International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 11 (November 2014) www.ijirae.com

Scope and Challenges in Visual Cryptography

Monish Kumar Dutta
Department of Computer Science
St. Xavier's College(Autonomous)
Kolkata, India

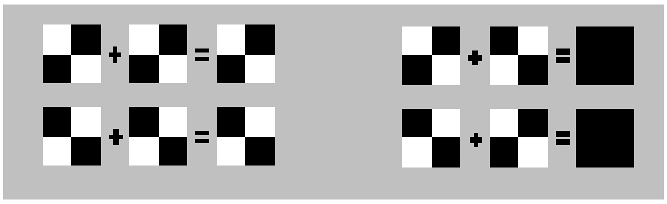
Asoke Nath
Department of Computer Science
St. Xavoier's College(Autonomous)
Kolkata, India

Abstract— Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using the tool, thus gets the original image. The proposed Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using the application here sender gets the two or more transparencies of the same image. The application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using the application one can send encrypted images that are in the format of GIF and PNG. The encrypted transparencies can be saved in the machine and can be sent to the intended person by other means. In the present work the author has made a systematic study on various methods in visual cryptography and also how it can be upgraded by embossing encrypted secret message in multiple shares using some standard cryptographic methods developed by Nath et al to make the whole system more secured.

Keywords— Visual Cryptography, encryption, decryption, transparencies, halftone

I. Introduction

The network services are now open to all so confidential data may not be safe at all through the network. So it needs to be encrypted first so that if somebody manages to retrieve/capture the data from network, he shouldn't be able to decrypt the original message. In classical cryptography there are two methods. One of them is symmetric key cryptography, where same key will be used for encryption as well as decryption also, but will be used in opposite manner. Another method is asymmetric key, where encryption will be done using public key which may be known to all but decryption will be done by private key that is known to the user/receiver only. The basic idea of cryptography is that the computation process should be complex enough such that nobody i.e. the intruder will be able to break the system. In 1994, Naor and Shamir introduced first time securing data without cryptographic computation, termed as **Visual Cryptography**. It exploits human visual system to read messages from some overlapping shares, which reduces the computational overhead that is the disadvantage of complex computation in classical cryptography. 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. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image. In Visual cryptography technology, the end user identifies an image, which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Prior to this the data is embedded into the image and then sent. The image if hacked or interpreted by a third party user will open up in any image previewed but not displaying the data. This protects the data from being invisible and hence is secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the image. This method can be used in forensic department or in defense for keeping confidential information secret. Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.



Although most of techniques are on the basis of black and white images or few grey scale images, Rijmen and Preneel have proposed a visual cryptography for color images. They expanded each color pixel into 2X2 block to form two sharing images. And each block is filled by red, green, blue and white respectively. Hence no clue about the secret image will be identified using any one of them alone. And they claimed that there will be 24 color combinations using those four colors.

II. BASICS OF VISUAL CRYPTOGRAPHY

A. Visual Cryptography for General Access Structure by Multi-pixel Encoding with Variable Block Size

Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each run. However its encoding efficiency is still low. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

B. Halftone Visual Cryptography

In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares carrying significant visual information. The simulation shows that the visual qualities of the obtained halftone shares are observably better than that attained by any available visual cryptography method known to date.

C. Visual Cryptography for Print and Scan Applications

Visual cryptography is not much in use because of the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. The print and scan process can introduce noise as well which can make the alignment difficult. In this paper, we consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the vulnerabilities in the spatial domain, we have developed a frequency domain alignment scheme. We employ the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Our experimental results show that the technique can be useful in print and scan applications.

D. Joint Visual Cryptography and Watermarking

In this paper, we discuss how to use watermarking technique for visual cryptography. Both halftone watermarking and visual cryptography involve a hidden secret image. However, their concepts are different. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in a single halftone image while preserving the quality of the watermarked halftone image. In this paper, they proposed a joint visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking.

E. An Improved Visual Cryptography Scheme for Secret Hiding

This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity. The Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images (either binary or color) and number of secret images (either single or multiple) encrypted by the scheme. Recently, Chang et al. proposed a color sharing system. The algorithm first creates a palette of a secret image and assigns a unique code on the palette. It then selects two colored cover images with size same as the secret image. Every pixel in the two cover images will be expanded into a block with M(=K x K)sub pixels, of which floor(M/2)+1 sub pixels are randomly selected and filled with the color of the expanded pixel and the rest are filled with white(transparent) color. The selection condition is that N positions of the two expanded blocks are overlapped, where N is the index of the palette of the secret image and is used to indicate the pixel color shared by two expanded blocks. The algorithm computes the no. of overlapping sub pixels of every k x k block in the two camouflage image and then retrieves the Nth color from the palette to reconstruct the color of the corresponding pixel of the secret image. But this method can only deal with a color image with limited different colors. Hou et al. proposed a method to improve the above drawback. The used the binary encoding to represent the sub pixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking sub pixels of every block in the cover images. The code ranges from 0 to255, but it can be even larger depending on expanding factor. Although Chang and Hou et al. achieved a certain degree of sharing color image information, the drawback is that secret image must be decrypted with heavy computation, which would violate the principle of visual cryptography that uses human eyes to decrypt secret images. Hou et al. used the concepts of color decomposition and contrast adjustment to produce two shares needed by visual cryptography. Although this method requires no mass computation to reconstruct secret images, it is none the less difficult to obtain totally random noise shares.

III. ALGORITHMS USED IN VISUAL CRYPTOGRAPHY

A. Existing System

Visual cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended recipient even realizes the original image, a form of security through obscurity. By contrast, cryptography obscures the original image, but it does not conceal the fact that it is not the actual image.

After generating the covering shares, the embedding process can be realized by the following algorithm.
The embedding process:
Input: The corresponding VCS (c0, c1) with pixel expansion and the secret image.
Output: The n embedded shares e0,e1 ...en-1.
Step1: Dividing the covering shares into blocks that contain (t ≥ m) sub pixels each.
Step2: Choose m embedding positions in each block in the n covering shares.
Step3: For each black (respectively, white) pixel in I, randomly choose a share matrix M C1. ∈
Step4: Embed the m sub pixel of each row of the share matrix M into the m embedding positions chosen in Step2.

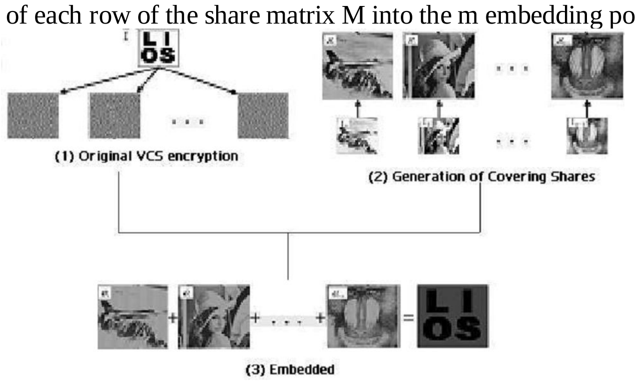

I
LI
OS
(1) Original VCS encryption
(2) Generation of Covering Shares
(3) Embedded

Fig. Embedding Process

B. The HalftoneTechnology

According to their physical characteristics, different media use different ways to represent color level of images. The diversity of the lightness generates different color levels. The general printer, laser printer, jet printer can only control a single pixel to be printed (black) or not to be printed (white), instead of displaying the grey level or the color tone of an image directly. As such, the way to represent the grey level of images is to use the density of printed dots; for example, the printed dots in the bright part of the image are sparse, and in the dark part are dense. This method is called "Halftone" and transforms an image with grey level into a binary image before processing.

C. Floyd's Error Diffusion Halftoning

Let P(i,j) be the original image of size n x m. Then we can calculate errors as follows

```
for i=1 to n do
          for j-1 to m do
                    if P(i,j) > 127 then
                              Q(i,j)=1
                    else
                              Q(i,j)=0
                    end
                    error=255*Q(i,j)-P(i,j)
                    P(i,j+1)=7/16*error
                    P(i+1,j+1)=1/16*error
                    P(i+1,j)=5/16*error
                    P(i+1,j-1)=3/16*error
          end
end
```

D. Jarvis's Error Diffusion Half toning

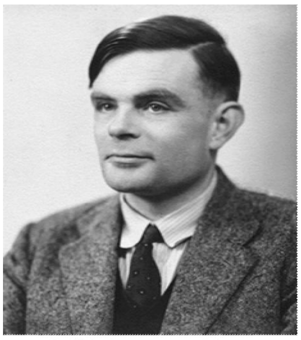


Fig. 1(a) Continuous tone greys cale image

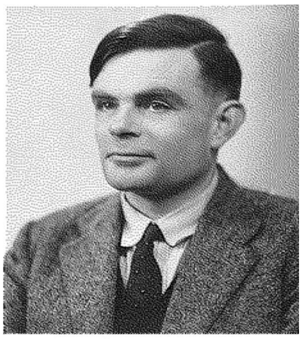


Fig. 1(b) Halftone greys cale image

Let P(i,j) be the original image of size n x m. Then we can calculate errors as follows

```
        for i=1 to n do
                for j-1 to m do
                        if P(i,j) > 127 then
                                Q(i,j)=1
                        else
                                Q(i,j)=0
                        end
                        error=255*Q(i,j)-P(i,j)
                        distribute error accordingly as in         table 2
end
        end
```

Table 1
Floyd's Error Diffusion Matrix

	P(i,j) error	7/16
3/16	5/16	1/16

Table 2
Jarvis's Error Diffusion Matrix

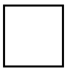
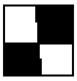
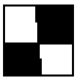
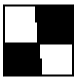
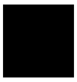
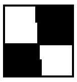
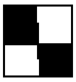
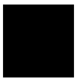
		P(i,j) error	/48	5/48
3/48	5/48	7/48	5/48	3/48
1/48	3/48	5/48	3/48	1/48

E. Virtual cryptography for grey scale images

Since most printers have to transform grey scale images into halftone once before printing, and the transformed halftone images are black and white only, such an image format is very suitable for the traditional method to generate shares of visual cryptography.

The algorithm is as follows

- Step1: transform the grey level image into a black and white halftone image.
- Step2: black or white pixel in the halftone image, decompose it into a 2x2 block of the two transparencies according to rules in the table. If the pixel is white, select the combination from the former two rows in table as the content of blocks in shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies.
- Step3: repeat step2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

Secret image	Share1	Share2	Stacked image
			
			

Virtual cryptography for color images

Here a color secret image is transformed into three R,G,B halftone images. Then every pixel of each halftone image is expanded into two 2x2 blocks to which a color is assigned.

The algorithm is as follows

- step1: read RGB image and then store R,G,B components in three 2 dimensional matrices.
- step2: apply half toning on every component
- step3: now choose halftone R matrix and apply the following operation on each element of R matrix say P(i,j) as follows

- step3.1: to create a mask, select a 2x2 block(mask_block) and assign two white pixels randomly and leave rest two black. Therefore , total number of combinations possible is 4C2=6

1	0		0	1		1	0		0	1		1	1		0	0
0	1		1	0		1	0		0	1		0	0		1	1

Mask	Pixel Color (R, G, B)	Share-1	Share-2	Share-3
⬜⬛ ⬛⬜	(0,0,0)	🟥⬛ ⬛🟥	🟩⬛ ⬛🟩	🟦⬛ ⬛🟦
	(1,0,0)	⬛🟥 🟥⬛	🟩⬛ ⬛🟩	🟦⬛ ⬛🟦
	(0,1,0)	🟥⬛ ⬛🟥	⬛🟩 🟩⬛	🟦⬛ ⬛🟦
	(0,0,1)	🟥⬛ ⬛🟥	🟩⬛ ⬛🟩	⬛🟦 🟦⬛
	(1,1,0)	⬛🟥 🟥⬛	⬛🟩 🟩⬛	🟦⬛ ⬛🟦
	(0,1,1)	🟥⬛ ⬛🟥	⬛🟩 🟩⬛	⬛🟦 🟦⬛
	(1,0,1)	⬛🟥 🟥⬛	🟩⬛ ⬛🟩	⬛🟦 🟦⬛
	(1,1,1)	⬛🟥 🟥⬛	⬛🟩 🟩⬛	⬛🟦 🟦⬛

- step3.2: determine the positions of the red pixels in halftone R matrix and assign the block in share1.

If Rij=1 then new _block=~mask_block
if Rij=0 then new_block=mask_block
now add new_block to the corresponding position in share1.

- Step4: repeat step 3 for green and blue components for creating share 1 and share 3 respectively.
- Step5: after creating all the shares, combine them to get one share only. This share acts as a public key. Example:

1	0		0	0		1	0
0	1		1	1		1	0

Share-1 Share-2 Share-3

After combining we get a 3 dimensional array A
A(1,1,1)=1, A(1,1,2)=0, A(1,1,3)=1, A(1,2,1)=0, A(1,2,2)=0, A(1,2,3)=0, A(2,1,1)=0, A(2,1,2)=1, A(2,1,3)=1, A(2,2,1)=1, A(2,2,2)=1, A(2,2,3)=0

- Step6: combine all 3 masks to get the second share which acts as the private key.

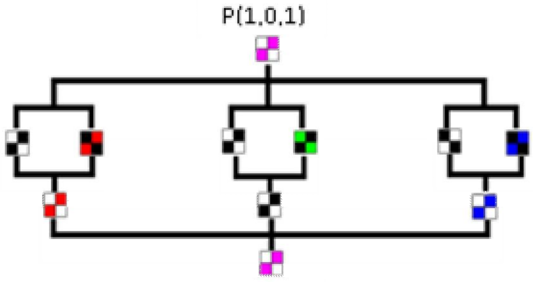
Example: after combining we get a 3 dimensional array A

0	0		0	1		1	1
1	1		1	0		0	0

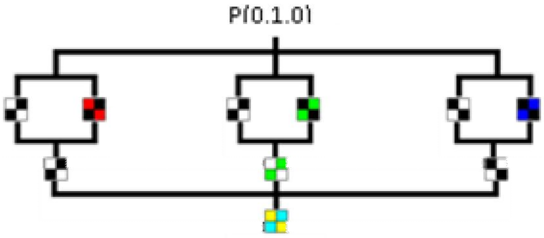
Mas k-1 Mas k-2 Mas k-3

A(1,1,1)=0, A(1,1,2)=0, A(1,1,3)=1, A(1,2,1)=0, A(1,2,2)=0, A(1,2,3)=1, A(2,1,1)=1, A(2,1,2)=1, A(2,1,3)=0, A(2,2,1)=1, A(2,2,2)=0, A(2,2,3)=0

- Step7: now take a cover image which is large enough to accommodate embedding the share obtained in the previous step. By that we mean, if size of the share is r1xc1x3 and embedding starts from location (i,j,1), then the size of the secret image should be at least (since we are embedding in the LSB,LSB+1,LSB+2 positions){(i-1)xc2+(j-1)}x3+r1xc1+100 where r2xc2x3 is the size of the cover image. 100 bits are required to embed size of the secret image and other additional information (if required).
- Step8: for decryption we first extract the public share embedded in the cover image.
- Step9: once the share has been extracted, perform bitwise or operation between each component of the share and its corresponding mask.



- step10: since separate masks were used for encryption, after performing OR operation some unwanted colors may show up.



The output block was supposed to be . A simple technique can fix this. The idea is that if more than one of R, G, B components have blocks containing 0's, their distribution of black and white pixels has to be same. This takes care of the undesired colors. Thus the secret image is decrypted.

IV. Results and Discussions

A. Greyscale Images

Fig. 4(a)Share-1

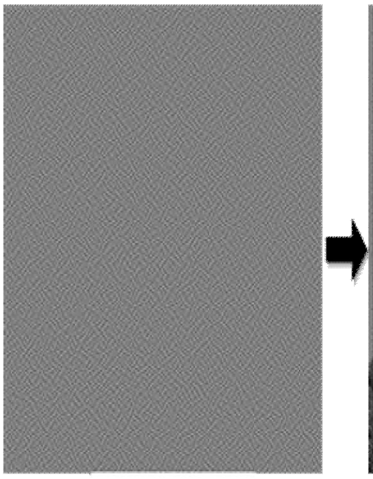


Fig. 4(b)Share-2

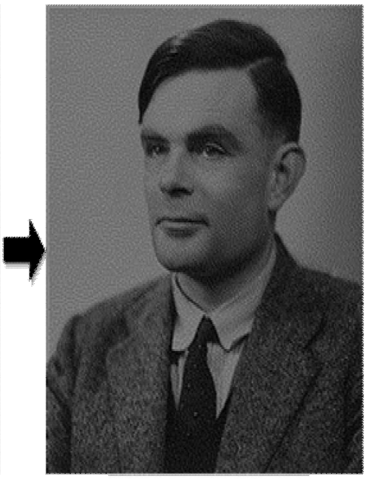


Fig. 4(c)Stacked Image

B. Color Images

1) Example-1:

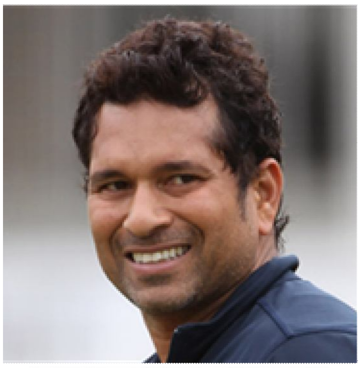


Fig. 5(a) Continuous Tone

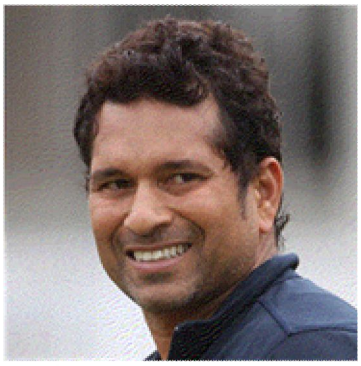


Fig. 5(b) Halftone

Fig. 6(a) Share-1

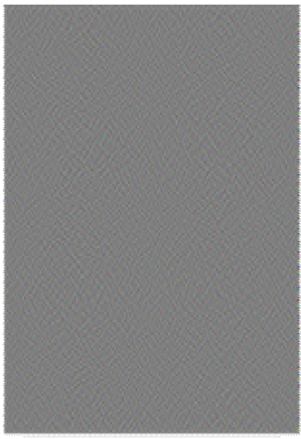


Fig. 6(b) Share-2

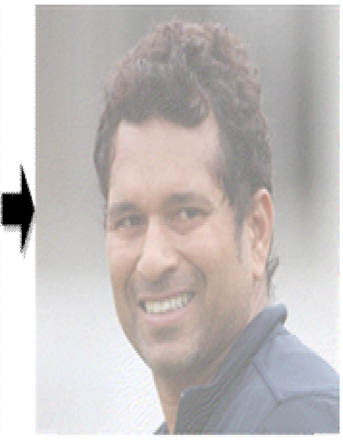
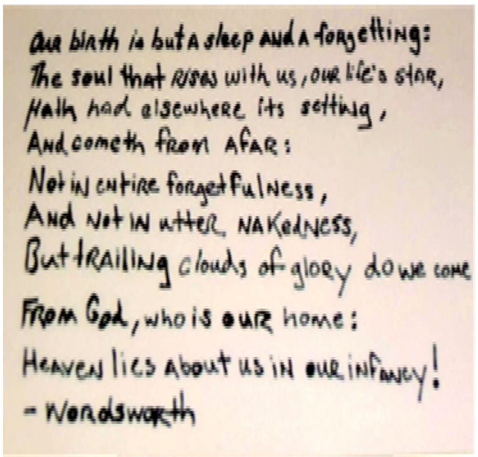


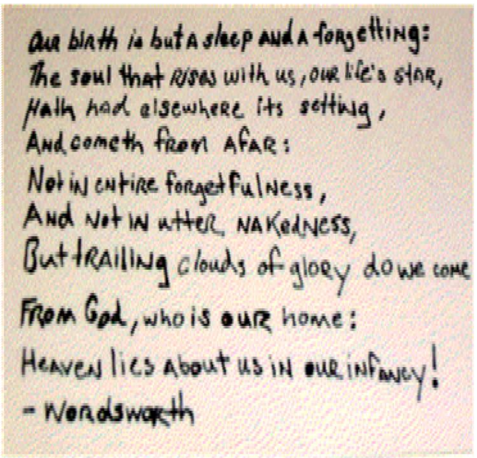
Fig. 6(c) Decrypted Image

2) Example-2:



Our birth is but a sleep and a forgetting:
The soul that rises with us, our life's star,
Hath had elsewhere its setting,
And cometh from afar:
Not in entire forgetfulness,
And not in utter nakedness,
But trailing clouds of glory do we come
From God, who is our home:
Heaven lies about us in our infancy!
- Wordsworth

Fig. 7(a) Continuous Tone



Our birth is but a sleep and a forgetting:
The soul that rises with us, our life's star,
Hath had elsewhere its setting,
And cometh from afar:
Not in entire forgetfulness,
And not in utter nakedness,
But trailing clouds of glory do we come
From God, who is our home:
Heaven lies about us in our infancy!
- Wordsworth

Fig. 7(b) Halftone

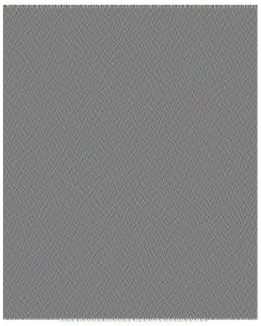


Fig.8(a)Share-1

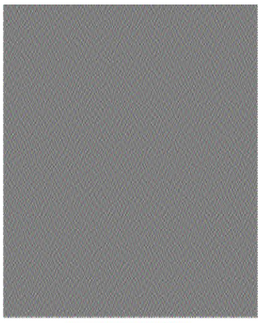
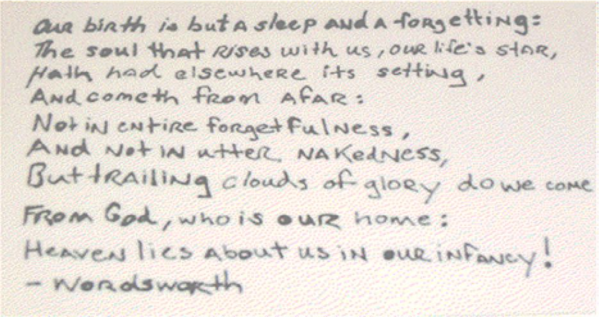


Fig.8(b)Share-2



Our birth is but a sleep and a forgetting:
The soul that rises with us, our life's star,
Hath had elsewhere its setting,
And cometh from afar:
Not in entire forgetfulness,
And not in utter nakedness,
But trailing clouds of glory do we come
From God, who is our home:
Heaven lies about us in our infancy!
- Wordsworth

Fig. 8(c) Decrypted Image

3) Example-3:

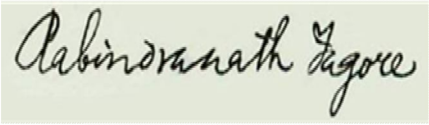


Fig. 9(a) Continuous Tone

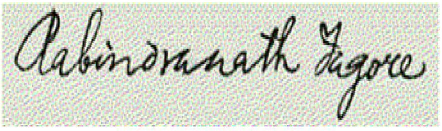


Fig 9(b) Halftone

Fig. 10(a)Share-1

Fig. 10(b)Share-2

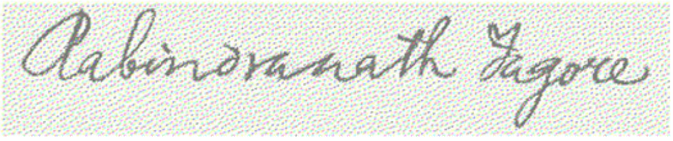


Fig. 10(c) Decrypted Image

V. CONCLUSIONS

The Embedded visual cryptography scheme tool is simple and easy to use. Various visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. Security is the primary concern of today's communication world, is successfully implemented using the IDEA algorithm. It provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption. The scope of the System provides a friendly environment to deal with images. Generally tools supports only one kind of image formats. This application supports .gif and .png (portable network graphics) formatted images and the application has been developed using swing and applet technologies, hence provides a friendly environment to users. The existing method may be further strengthened by encrypting the initial secret message using some standard cryptographic methods developed by Nath et al.

ACKNOWLEDGMENT

The authors are very much grateful to Prof. Shalabh Agarwal, Hesd, Department of Computer Science for allowing to do research work in Visual Cryptography. One of the authors AN is very much grateful to Fr. Dr. J. Felix Raj, principal of St. xavier's College(Autonomous) for giving opportunity to do research project in the Department of Computer science.

REFERENCES

[1] M. Naor, A. Shamir, in: A. De Santis (Ed.), *Visual Cryptography, Advances in Cryptology: Eurpocrypt'94,Lecture Notes in Computer Science*, Vol. 950, Springer,Berlin, 1995, pp. 1–12.

[2] M. Naor, A. Shamir, in: M. Lomas (Ed.), *Visual Cryptography, II: Improving the Contrast via the Cover Base,Presented at Security in Communication Networks*, Amalfi,Italy, September 16–17, 1996. Lecture Notes in ComputerScience, Vol. 1189, Springer, Berlin, 1997, pp. 197–202.

[3] C.C. Chang, C.S. Tsai, T.S. Chen, *A technique for sharing a secret color image,* Proceedings of the Ninth NationalConference on Information Security, Taichung, May 1999,pp. LXIII–LXXII.

[4] Y.C. Hou, F. Lin, C.Y. Chang, *Improvement and implementationof the secret color image sharing technique*, Proceedingsof the Fifth Conference on Information Management, Taipei,November 1999, pp. 592–597.

[5] Y.C. Hou, F. Lin, C.Y. Chang, *A new approach on 256 colorsecret image sharing technique*, MIS Review, No. 9, December1999, pp. 89–105.

[6] Y.C. Hou, C.Y. Chang, F. Lin, *Visual cryptography for colorimages based on color decomposition*, Proceedings of the FifthConference on Information Management, Taipei, November1999, pp. 584–591.

[7] 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).

[8] Asoke Nath, Sankar Das, Amlan Chakraborti, *Data Hiding and Retrieval* : published in IEEE "Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN 2010)" held from 26-28 NOV'2010 at Bhupal, Page: 392-397(2010).

[9] Feng Liu and chuankun Wu.(2011), *'Embedded Extended Visual Cryptography Schemes'*, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, pp. 307-322