ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Secure Approach for Data Hiding using Visual Cryptography

Sankar Das, Asoke Nath, Arijit Samanta, Abhishek Roy, Saptarshi Bhattacharyya

Dept. of Computer Science, St. Xavier's Collage (Autonomous), Kolkata, India

ABSTRACT: Visual Cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by Human Visual System. There have various approaches developed for encrypting image. The former being encrypting the images through encryption algorithms using keys, and the later approach involves dividing the image into random shares without the use of keys. But unfortunately there has heavy computation cost and key management and the poor quality of the recovered image from the random shares limit the applications. In this paper we propose a novel approach with the use of random share and key share. The approach employs generating two shares of the original image. One random share and the other key share. The original secret image can be recovered from the two shares simply by Xoring the two shares without any loss of image quality.

KEYWORDS: Visual Cryptography, Overlapping, Shares, Image Encryption, Color image, Grayscale Images, Monochrome images.

I. INTRODUCTION

The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR.

The main purpose of developing Visual Cryptography schemes project is to provide secret image sharing and recover the secret information. The main advantage of this system is we are not going to lose visual image quality and image pixel size. Visual cryptography allows for image encryption and decryption using visual technique. This technique uses an encoding and decoding scheme to protect the data privacy. By use of this technique no one accept the sender and intended receiver knows about the data transferred. Due to its simplicity the system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations.

Our main objective is to build a tool based on Visual Cryptography System. By which we can encode a secrete image and create 2 or more shares of that image. It will encoded such a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together.

II. LITERATURE REVIEW

Visual Cryptography mainly operates on binary inputs. Hence natural images must be converted into halftone images using density of dots in order to simulate gray level. Binary data can be displayed as transparent when printed on transparent screen. Each pixel of the image is divided into smaller blocks. There are always same numbers of black and white blocks. If a pixel is divided into 2 parts there is only 1 black and 1 white block. If a pixel is divided into 4 parts there are 2 black and 2 white blocks.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

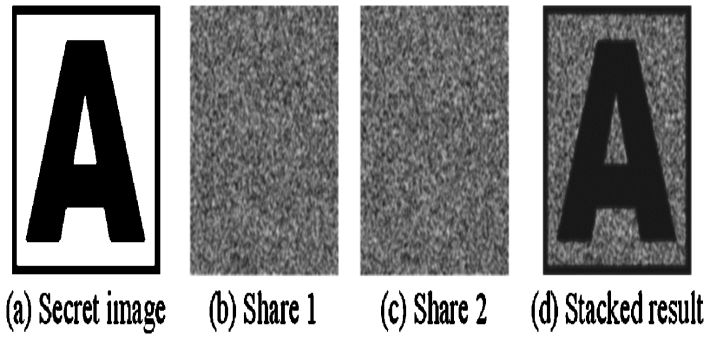
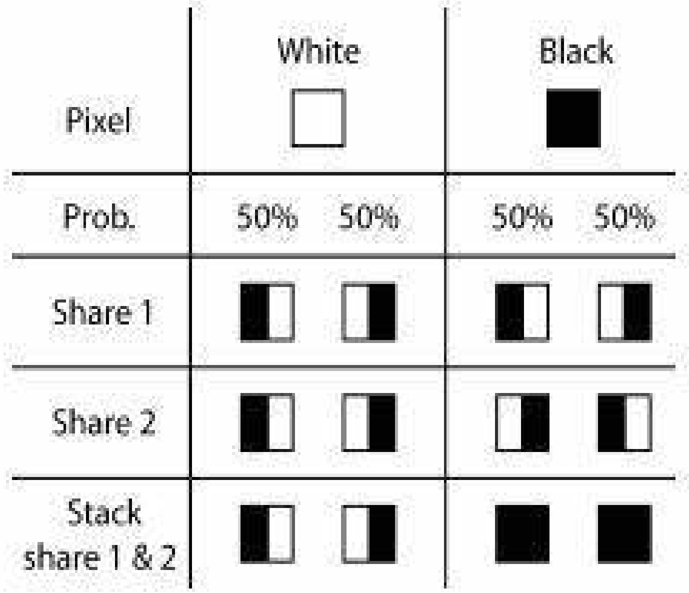


Fig-1: Example of Visual Cryptography

The basic model of Visual Cryptography proposed by Naor and Shamir accepts a binary image as a secret image which is divided into n number of shares. Each pixel of image is represented by m sub pixels. The resulting structure of shared image is represented by s where S = [Sij], an n x m matrix. Any black and white visual cryptography scheme can be described using 2 n x m Boolean matrices (S0 and S1). S0 is used if pixel in the original image is white and S1 is used if pixel in original image is black. In Visual Cryptography white pixel is represented by 0 and black pixel is represented by 1. There are different Visual Cryptography schemes such as 2 out of 2, 2 out of n, n out of n and k out of n. The most commonly used is 2 out of 2 Visual Cryptography scheme.
For 2 out of 2 Visual Cryptography scheme S0 and S1 are as follows

$$S0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



.

Fig-2: Construction of 2, 2 Visual Cryptography scheme

There are 2 collections of matrices C0 and C1. To share a white pixel we choose one of the matrixes in C0 and to share black pixel we chooses one of the matrix in C1. The first row of chosen matrix is used for share S1 and the second row is used for share S2.
The disadvantage is that for every pixel encoded from original image into 2 sub pixels and placed on each share to share have size of S x 2S if secret image is of size S x S. There is a distortion; hence we go for 4 sub pixel layout design. Here pixel is expanded into 2 x 2 sub pixels.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

$$S0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad S1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

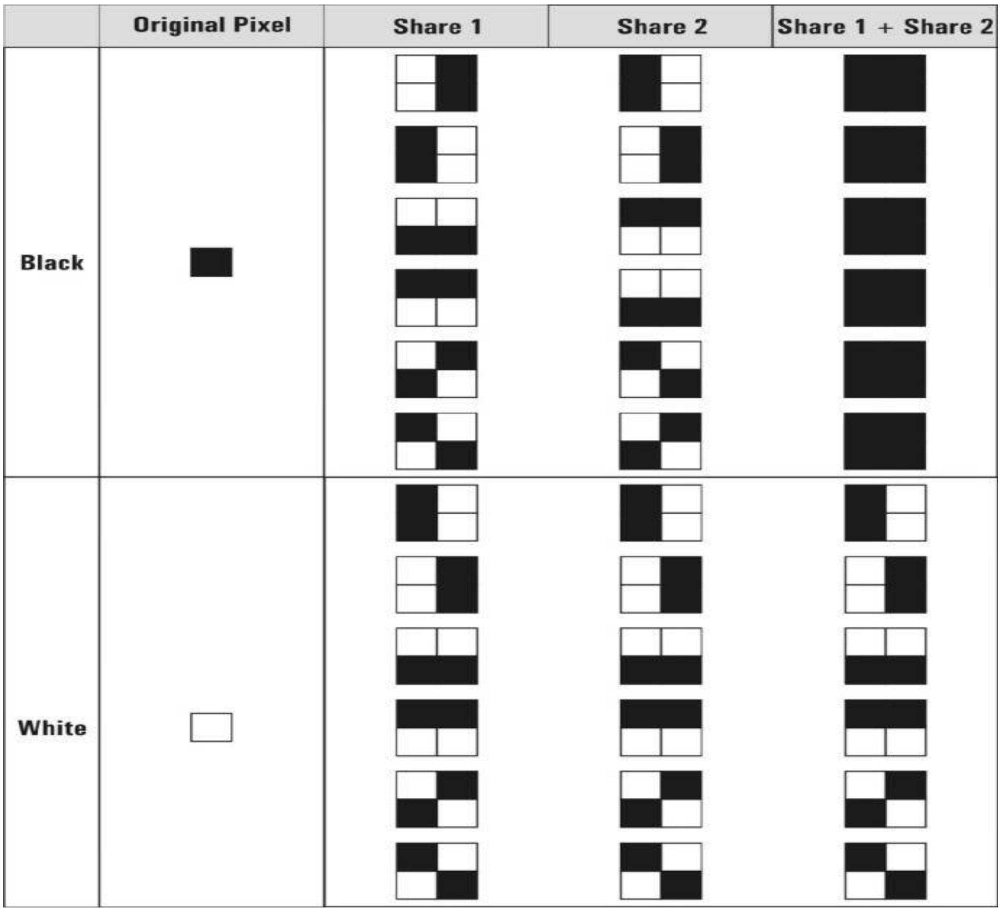


Fig-3: Construction of 2, 2 Visual Cryptography scheme with 4 sub pixel layout design

III. PROPOSED ALGORITHM

In our project we have used a hybrid approach of Visual Cryptography where we take the image and split the image into two shares. The first share is the random share and the second share is the key share. These two shares have no resemblance to the original image. When the two shares are combined using XOR it reveals the original image. The quality of the image revealed is same as the original image. This algorithm has perfect reconstruction property and there is no loss of picture quality. This algorithm can also be used on Black and white images without any loss of image quality.

Algorithm:

Step 1: Random Share generation
Step 2: Key Share generation
Step 3: Overlapping the two shares

In RGB model every color image is composed of pixels where each pixel is a series of bits composed of RGB values. Each value is in the range of 0-255. i.e. Red ranges from 0-255, Green ranges from 0-255 and Blue ranges from 0-255. When all these three values for RGB are combined we get a color which defines the pixel of the image.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

In step 1: Random Share generation for color image, a random share is generated by taking any random value for R, G and B for each pixel. And for monochrome image each pixel has only one value either 0 or 1. So, random share will be created by taking 0 or 1 randomly. The size of the share is same as the original image. Every time we create a random share it gives a different value for each pixel. So, two random shares of the same image are not same.

In step 2: Key share generation, a key share is generated by xoring every pixel of random share with every pixel of the original image. The size of this share is also same as the original image. No two key shares of the same image are same since no two random shares are same.

In step 3: Overlapping of the shares is done by xoring the random share with the key share pixel by pixel. This results in the generation of the original image.

For 24-bit color image

```
Algorithm RKO ( )
 {
  For every pixel i=0 to n
  {
    RSi = R (0-255) + G (0-255) + B (0-255)
    KSi = RSi ⊕ OIi
    }
    OI = RS ⊕ KS
  }
```

For Monochrome image

```
Algorithm RKO ( )
 {
  For every pixel i=0 to n
  {
    RSi = R (0-1)
    KSi = RSi ⊕ OIi
    }
      OI = RS ⊕ KS
   }
```

/* OI = Original Image, RS=Random Share, KS=Key Share*/

IV. RESULTS AND DISCUSSIONS

Test Reports:
All the test cases mentioned above passed successfully.

A. 24-bit Color image:

1. Example—1:

The RKO technique was implemented on color image showed in Fig.4. The two shares of the image are share1 and share2 shown in Fig 5 and Fig 6 respectively. The resultant image after overlapping both the shares is shown in Fig 7.

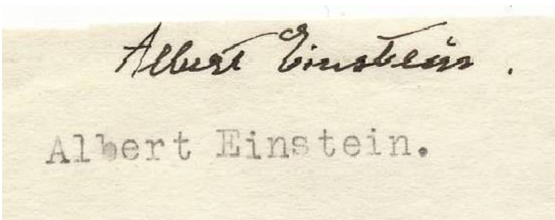


Fig.4. Color image

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

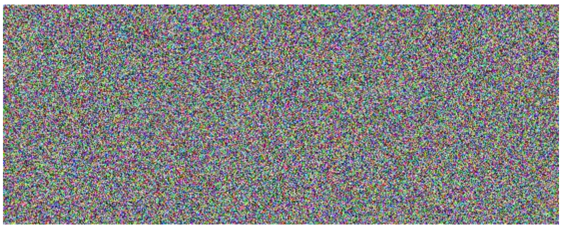


Fig 5. Share1

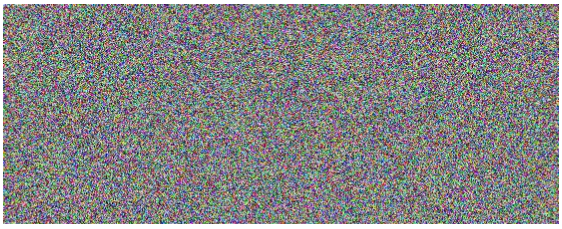


Fig 6. Share2

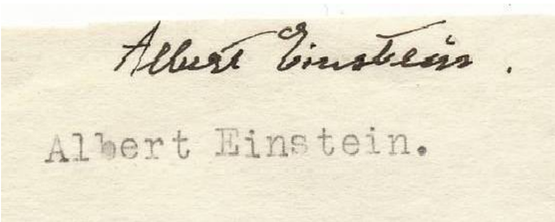


Fig 7. Resultant image

2. Example—2:

Fig 8. Color image

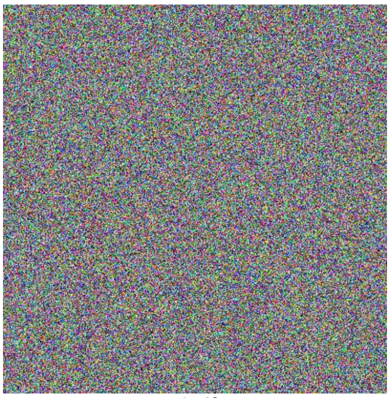


Fig 9. Share1

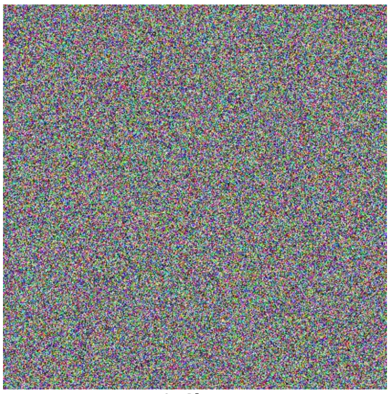


Fig 10. Share2

Fig 11. Resultant image

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

B. 8-bit Gray Scale Image:

1. Example—1:

The RKO technique was also implemented on gray scale image shown in Fig 12. The two shares of the image are share1 and share2 shown in Fig 13 and Fig 14 respectively. The resultant image after overlapping both the shares is shown in Fig 15.

Fig 12. Gray Scale Image

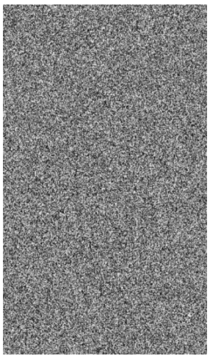


Fig 13. Share1

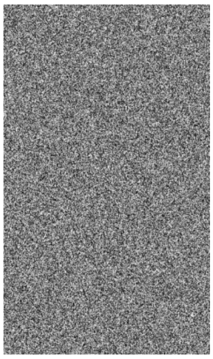


Fig 14. Share2

Fig 15. Resultant image

2. Example—2:

Fig 16. Gray Scale Image

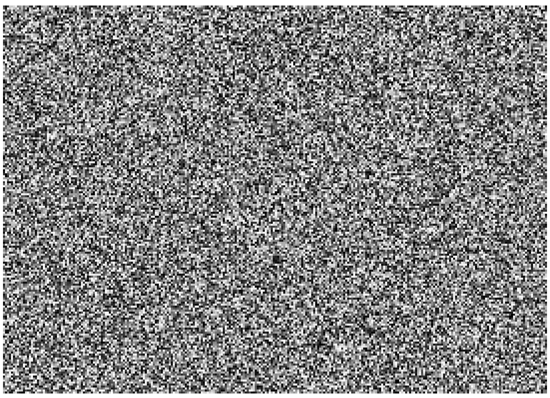


Fig 17. Share1

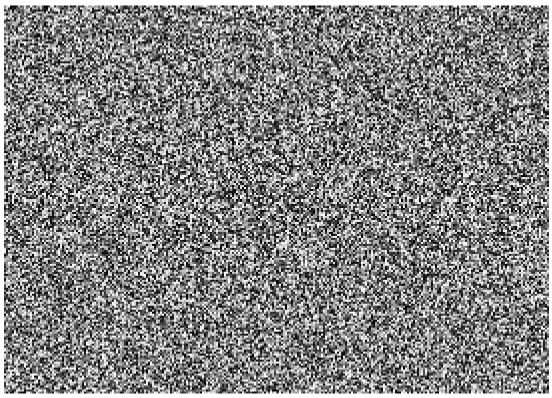


Fig 18. Share2

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Fig 19. Resultant image

C. 1-bit Black and White image:

1. Example—1:

The RKO technique was also implemented on black and white image shown in Fig 20. The two shares of the image are share1 and share2 shown in Fig 21 and Fig 22 respectively. The resultant image after overlapping both the shares is shown in Fig 23.

Fig 20. Monochrome image

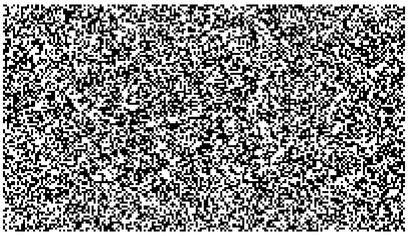


Fig 21. Share1

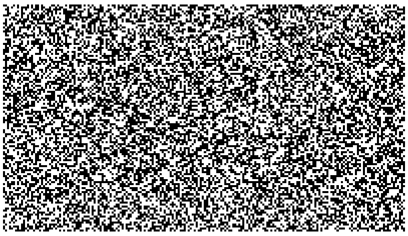


Fig 22. Share2

Fig 23. Resultant image

All shares and resultant image is generated programmatically. If we take a print out of these two black and white shares on a transparent sheet and if it is overlapped we will be able to see the message. It will look like –

2. Example—2:

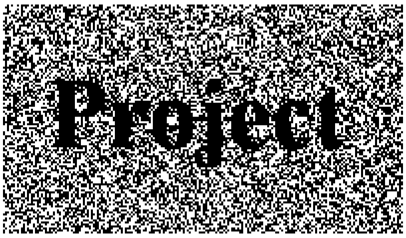


Fig 24. Overlapped image of printed shares

V. CONCLUSION

In this project a secret image is split into two images, one random image and one key image and with minimum computation the original secret image can be retrieved back.

This project has the following merits:
(a) The original secret image can be retrieved in totality.
(b) There is no pixel expansion and hence storage requirement per random share is same as original image.
(c) The quality of the image recovered is same as the original image.
(d) The same technique can be used on gray scale images and black and white images.
The scheme is suitable for authentication based application where authentication can be done by overlapping the shares over one another to reveal the secret image. If the secret image matches the original image then only access can be granted.

VI. FUTURE SCOPE

There is a lot of scope in Visual Cryptography for encrypting images. The RKO technique has used in this project which produce the output image as original image. Where it produces random shares also, this technique can be developed by increasing randomness in shares.

REFERENCES

1. RKO Technique for Color Visual Cryptography by Ms. Moushmee Kuri1, Dr. Tanuja Sarode2, 1(Computer Department, W.I.E.E.C.T/Mumbai University, India) 2(Computer Department, T.S.E.C/Mumbai University, India), IOSR Journal of Computer Engineering (IOSR-JCE) e- ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93.
2. http://in.mathworks.com/matlabcentral/answers/178981-how-to-apply-visual-cryptography-in-color-image-using-rko-technique [Access Date: 15/2/2016]
3. http://www.datagenetics.com/blog/november32013/ [Access Date: 15/2/2016]
4. http://numbersandshapes.net/2008/11/visual-cryptography/ [Access Date: 15/2/2016]
5. http://www.pirotechnologies.com/projects/matlab-projects/image-processing-based-matlab-projects/image-cryptography-based-matlab-projects [Access Date: 15/2/2016]
6. Hierarchical Implementation of RKO Technique for Visual Cryptography by Ms. Moushmee Kuri, 2 Dr. Tanuja Sarode , IJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014 ISSN: 2348 – 6090
7. An Implementation of Algorithms in Visual Cryptography in Images by Archana B. Dhole, Prof. Nitin J. Janwe, International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013
8. http://users.telenet.be/d.rijmenants/en/visualcrypto.htm. [Access Date: 18/2/2016]
9. https://www.researchgate.net/publication/228980617_New_Algorithm_For _Halftone_Image_Visual_Cryptography [Access Date: 10/1/2016]
10. Data Hiding and Retrieval using Visual Cryptography by Sougata Mandal, Sankar Das, Asoke Nath , International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1 Issue 1 (April 2014).
11. Visual Cryptography using Three Independent Shares in Color Images by Sankar Das, Sandipan Chowdhury, Dibya Chakraborty, Arijit Das, Asoke Nath, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 4, Volume 2 (April 2015)
12. Scope and Challenges in Visual Cryptography by Monish Kumar Dutta, Asoke Nath, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 11 (November 2014)
13. Y. C. Hou, "Visual cryptography for color images," Pattern Recognition, vol. 36, pp. 1619-1629, 2003.
14. M. Naor and A. Shamir, "Visual cryptography," in Proc. *EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS*

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

15. A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
16. Secret Sharing Using Visual Cryptography by Renu Poriye, Dr S. S Tyagi, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 1, Issue 4, August 2014, PP 46-52 ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
17. L. W. Hawkes, A. Yasinsac and C. Cline, "An Application of Visual Cryptography to Financial Documents," *Technical report TR001001,Florida State University, 2000.*
18. Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, Symmetric Key Cryptography using Random Key generator : “Proceedings of International conference on security and management(SAM’10” held at Las Vegas, USA Jull 12-15, 2010), Vol-2, Page: 239-244(2010).
19. Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, Advanced steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2 and LSB+3 bits in non-standard cover files:, International Journal of Computer Applications, Vol14-No.7,Page-31-35, Feb(2011).
20. A. Shamir, Visual cryptanalysis, Proceedings of the Eurocrypt’98, Espoo, 1998.
21. D.R. Stinson, An introduction to visual cryptography, presented at Public Key Solutions ’97, Toronto, Canada, April28–30, 1997.