Visual Cryptography (VC) using Zigzag Scan Approach

Soumya.S.Hegde, Bhaskara Rao.N
Department of Computer Science and Engineering,
Visveswaraiah Technological University,
Dayananda Sagar College of Engineering, Bangalore, India

***Abstract*— This paper proposes a new method of Visual Secret Sharing using Zigzag Scan approach. Non-expanded shares are generated by this scheme. This overcomes the drawback of Hilbert Curve approach, that is, the input should be a square image of size which is an integral power of 2.**

***Index Terms*—Visual Cryptography, Visual Secret Sharing, Zigzag Scan.**

I. INTRODUCTION

Visual Cryptography is a technique of encrypting a secret image into two or more shares [1]. The technique was proposed by Naor and Shamir in 1994. In the conventional Visual Cryptographic scheme [1], the shares are expanded in size when compared to the secret image size. This increases the space required to store and higher bandwidth to transmit the shares. The proposed method overcomes this by using non-expanded shares. Another advantage of this method is that the secret images need not be squares having integral powers of 2 as their sizes. Therefore the proposed scheme overcomes the drawback of Hilbert Curve approach [2]. The rest of the paper is organized as follows: section 2 introduces the proposed method for Visual cryptography using Zigzag Scan approach. Section 3 gives the experimental results to show the effectiveness of this scheme and this paper is finalized in section 4.

II. PROPOSED METHOD

The encoding consists of two phases: Zigzag scanning, to convert the 2D image matrix into a 1−D vector and share generation. The decoding also consists of two phases: secret image recovery and Inverse zigzag scanning to convert 1−D vector to 2D image matrix.

A. Two-out-of-two Visual Secret Sharing scheme

1) Encoding: The Encoding consists of two algorithms: 1. Zigzag Scanning Algorithm and 2.Share generation algorithm. The input to the Zigzag scanning algorithm is the 2−Dimensional secret image matrix A, of size m x n and the output is 1−Dimensional vector L, of size 1 x m*n. The elements of A are 0's and 1's with 0 representing the black pixel and 1 the white pixel. Zigzag Scanning is applied over the secret image to convert the 2D image matrix of size m x n to 1D vector of size 1 x m*n. The zigzag scanning algorithm [3] is a well known standard algorithm of converting 2D image matrix to 1D vector. By using Zigzag scanning, adjacency connectivity among the original image pixels are destroyed. The neighboring pixels in the 2D image are widely separated and dispersed in the 1D data. This will prevent partial patterns of the image from sneaking into the shares.

The diagram in the Fig.1 depicts the Zigzag scanning:

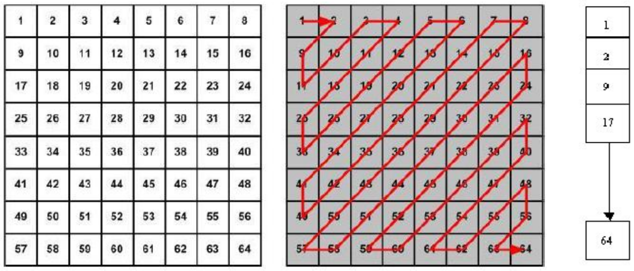


Fig.1a Fig.1b Fig.1c

Fig.1 Zigzag Scanning

The output of zigzag scanning results in a 1−D vector as shown in Fig.1c.

Next is the Share generation algorithm. The input to this algorithm is a 1−D vector which is the output of Zigzag scanning algorithm. The outputs of Share generation algorithm are two non-expanded 1−D shares. In our proposed method, the expansion of shares is avoided. Initially, black pixels and white pixels are separated in two different arrays. A group of four white pixels are replaced by corresponding four pixels from first or second row of **C** in share 1.The same four pixels are copied to share 2.Matrix **C** is as given below:

$$\mathbf{C} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

For black pixel processing, group of four black pixels are replaced by first or second row of **C** in share 1 and the complement of these four pixels are copied to share 2. Hence, four secret image pixels are replaced by four pixels from **C**, making the shares non-expanded.

Figure 2 shows the generation of two shares. Share generation for a sequence of four white pixels is shown in Fig.2a and for black pixels share generation is shown in Fig.2

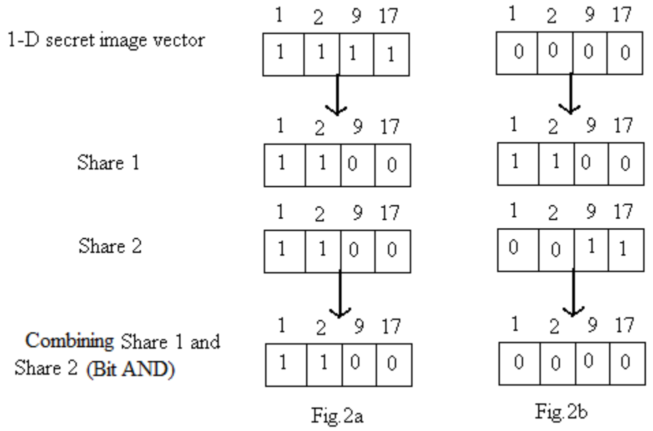


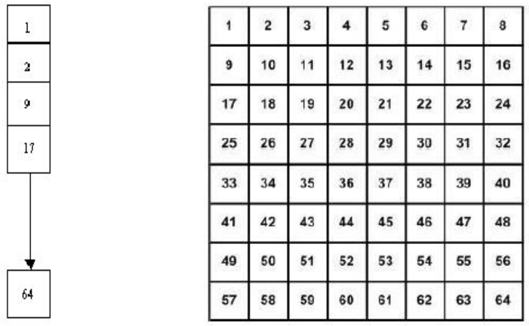
Fig.2 Share generation in 2-out-of-2 VSS scheme

Four pixels from any row (1^{st} or 2^{nd} row) of C are randomly chosen to eliminate the pattern effect (that is contiguous black or white pixels do not appear as patterns in shares).

2) Decoding: The decoding also consists of two algorithms: 1. Secret image recovery algorithm 2.Inverse Zigzag algorithm.

Secret image recovery algorithm takes two inputs, share1 and share2 (1−D shares). This algorithm performs bitwise OR-operation on the two 1−D shares, yielding a 1−D recovered secret image.

Next is the Inverse zigzag algorithm, which takes 1−D recovered secret image as the input. The output is a 2−D recovered secret image. Inverse Zigzag algorithm is as depicted in the Fig.3.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Fig.3a Fig.3b

Fig.3 Inverse Zigzag scanning

Fig.3a shows the 1−D input and Fig.3b shows the 2−D image matrix which is the output of the Inverse Zigzag algorithm.

Algorithm 1 and Algorithm 2 depict the SHARE GENERATION algorithm and SECRET IMAGE RECOVERY algorithm respectively.

Algorithm 1: *Share generation*

Given the input to the algorithm is a 2−D image matrix A of size M*N, which is later converted to 1−D image vector L of size 1 x M*N by applying Zigzag scanning. The algorithm generates two non-expanded 1−D shares.

```
procedure SHARE GENERATION (A)
1. Find the positions (indices) of white pixels in L. This is
done as follows:
  yw=find(L==1)
  where L=Zigzag(A).
  yw contains the indices of white pixels in L.
2. Find the positions (indices) of black pixels in L. This is
done as follows:
  yb=find(L==0)
  yb contains the indices of black pixels in L.
3. Get lw=length(yw)
4. Initialize S1 and S2 with zeros as follows:
  S1=zeros(1,M*N)
  S2=zeros(1,M*N)
  where [M N]=size(A),A is secret image
5.Process white pixels as follows:
  for i=1 to (lw/4) do
     Set p=C(1,:) or p=C(2,: ).ie. set p to either first row or
     second row of C.
     Where C=[1 1 0 0
              0 0 1 1]

     Generate 1−D shares, S1 and S2 as follows:
     for j=1:4
  if 4*i-(4-j)<=lw
  S1(yw(4*i-(4-j)))=p(j);
  S2(yw(4*i-(4-j)))=p(j);
  end if
  end for
  end for
  The conditions i=1 to (lw/4) and 4*i-(4-j)<=lw are used to
prevent the overflow at the extreme end(while processing the
last block) and to prevent from exceeding the matrix
dimensions.
6. Get lb=length(yb)
7. Process black pixels as follows:
   for i=1 to lb/4
  Set p1=C(1,:) or p1=C(2,: )i.e., set p1 to either first or
  second row of C randomly.
  Set p2=~p1 (i.e., compliment of p1).
  Continue generating 1-D shares, S1and S2 as follows:
  for j=1:4
  if 4*i-(4-j)<=lb
  S1(yb(4*i-(4-j)))=p1(j);
  S2(yb(4*i-(4-j)))=p2(j);
  end if
  end for
  end for
  end procedure
```

The outputs of Share generation algorithm are two 1−D shares (*S1* and *S2*) which are of same size as that of 1−D secret image.

Algorithm 2: *Secret Image Recovery*

Given the inputs to the algorithm are two 1−D image vectors *S1*(share 1) and *S2*(share 2) of size 1 x m*n. The algorithm generates non-expanded 1−D recovered secret image vector, *R* of size 1 x m*n.

```
procedure SECRET IMAGE RECOVERY(S1,S2)

    1. Perform bitwise OR operation on the two 1−D shares, S1
    and S2 as follows:
    $R = S1 \oplus S2$
    Where R is the recovered 1−D secret image.
```

This output (R) is taken as the input to the Inverse Zigzag algorithm. Inverse Zigzag algorithm converts the 1−D secret image vector to 2−D secret image matrix.

B. Two-out-of-three Visual Secret Sharing scheme

The 2-out-of-3 VSS scheme has following characteristics:

1. Secret image is concealed in three shares.
2. At least two shares are needed to recover the secret(2 or more shares).
3. The matrix C is of size 3 X 6.

C=[1 1 0 0 0 0
0 0 1 1 0 0
0 0 0 0 1 1]

Figure 4 shows the share generation. Fig.4a and Fig.4b show the use of all three shares to decrypt the secret. Fig.4c and Fig.4d show the use of only two shares to recover the secret.

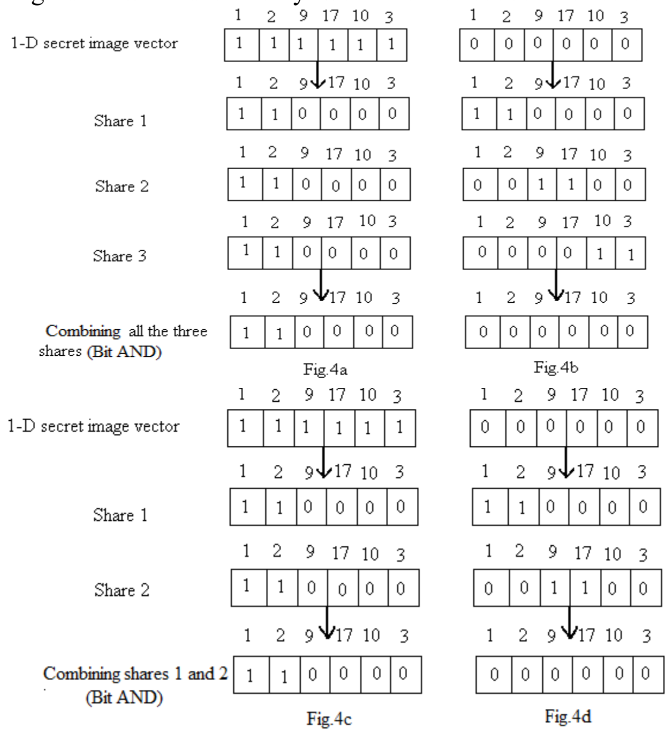


Fig.4a

Fig.4b

Fig.4c

Fig.4d

Fig.4 Share generation in 2-out-of-3 VSS scheme

In Figure 4, group of six white or black pixels from the 1−D image vector are replaced by six pixels from any row of matrix C, in each share. Fig.4a and Fig.4c show the white pixel processing. Fig.4b and Fig.4d show the black pixel processing.

For a group of six black pixels, six pixels from 1st row of C are selected in Share 1.These six pixels are circularly right shifted by two positions and then assigned for Share 2. The same six pixels are circularly right shifted by four positions and are assigned to Share 3. By overlapping all the three shares, the resultant value obtained is black. As shown in the Figure 4, white pixels remain 50% white and black pixels remain 100% black.

The modified Share generation algorithm and Secret image recovery algorithm for 2-out-of-3 are given below:

Algorithm 3: *Share generation*

Given the input to the algorithm is 2−D image vector A of size m x n, which is later converted to 1−D image vector L of size 1 x m*n, by Zigzag scanning.. The algorithm generates three non-expanded 1−D shares.

```
procedure SHARE GENERATION (A)

1. Find the positions (indices) of white pixels in L. This is
done as follows:
   yw=find(L==1)
  where L=Zigzag(A).
2. Find the positions (indices) of black pixels in L. This is
done as follows:
yb=find(L==0)
3. Get lw=length(yw)
4. Initialize S1 and S2 with zeros as follows:
   S1=zeros(1,M*N)
   S2=zeros(1,M*N)
   S3=zeros(1,M*N)

   where [M N]=size(A),A is secret image

5.Process white pixels as follows:
   for i=1 to (lw/6) do
      Set p=C(1,:) or p=C(2,:  ) or p=C(3,: ) .ie. set p to either
      first or second or third row of C.
      Where C=[1 1 0 0 0 0
               0 0 1 1 0 0
               0 0 0 0 1 1]

      Generate 1−D shares, S1 , S2 and  S3 as follows:
      for j=1:6
   if 6*i-(6-j)<=lw
   S1(yw(6*i-(6-j)))=p(j);
   S2(yw(6*i-(6-j)))=p(j);
   S3(yw(6*i-(6-j)))=p(j);
   end if
   end for
   end for
```

The conditions *i=1 to (lw/6) and 6*i-(6-j)<=lw* are used to prevent the overflow at the extreme end(while processing the last block) and to prevent from exceeding the matrix dimensions.

```
6. Get lb=length(yb)
7. Process black pixels as follows:
    for i=1 to lb/6
    Set p1=C(1,:) or p1=C(2,: ) or p1=C(3,: )i.e., set p1 to
    either first or second or third row of C randomly.
    Set p1=C(1,:) or p1=C(2,: ) or p1=C(3,: ) i.e., set p1 to
    either first or second or third  row of C randomly.
    Set p2=circshift(p1',2)';i.e., circularly right shift p1 by 2
    positions.
    Set p3=circshift(p1',4)';i.e., circularly right shift p1 by 4
    positions

    Continue generating 1-D shares, S1 S2 and S3 as follows:
    for j=1:6
    if 6*i-(6-j)<=lb
    S1(yb(6*i-(6-j)))=p1(j);
    S2(yb(6*i-(6-j)))=p2(j);
    S3(yb(6*i-(6-j)))=p3(j);
    end if
    end for
    end for
    end procedure
```

The outputs of Share generation algorithm are three 1−D shares (*S1 S2* and *S3*) which are of same size as that of 1−D secret image.

Algorithm 4: *Secret Image Recovery*

Given the inputs to the algorithm are two or three 1−D image vectors *s1*(share 1) s2(share 2) and *s3*(share 3) of size 1 x m*n. The algorithm generates non-expanded 1−D recovered secret image vector, *R1 or R2* of size 1 x m*n.

Only two shares are sufficient to reveal the secret. If all the three shares are ORed, then the corresponding recovered image is more clearer than the one recovered using just two shares.

procedure SECRET IMAGE RECOVERY(S1,S2,S3)

1. Perform bitwise OR operation on the two 1−D shares, S1 and S2 as follows:

$$R1 = S1 \oplus S2$$

2. Perform bitwise OR operation on R1 and S3 as follows:

$$R2 = R1 \oplus S3$$

Where R2 is the recovered 1−D secret image.

This output (R1 or R2) is taken as the input to the Inverse Zigzag algorithm. Inverse Zigzag algorithm converts the 1−D secret image vector to 2−D secret image matrix.

The encoding and decoding are shown in the figures Fig.5 and Fig.6 respectively:

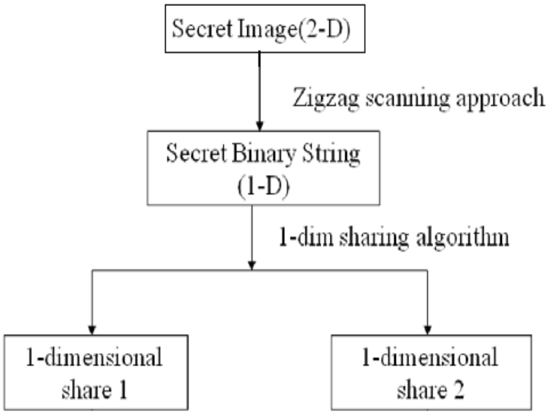


Fig.5. Encoding

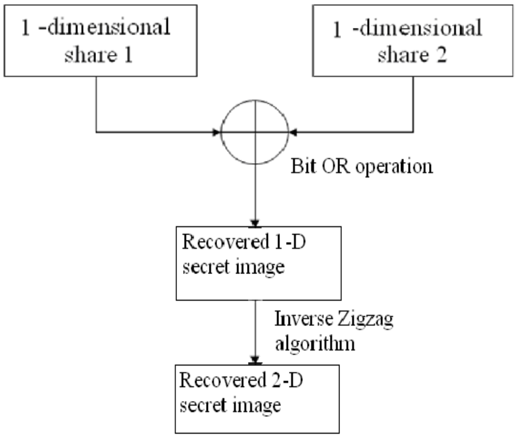


Fig.6. Decoding

III. TEST RESULTS

The experimental results demonstrate an example of applying this scheme to a secret image. The secret image can be black and white or scale image.

Figure 7 shows an example of applying 2-out-of-2 VSS scheme to a black and white secret image. Fig.7a shows the black and white secret image. This is the confidential data that has to be encrypted. Fig.7b shows the 2−D converted non-expanded share 1. Fig.7c shows the 2−D converted non-expanded share 2. Figures 7b and 7c are the output of the VC algorithm using Zigzag scanning. Fig.7d shows the recovered secret image by overlapping the two shares. In computer, the overlapping can be done using bitwise OR operation.

Figure 8 shows an example of applying 2-out-of-3(3-out-of-3) VSS scheme to a black and white secret image. The black and white secret image is shown in Fig.7a. Fig.8a shows the 2−D converted non-expanded share 1. Fig.8b shows the 2−D converted non-expanded share 2. Fig.8c shows the 2−D converted non-expanded share 3. Fig.8d shows the recovered secret image by overlapping the two shares, share 1 and share

2. Fig.8e shows the recovered secret image by overlapping all the two shares, share 1, share 2 and share 3.It can been seen in the figures that Fig.8e is clearer than Fig.8d.

Figure 9 shows an example of applying 2-out-of-2 VSS scheme to a gray scale secret image. Fig.9a shows the gray scale secret image. For gray scale images, initially the gray scale image has to be halftoned using any standard halftoning algorithm [4]. This halftoned image is the confidential data that has to be encrypted. Fig.9b shows the halftoned secret image. Fig.9c and Fig.9d shows the 2−D converted non-expanded share 1 and share 2 respectively. Fig.9e shows the recovered secret image by overlapping the two shares.

From the experimental results it can be seen that there is very less quality loss in the decoded image. Also the proposed scheme provides non expanded shares. Another advantage is that this scheme overcomes the drawback of Hilbert Curve approach.

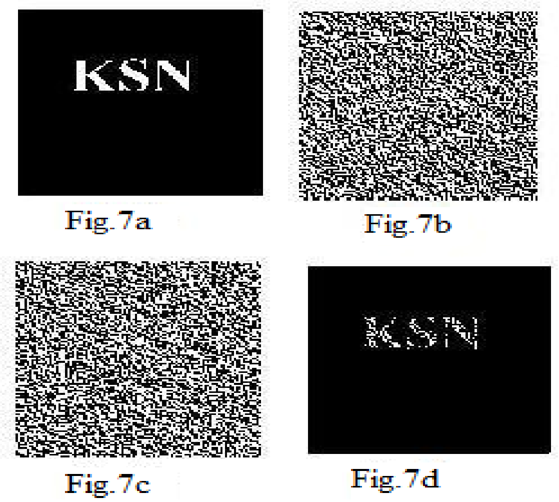


Fig.7 2-out-of-2 VSS scheme for Black and white secret image((a) Secret Image (b) 2−D converted Share 1 (c) 2−D converted Share 2 (d) Decoded Secret Image)

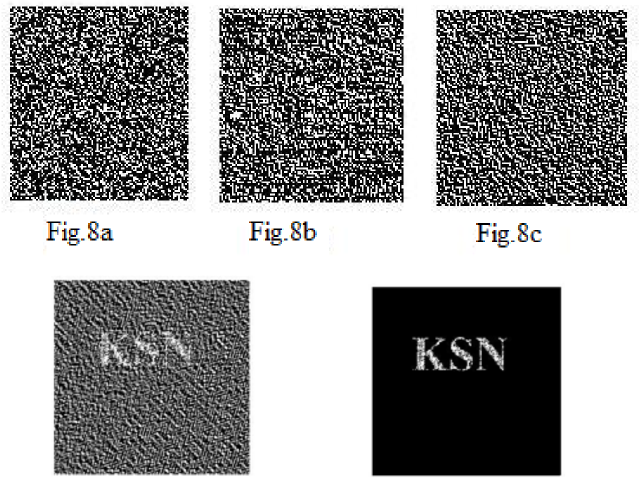


Fig.8d Fig.8e

Fig.8 2-out-of-3 VSS scheme for Black and white secret image((a) 2−D converted Share 1 (b) 2−D converted Share 2 (c) 2−D converted Share 3(d)Overlapping any two shares(e) Overlapping all three shares)

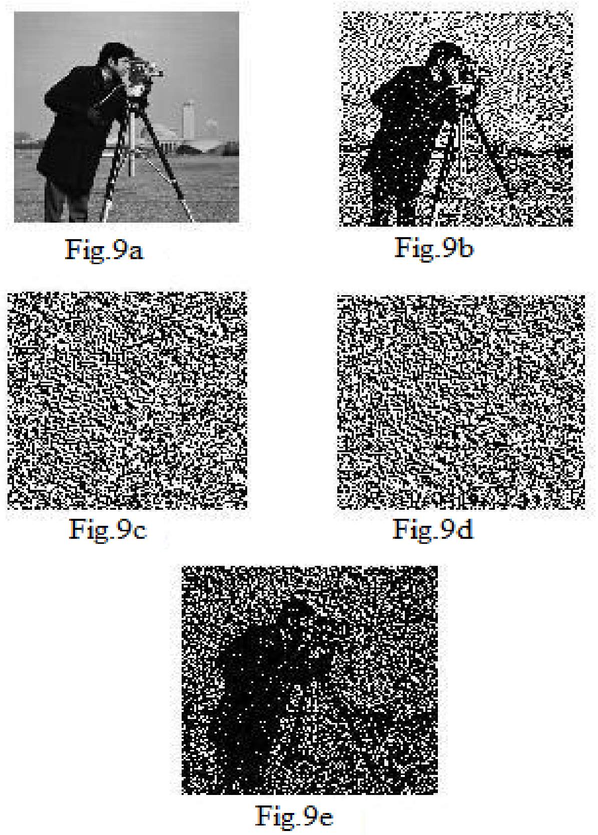


Fig.9 2-out-of-2 VSS scheme for Gray Scale secret image((a) Secret Image **(b)** Halftoned Secret Image **(c)** 2−D converted Share 1 **(d)** 2−D converted Share 2 **(e)** Decoded Secret Image)

The performance of the proposed method is very good. The MSE (Mean Square Error) of the proposed method is 0.0156 and the PSNR (Peak Signal to Noise Ratio) is 152.4239. The encoding time is 1.2970 seconds and the decoding time is 0.0160 seconds. The table below gives the MSE, PSNR and encoding/decoding time of different methods.

Methods	MSE	PSNR	Encoding Time (seconds)	Decoding Time (seconds)
Basic VC	0.5221	117.3235	1.3430	0.0460
Hilbert Curve Method	0.4891	117.9780	4.1570	0.0160
Proposed method	0.0156	152.4239	1.2970	0.0160

Table 1 Comparison of various methods based on MSE, PSNR and Encoding and Decoding time.

From this it can be seen that MSE is very less when compared to the other methods. The PSNR is high when compared to other methods. The encoding and decoding time are less for the proposed method when compared to other methods.

IV. CONCLUSION

In this paper a new Visual Cryptography Scheme using Zigzag Scan approach is proposed. The advantage of this approach is that the shares generated are non-expanded shares. This approach also overcomes the drawback of Hilbert Curve approach, i.e., there is no input image size restriction. The proposed method can be extended to k-out-of-n VSS scheme.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science*, Vol. 950, pp. 1 - 12, 1995.

[2] Sen-Jen Lin, Ja-Chen Lin, Wen-Pinn Fang, " Visual Cryptography (VC) with Non-expanded Shadow Images: Hilbert-curve Approach", 2008.

[3] http://en.wikipedia.org/wiki/File:Zigzag_scanning.jpg

[4] Wei Qiao, Hongdong Yin, Huaqing Liang," A Kind of Visual Cryptography Scheme For Color Images Based on Halftone Technique", 2009.

[5] www.mathworks.com