International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)) Volume 4, Issue 7, July 2015)

Improvement in Performance of Visual Cryptography by Dividing in Matrix

Navdeep[1], Jitender Yadav[2]

[1]*Mtech Student, Department of Computer Science and Application, RPS College, Mahendergarh, Haryana, India*

[2]*Assistant Professor, Department of Computer Science and Application, RPS College, Mahendergarh, Haryana, India*

[1]navdeepsourav@gmail.com, [2]jitu820@gmail.com

***Abstract*-- Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption. On a similar front like this, we have Visual Cryptography which deals with the protection and hiding of information which is based on the videos.**

***Keyword*-- Encryption, Visual cryptography,**

I. Introduction

Visual Cryptography deals with the encryption and decryption of the videos to protect the information related to them. The encryption requires certain levels of computation to divide the original video into several shares. This is done keeping in mind the fact that the resultant shares show no resemblance to the original video. As a new type of the technique of Visual Cryptography, the shares are so manipulated that by looking at them one may extract some other information alone which would not be correct. Such a technique results into the formation of the innocent shares. After the formation of the shares, they are simply overlapped or better stated in terms of video processing are simply "and-ed" to get the original video back.

We can implement the Visual Cryptography by using one of following access structure schemes

- (2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret video and encrypts it into two different shares that reveal the secret video when they are overlaid. No additional information is required to create this kind of access structure.
- (2, n) – Threshold VCS: This scheme encrypts the secret video into n shares such that when any two (or more) of the shares are overlaid the secret video is revealed. The user will be prompted for n, the number of participants.
- (n, n) – Threshold VCS: This scheme encrypts the secret video into n shares such that only when all n of the shares are combined will the secret video be revealed. The user will be prompted for n, the number of participants.
- (k, n) – Threshold VCS: This scheme encrypts the secret video into n shares such that when any group of at least k shares are overlaid the secret video will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

With the increase in digital media, the need for methods to protect such information is becoming more necessary. The source of digital media's growth can be linked to the wealth of information provided by the Internet. The amount of information that is downloaded and uploaded increases on a daily basis, with data ranging from simple text documents to photos of individuals to hyper spectral image cubes of the world. The Internet provides an ease of access that demands knowledge of the best way to protect the visual information available on the Internet from theft, replication, or unauthorized use.

The field of Visual Cryptography has been developed over the last several years. The original method was proposed by Naor and Shamir [1] for binary images. This provides a perfectly secure system where secret messages are contained in \shares". Individually these shares resemble random noise, but when they are stacked and aligned perfectly, their message is decrypted using only the human visual system. While this method gives security for text and binary images, the growth of digital media requires the expansion of this technique to provide security for gray and color images. Several methods have been developed for securing gray and color images, including half toning [2], dithering [3], color sub pixel groupings [4], and meaningful image shares [5, 6]. Through this expansion of the original method, Visual Cryptography provides a secure way to store and transmit text, binary images, gray images, and color images.

Since the original method was released in 1994, there have been an abundance of variations, modifications, and improvements added to the collection of available Visual Cryptography techniques. As the number of published methods increase, a technique for evaluating the effectiveness, quality, and ideal use of each of the algorithms is necessary. Currently, this information can be determined by reading through the paper, evaluating its contents, and determining if it is a suitable method for a given project. While it is possible to perform this process on several algorithms before deciding on the final method to be used, it would be beneficial for a set of standards and performance metrics to be available for use in determining the ideal Visual Cryptography method for a specified project. The development of a proper benchmarking scheme would allow these standards and performance metrics to exist in one uniform format. The contents of this benchmarking scheme would contain information regarding the capabilities of the algorithms. It would determine the primary approach and methodology used to generate the image shares. Also, it would provide external implementation and validation of the code presented to execute the algorithm. Additionally, it would provide information on image reconstruction, overall quality of reconstructed images, and a ranking (or grade) of the algorithm compared to a given Visual Cryptography standard.

Ideally, the benchmarking scheme would result in a report card that could be read to determine whether or not the algorithm would be a suitable method for a given project. These report cards could either be required when publishing a new algorithm or published on the Internet for easy access and search. The development of this benchmarking scheme would allow easy access to the information available from published Visual Cryptography algorithms and provide a standard metric for evaluating their capabilities and performance.

II. Motivation

The easiness to access the data in today's arena has propelled the need of authority to access the data. The measures which are currently in practice for encryption of data is not meant for the novice users as it involves a lot of computation. There have been many attempts to reduce this complexity. One such attempt is visual cryptography. We took this topic as our project because the actual process of decryption doesn't involve any computation and hence it is easy for anyone to use. Also our interest in video processing motivated us to undertake a project based on the same field.

III. Problem Description

Our project aims at implementing the various schemes of Visual Cryptography as formulated originally by Moni Naor and Adi Shamir in 1994. We have successfully implemented the two schemes of the Visual Cryptography. In both the schemes we have a grey scale video which is further divided into various numbers of shares depending upon the scheme being followed. Formation of shares is a part of encryption process, where in the resulting shares do not show any resemblance to the original video.

After the shares have been formed the number of shares to be selected to obtain the original video back, depends on the type of scheme which is being used to encrypt the videos. The selected shares are just overlapped with each other and then we get the original video back. The simple overlapping is done because of the reason that the Visual Cryptography doesn't involve any computation in the decryption process. It is the human eyes which simply does the decryption and hence the simple overlapping of the shares to produce the original video.

IV. Design Of The Project

1. For (2, 2) – Extended Visual Cryptography

The main concept behind the visual cryptography is that the original video is divided into 2 identical meaningless shares printed on transparencies. When these two shares are superimposed (recombined) then they yield the original video back.

The VSS can be described by a 2X2 Boolean matrix s[i, j] = 1 if the jth sub pixel in the ith share is black otherwise s[i, j] = 0.

S_0 = 10 or 01
10 01

Represents the matrix for white pixel while

S_1 = 10 or 01
01 10

Represents the matrix for black pixel

After defining the substitutes in the new shares for the pixel value, we read the individual pixel value and then randomly select any one of the matrix from s_0 for white and from s_1 for black respectively. The new matrices for the shares are thus formed. When displayed we can easily notice that the new shares show no resemblance to the original video.

This was the method to implement 2 shares. But in case we want 2 innocent shares (Extended Visual Cryptography) we make a few changes:

1) At every alternate pixel of 1st share add alternate pixels of an innocent video.
2) At every alternate pixel of 2nd share add alternate pixels of negative of innocent video.

We do this, since when we combine an video with its negative we get all black pixels.

For the gray scale videos we can achieve the same feat by first converting the video in to black and white and then following the same procedure.

We can also use some alternative methods and logic to obtain these two shares but the only thing to be kept in mind is that the shares should conceal the information of the original video.

After obtaining the shares we can simply superimpose them to get the same video back.

1. For (n, n) Visual Cryptography

The main concept here is that the original video is divided into n meaningless shares printed on transparencies. When all these n shares are superimposed (recombined) then they yield the original video back.

To create basis matrix (n x m) for (n, n) we have, m(pixel expansion)=2^(n-1).

Consider a set of n elements. Make 2 lists, one with all subsets of even cardinality, other with subsets of odd cardinality.

The list with subsets of odd cardinality is used to make a basis matrix C1 for white pixels and the other list to make a basis matrix C0 for black pixels.

C1 (i, j) =1 at all locations signified by odd cardinality subsets

C0 (i, j) =1 at all locations signified by even cardinality subsets

Example for creating basis matrix for (4,4):
C1-e1, e2, e3, e4, e1e2e3, e1e2e4, e1e3e4, e2e3e4
C0-Null, e1e2, e1e3, e1e4, e2e3, e2e4, e3e4, e1e2e3e4

C1

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

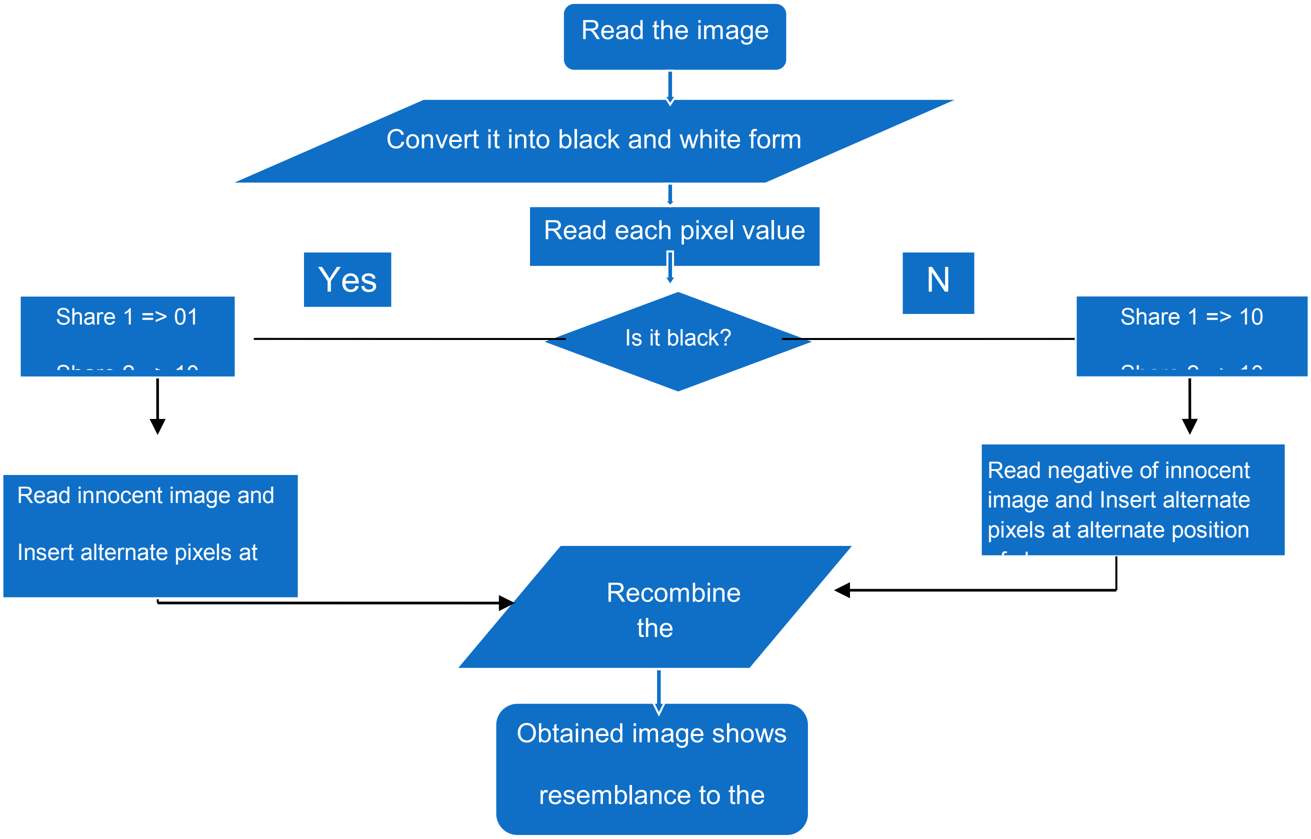
C0

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

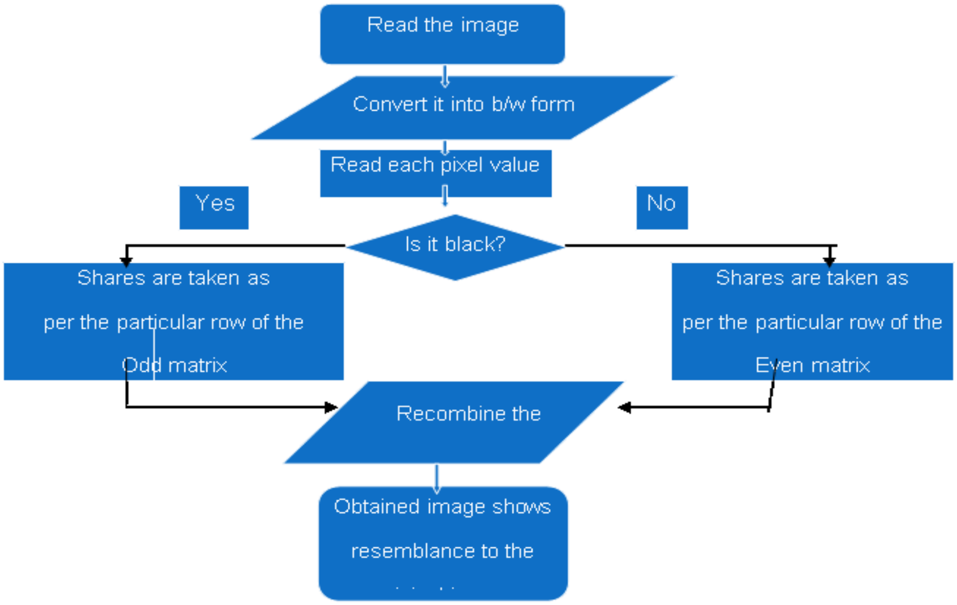
After defining the substitutes in the new shares for the pixel value, we read the individual pixel value and then randomly select any one of the matrix from C0 for black and from C1 for white respectively. The new matrices for the shares are thus formed. When displayed we can easily notice that the new shares show no resemblance to the original video.

V. FLOWCHART

1. For (2, 2) Extended Visual Cryptography



2. For (n, n) visual cryptography scheme



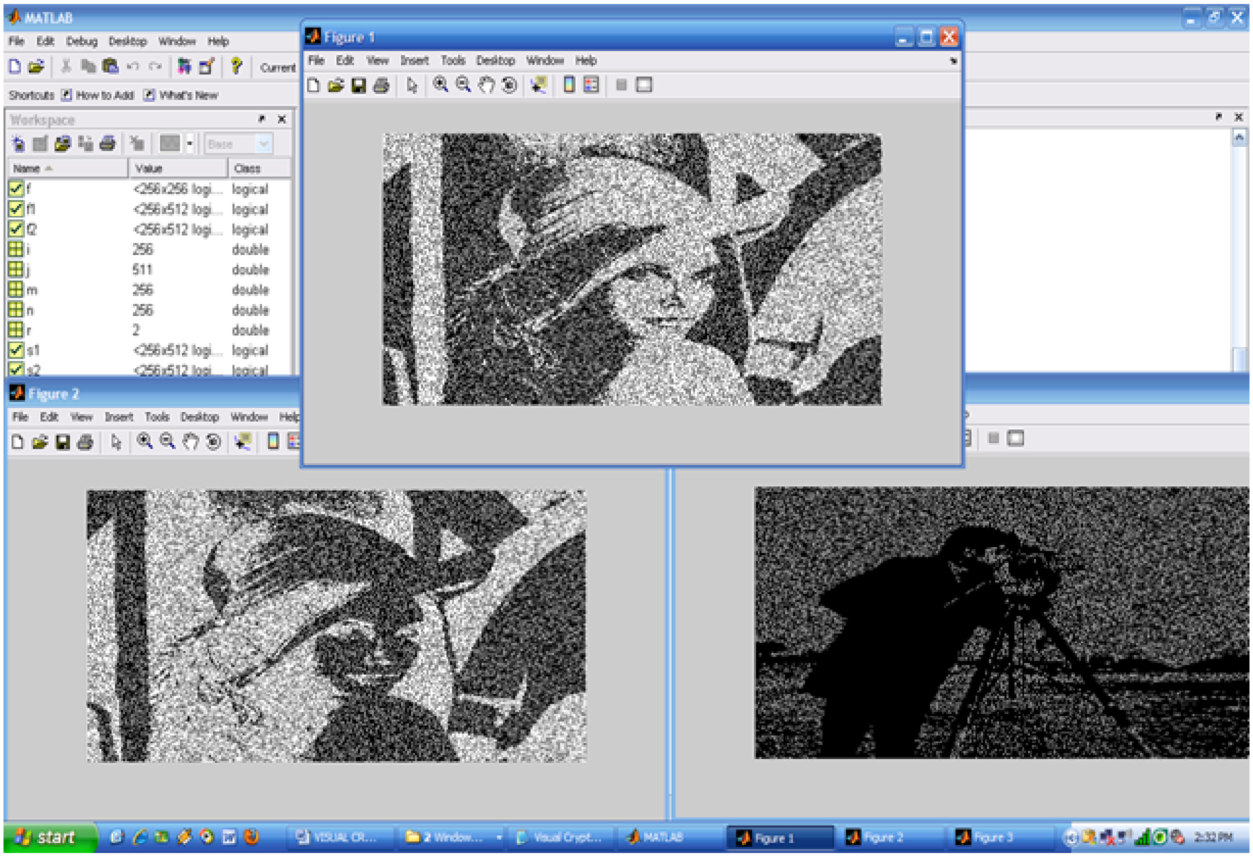
VI. RESULTS

1. Algorithm For (2, n) scheme

1) Read the original Video which is the secret and convert it to black and white
2) Read an innocent Video and its negative and resize it equal to the size of shares
3) Initialize 2 matrices s1, s2 representing the 2 shares, to zero
4) Define 2 basis matrices:
   C0 for black and C1 for white

C0:	C1:
0 1	1 0
10	1 0

5) Read each pixel of original video
6) If pixel is black:
   Replace corresponding pixel in s1 and s2 by C0 or column permutation of C0
   If pixel is white:
   Replace corresponding pixel in s1 and s2 by C1 or column permutation of C1
7) Now replace alternate pixels of s1 (s2) by alternate pixels of innocent video (negative) to get the final innocent shares.
8) To get back the original secret video, print the shares on transparencies and stack them together.


MATLAB
File Edit Debug Desktop Window Help
Current
Shortcuts How to Add What's New
Workspace
Base
Figure 1
File Edit View Insert Tools Desktop Window Help
Figure 2
File Edit View Insert Tools Desktop Window Help
start
VISUAL CR...
2 Window...
Visual Crypt...
MATLAB
Figure 1
Figure 2
Figure 3
2:32 PM

Name	Value	Class
f	<256x256 logi...	logical
f1	<256x512 logi...	logical
f2	<256x512 logi...	logical
i	256	double
j	511	double
m	256	double
n	256	double
r	2	double
s1	<256x512 logi...	logical
s2	<256x512 logi...	logical

Fig 1 Snapshot for the (2, 2) extended visual cryptography

2. Algorithm For (n, n) scheme

1) n - number of shares that we have to generate (namely S1,S2,S3,S4....Sk.....S(n-1), Sn)

2) Generate two groups:-

a) One containing all the even clusters of the shares taken together viz:-

[0 occurrence], [any 2 occurrence of the shares viz S1S2, S2S3 etc.]…

So on till n or n-1 which would depend on the fact whether n is an even number or an odd number.

b) Other containing all th odd clusters of the shares taken together viz:-

[Just 1 occurrence of the shares viz S1, S2..., Sn], [any 3 occurrence of the shares viz S1S2S3, S2S3S4 etc]…

so on till n or n-1 which would depend on the fact whether n is an even number or an odd number

3) Now generate the matrices to be used in place of white and black pixels. white matrix would contain the corresponding odd clusters while black matrix would contain the even clusters.

4) Significance of the rows and columns of the matrices:-

Rows => this signifies the total number of shares and their respective white/black pixel replacement

Columns => this signifies the total pixel expansion

5) General structure of the matrix:

Number of rows = total number of the shares

Number of columns = total number of the different members in the clusters

	entry1	entry2	entry3.....	Entry (k)
S1	0/1	same	same	.....
S2	0/1	same	same	.....
S3	0/1	.		
S4	0/1	.		
Sn	. .			

where k = 2^(n-1)

6) Entering the values in the matrices [ME,MO where ME=> even matrix and MO=> odd matrix]:-

a) Choose a cluster

b) Choose a particular entry/group from cluster

c) M (i, j) = 1 if and only if

The element of the cluster contains the i^{th} element in it. e.g for S1S2S3 the S1th , S2th and S3rd row would bear the value 1 and rest all rows would contain 0

d) Above step is repeated till all such clusters are exhausted.

e) The above steps are same for forming the even and odd matrices respectively.

7) The pixel expansion is always done in the way to satisfy the symmetrical structure of the video. Here we get the two cases:-

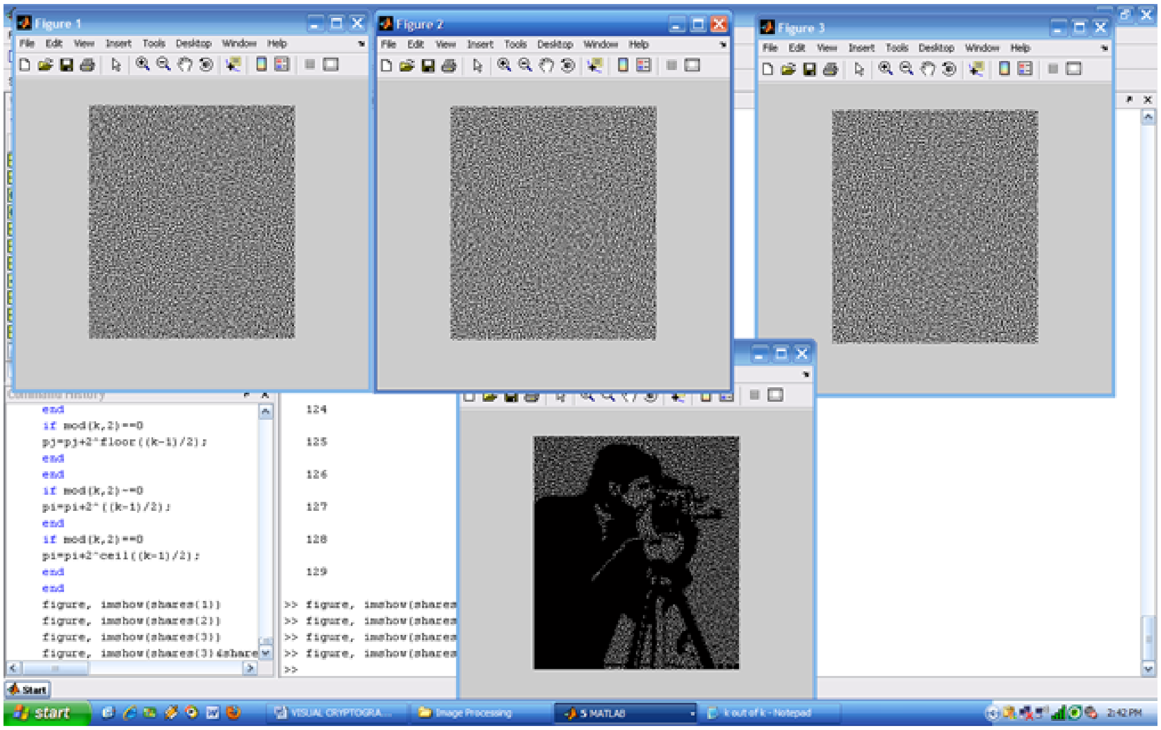
a) If the n (no of shares is odd) then 2^(n-1) would be a perfect square and hence each pixel(of the original video) is replaced by a square matrix of order sqrt (n-1)

b) If the n (no of shares is even) then we try and achieve the order (2^m) x (2^n)

Where m = ceiling of n-1/2

n = floor of n-1/2

8) After generation of the matrix, the black and white pixels in the original video are replaced by the permutated columns of the subsequent matrices and hence we get the shares.



```
Command History
    end
    if mod(k,2)==0
    pj=pj+2^floor((k-1)/2);
    end
    end
    if mod(k,2)~=0
    pi=pi+2^((k-1)/2);
    end
    if mod(k,2)==0
    pi=pi+2^ceil((k-1)/2);
    end
    end
    figure, imshow(shares(1))
    figure, imshow(shares(2))
    figure, imshow(shares(3))
    figure, imshow(shares(3)&share
```

```
   124

   125

   126

   127

   128

   129

>> figure, imshow(shares
>> figure, imshow(shares
>> figure, imshow(shares
>> figure, imshow(shares
>>
```

Fig 2 Snapshot for n, n Visual Cryptography Scheme

VII. Conclusion

We have successfully demonstrated the techniques of Visual cryptography for videos and videos. The implementation of the 2 schemes namely (2, 2) and (n, n) has been successfully implemented. For both the schemes we have created the shares showing no resemblance to the original video and the main criteria of the Visual cryptography is satisfied as there has been no manipulation on the decryption phase which is evident in the code.

In the (n, n) scheme of Visual cryptography we have clearly shown that on super imposing less than n shares doesn't correspond to the original video, which is the essential security criteria for the concerned scheme.

Through the rigorous implementation of the (n, n) scheme we have also concluded that in Matlab the best results are obtained for n<=5. On increasing the value of n further we face the problem of exhausting the space constraint and hence the result becomes unreadable.

Hence we can conclude that the aim and objective of the project is achieved.

REFERENCES

[1] Moni Naor and Adi Shamir "Visual cryptography" EUROCRYPT, pages 1{12, 1994.

[2] Luiz Velho and Jonas de Miranda Gomes "Digital halftoning with space lling curves" Computer Graphics, 25(4):81{90, July 1991.

[3] Chang-Chou Lin andWen-Hsiang Tsai "Visual cryptography for gray-level images by dithering techniques" Pattern Recognition Letters, 24:349{358, 2003..

[4] Young-Chang Hou "Visual cryptography for color images" Pattern Recognition, 36:1619{1629, August 2002.

[5] Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, and Chwei-Shyong Tsai "A novel authenticable color visual secret sharing scheme using non-expanded meaningful shares" Displays, 32:118{134, February 2011.

[6] C-C Chang, W-L Tai, and C-C Lin. Hiding a secret colour image in two colour images. The Imaging Science Journal, 53:229{240, May 2005.