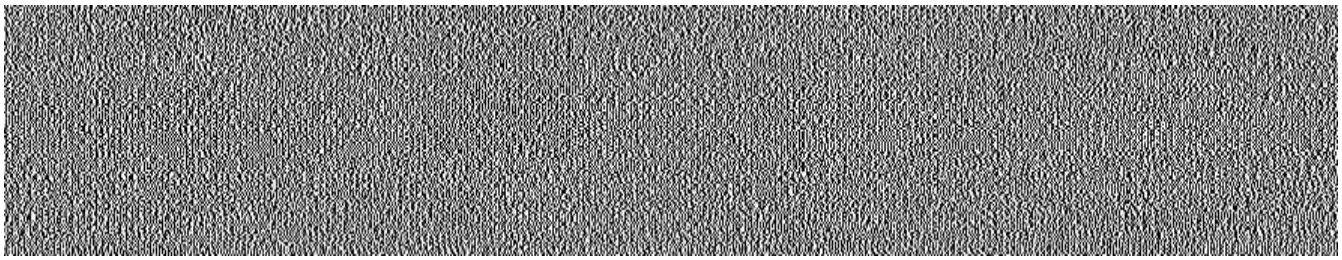
Share 2 (2-out of-3 scheme):



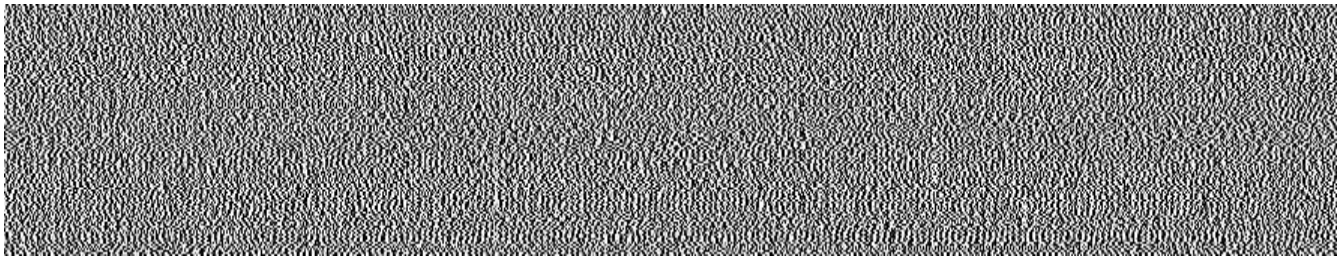
Share 3 (2-out of-3 scheme):



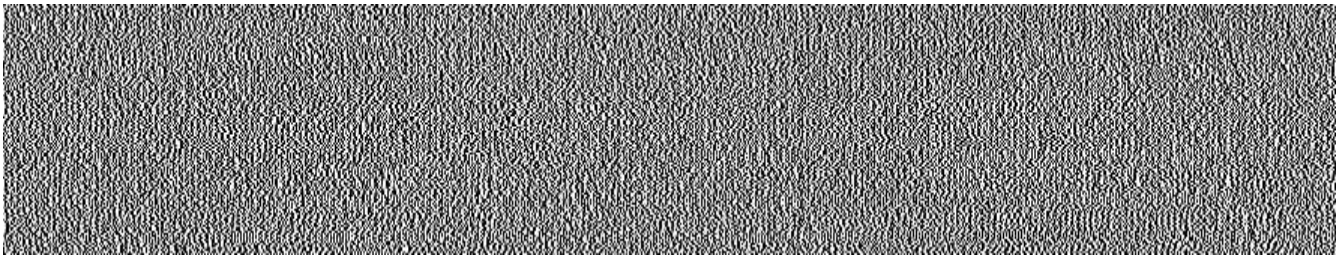
Share 1(3-out of-3 scheme):



Share 2(3-out of-3 scheme):

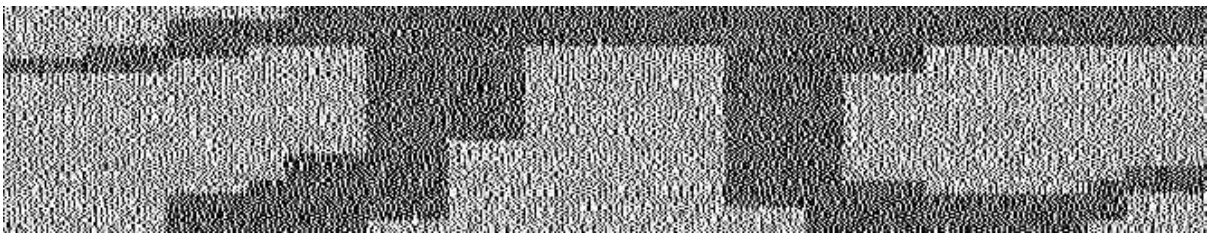


Share 3(3-out of-3 scheme):

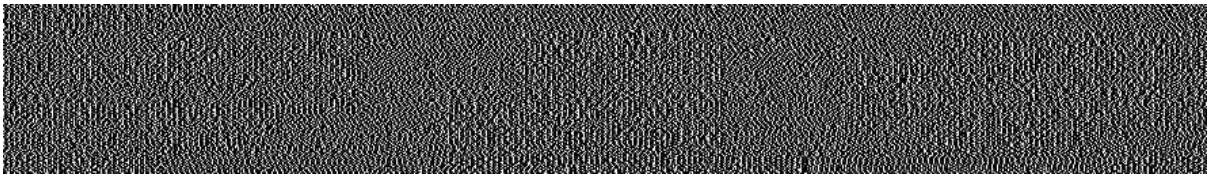


Recomputed Images:

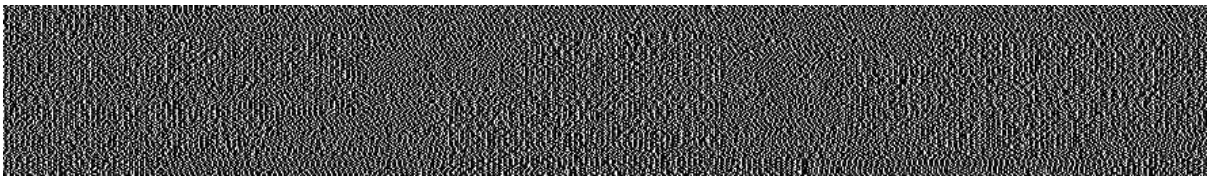
Share 1 + Share 2 (2-out of-3):



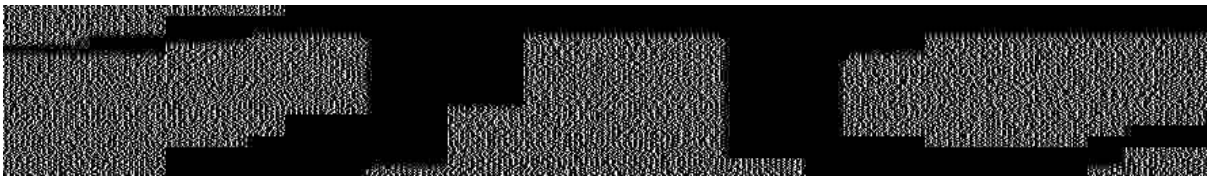
Share 1 + Share 2 (3-out of-3):



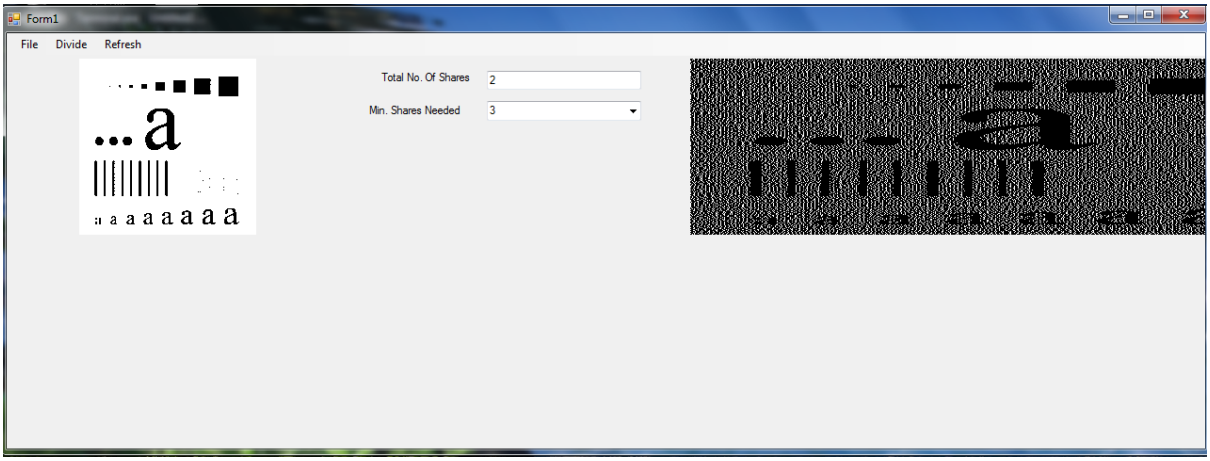
Share 1 + Share 2 (3-out of-3):



Share 1 + Share 2 + Share 3 (3-out of-3):



Screenshot of the Software:


Form1
File
Divide
Refresh
Total No. Of Shares
2
Min. Shares Needed
3