International Journal of Innovative Research in Advanced Engineering (IJIRAE)
Volume 1 Issue 1 (April 2014)

Data Hiding and Retrieval using Visual Cryptography

Sougata Mandal
Department of Computer Science
St. Xavier's College (Autonomous),
Kolkata, India
sougatamandal033@gmail.com

Sankar Das
Department of Computer Science
St. Xavier's College (Autonomous),
Kolkata, India
dassankar16@yahoo.in

Asoke Nath
Department of Computer Science
St. Xavier's College (Autonomous),
Kolkata, India
asokejoy1@gmail.com

Abstract— ***Nath et al. developed several methods for hiding data in a cover file using different steganography methods. In some methods Nath et al. first applied encryption method before hiding into the cover file. For security reasons the secret message is encrypted first before inserting into the cover file. To make the system more complex the authors used some random insertion of bits so that even if the intruders can extract the bits from cover file but they cannot reconstruct the original secret message. In the present work the authors applied different data hiding algorithm based on visual cryptography. Visual Cryptography is now a days a very popular method for hiding any secret message inside multiple shares. Initially people were trying to hide some secret message which is simply B/W in two shares. But slowly the researchers started to hide any color image (may be text or image or any object) in two or more shares. In the present work the authors tried to hide any color message/image in two or more shares. The interesting part of the present method is that from one share it impossible to create the second share or to extract the hidden secret message from one share without having the other share(s). The present method may be used for reconstructing password or any kind of important message or image. The present method may be applied in forensic department or in defense for sending some confidential message.***

Keywords— ***steganography, secret message, encryption, visual cryptography, halftone***

I. Introduction

Due to tremendous explorations in Internet it is a real challenge to keep secret message/information intact. The network services are now almost open to everyone and that is why the probability of reaching confidential data from one computer to another computer or from one client to another client may not be safe at all. Before sending data it must be encrypted first. If it can somehow be managed to encrypt the information and then send it, safety can be assured up to a fair extent. In this paper the authors have proposed to encrypt the information which cannot be decrypted without a proper key. The classical cryptography methods are of two types. One is called symmetric key cryptography where we use one key both for encryption as well as for decryption purpose. The second type of encryption methods are called public key cryptography where two keys are used one for encryption which is also called public key and the other key only for decryption purpose and that is called secret or private key and this key should be kept by receiver only or who wants to decrypt the message. Both symmetric key cryptography as well as public key cryptography methods are massive computation oriented [1-13]. The basic criteria of cryptography are that the computation process should be very complex so that no intruder can break the system. So there was a demand from users' side that there should be simple and at the same time some secured method for encrypting some secret message.

In 1994, Naor and Shamir [14] for the first time introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography. It exploits the human visual system to read the secret message from some overlapping shares, thus overcoming the disadvantage of complex computation. Quite a number of works have been done in visual cryptography [14–23]. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images. Rijmen and Preneel [21] have proposed a visual cryptography approach for color images. They expanded each color pixel into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent) respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Rijman and Preneel claimed that there would be 24 possible combinations according to the permutation of the four colors. Because human eyes cannot detect the color of a very tiny sub pixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 242 variations of the resultant color for forming a color image. The approach of Rijmen and Preneel indeed can produce visual cryptography for color images. But from the viewpoint of either the additive model or the subtractive model of chromatology, it is not appropriate to fill the blocks with red, green, blue, and white (transparent) colors [24]. Besides, if we use the average of the four-pixel colors in the stacking blocks to represent the corresponding pixel color in the original image, the problem of circular permutations occurs. Since two circular permutations of a stacking block are not considered different, two average colors with different permutations will be the same in the stacking block if they have the same combination. Hence the number of possible color variation is fewer than the authors claimed 242.

Recently, Chang et al. [25] proposed a color image sharing technique. The algorithm first creates a palette of a secret image and assigns a unique code to each color 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 × 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 the two expanded blocks. When recovering the secret image, the algorithm computes the number of the overlapping sub-pixels of every k × k block in the two camouflage images 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. For example, if k equals 3, floor(M/2)+1 is at most 5, which is obviously too small and unreasonably restrictive for today's applications.

Hou et al. [26, 27] proposed a method to improve the above drawback. They 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 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one. Although Chang and Hou et al. [25–27] achieved a certain degree of sharing color image information, the drawback is that secret images 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. [28] used the concepts of color decomposition and contrast adjustment to produce two shares needed by visual cryptography. Overlapping these two shares will reveal the secret information automatically. Although this method requires no mass computation to reconstruct secret images, it is nonetheless difficult to obtain totally random noise shares. Some image boundaries might be found on each share, thus compromising the secrecy required.

In the present paper, the previous results in visual cryptography, the halftone technology, and the color decomposition principle to develop algorithms of visual cryptography for grey-level and color images have been combined. This method retains the advantage of traditional visual cryptography, namely, decrypting secret images without any cryptography computation. For information security, it also ensures that hackers cannot perceive any clue about the secret image from any individual sharing image. In the present paper the authors aim at providing two-level security for transmitting secret information (images) over internet. Firstly, two shares from a secret image have been generated. One of them acts as a public key and the other as the private key. Only the owner of the private key can decrypt the information from the public key. Secondly, the public key has been embedded into a cover image. This will provide another layer of protection. The authors have shown a visual cryptography scheme which is suitable for grey-scale images based on halftone technology. Based on this grey-scale technique, a visual cryptography scheme suitable for color images has been presented here. The results show that the method proposed here is unbreakable.

II. Algorithm Used In Present Study

A. *The Halftone Technology*

According to their physical characteristics, different media use different ways to represent the color level of images. The computer screen uses the electric current to control the lightness of the pixels. The diversity of the lightness generates different color levels. The general printer, such as dot-matrix printers, laser printers, and jet printers, can only control a single pixel to be printed (black pixel) or not to be printed(white pixel), 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 an image are sparse, and those in the dark part are dense. The method that uses the density of the net dots to simulate the grey level is called "Halftone" [11] and transforms an image with grey level into a binary image before processing. Take the grey-level image in Fig. 1(a) for example. Every pixel of the transformed halftone image (Fig. 1(b)) has only two possible color levels (black or white). Because human eyes cannot identify too tiny printed dots and, when viewing a dot, tend to cover its nearby dots, we can simulate different grey levels through the density of printed dots, even though the transformed image actually has only two colors— black and white.

1) *Floyd's Error Diffusion Halftoning:* Let P(i,j) be the original image of size n×m. Then we can calculate the 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
```

2) *Jarvis's Error Diffusion Halftoning:* Let P(i,j) be the original image of size n×m. Then we can calculate the errors as follows:

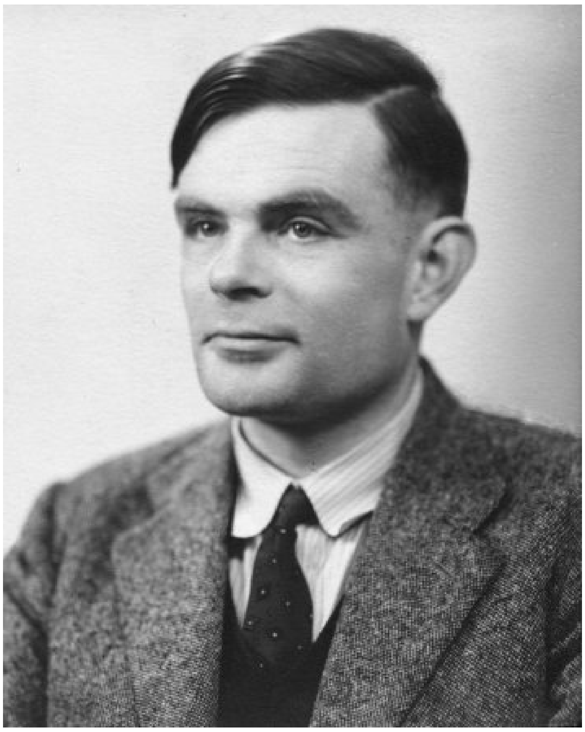


Fig. 1(a) Continuous tone greyscale image

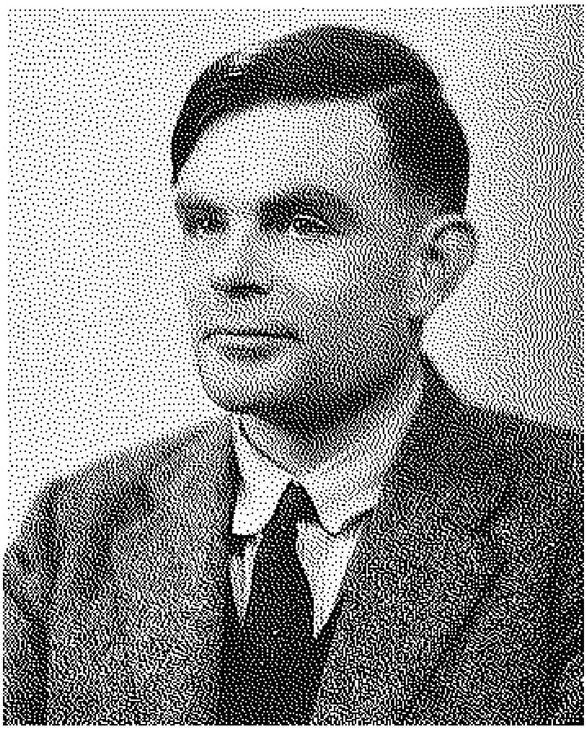


Fig. 1(b) Halftone greyscale image

```
   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 II
      end
   end
```

TABLE I
FLOYD'S ERROR DIFFUSION MATRIX

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

TABLE II
JARVIS'S ERROR DIFFUSION MATRIX

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

3) *Visual Cryptography for Greyscale Images:* Since most printers have to transform grey-level images into halftone ones 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 the shares of visual cryptography. So in this paper, we use transformed halftone images to generate the visual cryptography for greyscale images.

4) The algorithm is as follows:

- Step-1: Transform the grey-level image into a black-and-white halftone image.
- Step-2: Black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules in Table III. If the pixel is white, select the combination from the former two rows in Table III 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.
- Step-3: Repeat Step-2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

TABLE III

SHARING & STACKING SCHEME OF BLACK & WHITE PIXELS

Secret Image	Share-1	Share-2	Stacked Image
⬜	⬜⬛ ⬛⬜	⬜⬛ ⬛⬜	⬜⬛ ⬛⬜
⬛	⬜⬛ ⬛⬜	⬛⬜ ⬜⬛	⬛

5) *Visual 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 according to the scheme presented in Table IV. Therefore every block of the sharing images includes two black pixels and two color pixels. Furthermore a half-black and half-white mask are designed for each share and then combine them to get one mask which serves as a private key for decrypting the secret image. It is necessary to design separate masks for each component. If there is a colored object on a uniform background, that object can be discovered using the public share only. This can be avoided by creating separate masks. This randomizes the distribution of pixels in the public share and makes it impossible to get any clue about the secret image from the public share.

TABLE IV

DISTRIBUTION OF COLORS INTO BLOCKS IN SHARES

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)	⬛🟥 🟥⬛	⬛🟩 🟩⬛	⬛🟦 🟦⬛

If pixel P_{ij} of the halftone composed image is (0,0,0) or pure black, the shares are assigned blocks as in the first row. In RGB model, any color mixed with white color results in white color. Hence a half-black and half-white block in the final output image is obtained. In fact from the above table it can be seen that in any case the final output block contains two white and two color pixels. This in turn increases the contrast of the final output image by 50%. There are six possible combinations to construct a 2x2 black-white mask. One at a time is selected randomly and filled other pixels accordingly for better encryption.

Algorithm

Step-1: Read RGB image matrix and then store R, G, B components in three 2-dimensional matrices.

Step-2: Apply halftoning on every component (e.g. Floyd's Error Diffusion Method, Jarvis's Halftoning Method etc).

Step-3: Now choose halftone R-matrix and apply the following operations on each element of R-matrix say P(i,j) as follows:

Step-3.1: 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 ${}^4C_2 = 6$

The blocks should look like the following matrices:

$$\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline 1 & 0 \\ \hline 1 & 0 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline 0 & 1 \\ \hline 0 & 1 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 0 & 0 \\ \hline\end{array} \quad \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 1 & 1 \\ \hline\end{array}$$

Step-3.2 Determine the positions of the red pixels in Halftone R-matrix and assign the block in share-1 as described in Table IV. If R_{ij} = 1 then new_block=~mask_block

If R_{ij} = 0 then new_block=mask_block

Now add new_block to the corresponding position in share-1.

Step-4: Repeat step-3 for Green and Blue components for creating share-2 and share-3 respectively.

Step-5: After creating all the shares, combine them to get one share only. This share acts as a public key. Consider the following example:

$$\begin{array}{c}\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline\end{array} \\ \text{Share-1}\end{array} \quad \begin{array}{c}\begin{array}{|c|c|}\hline 0 & 0 \\ \hline 1 & 1 \\ \hline\end{array} \\ \text{Share-2}\end{array} \quad \begin{array}{c}\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 1 & 0 \\ \hline\end{array} \\ \text{Share-3}\end{array}$$

After combining we get a 3-dimensional array A where the elements of A are as follows:

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

Step-6: Combine all three masks to get the second share which acts as the private key. Consider the following example:

$$\begin{array}{c}\begin{array}{|c|c|}\hline 0 & 0 \\ \hline 1 & 1 \\ \hline\end{array} \\ \text{Mask-1}\end{array} \quad \begin{array}{c}\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline\end{array} \\ \text{Mask-2}\end{array} \quad \begin{array}{c}\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 0 & 0 \\ \hline\end{array} \\ \text{Mask-3}\end{array}$$

After combining we get a 3-dimensional array A where the elements of A are as follows:

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

Step-7: 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 r_1xc_1x3 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) $\{(i – 1) \times c_2 + (j – 1)\} \times 3 + r_1 \times c_1 + 100$ where r_2xc_2x3 is the size of the cover image. 100 bits are required to embed size of the secret image and other additional information (if required).

Step-8: For decryption we first extract the public share embedded in the cover image.

Step-9: Once the share has been extracted, perform bitwise or operation between each component of the share and its corresponding mask. If a pixel in the original image is Magenta, i.e. P(1,0,1) the corresponding block in the final output will be something like in Fig. 2.

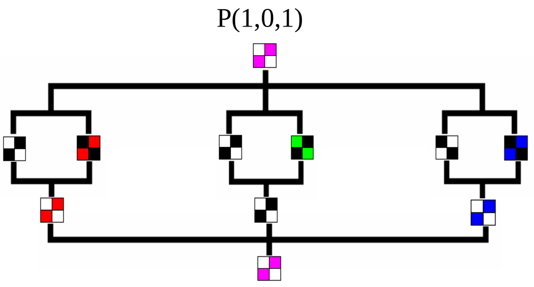


Fig. 2

Step-10: Since separate masks were used for encryption, after performing OR operation some unwanted colors may show up.

Consider the following example:

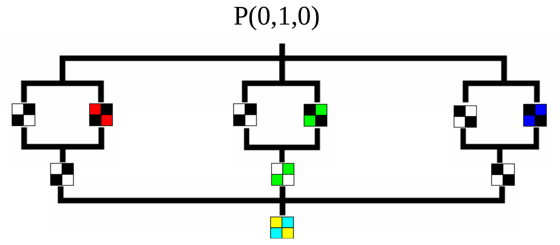


Fig. 3

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.

III. Results & Discussions

In this section some test results of the present method are illustrated. The authors have used some famous known face and also a few famous original handwritings for encryption as well as for decryption purpose.

A. *Greyscale Images*

Consider the image of Fig. 1(a). It is an 8-bit grayscale image. After halftoning we get the image of Fig. 1(b). Now grayscale visual cryptography scheme is applied to obtain the two shares (Fig. 4(a) & Fig. 4(b)).

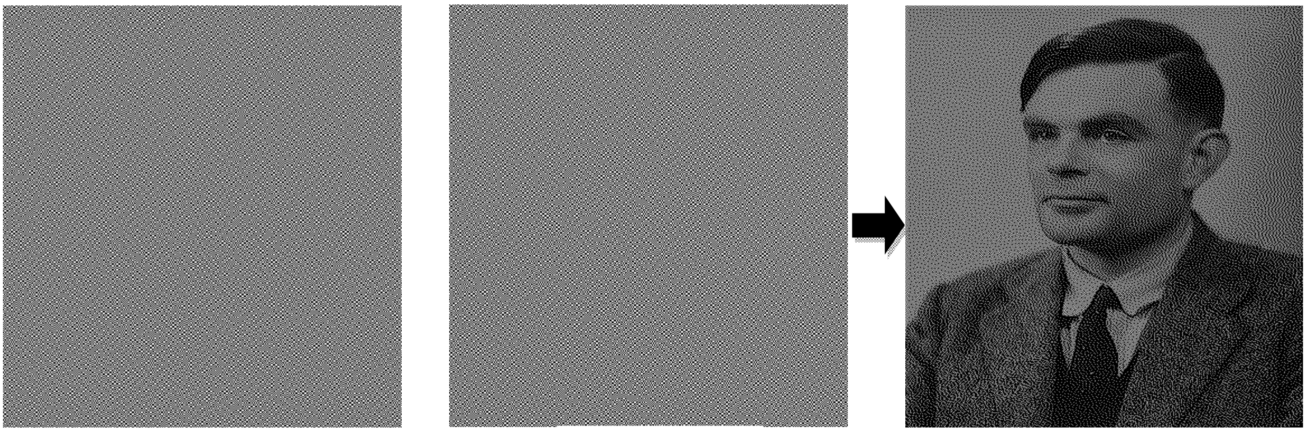


Fig. 4(a) Share-1

Fig. 4(b) Share-2

Fig. 4(c) Stacked Image

(Note: The sizes of the shares are not original but are scaled down to fit into the page)

B. *Color Images Example-1:*

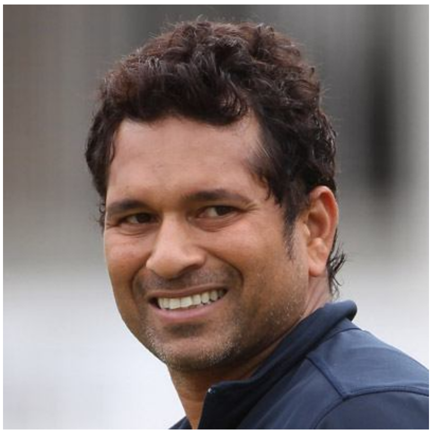


Fig. 5(a) Continuous Tone

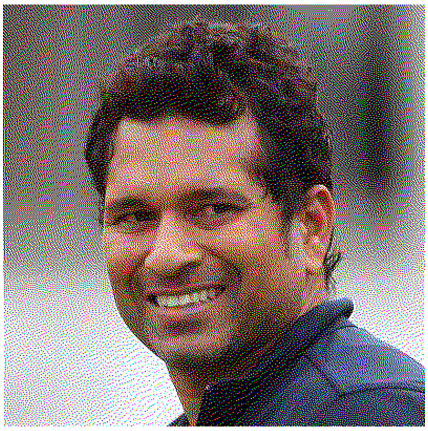


Fig. 5(b) Halftone

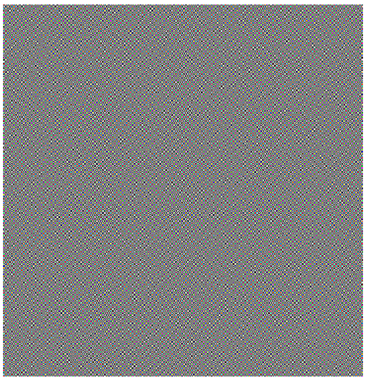


Fig. 6(a) Share-1

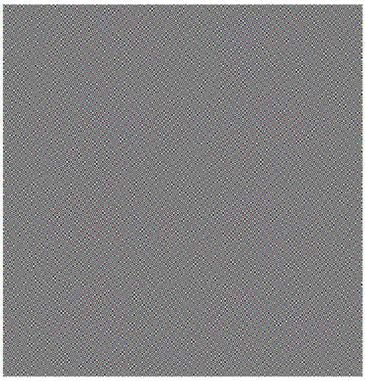


Fig. 6(b) Share-2

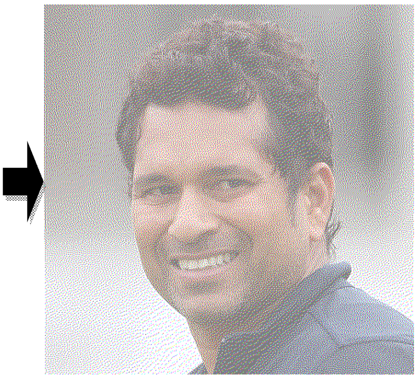
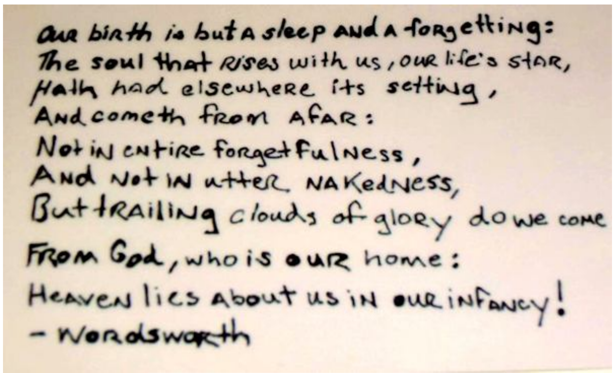


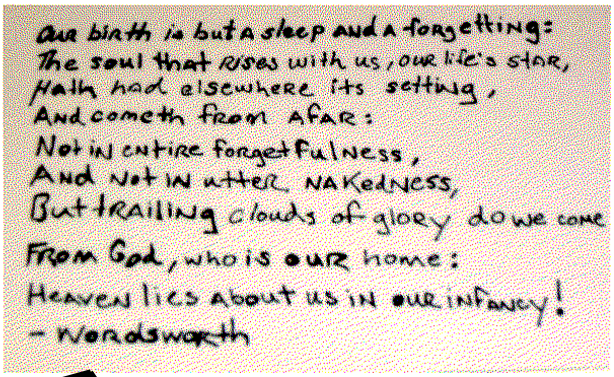
Fig. 6(c) Decrypted Image

1) *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

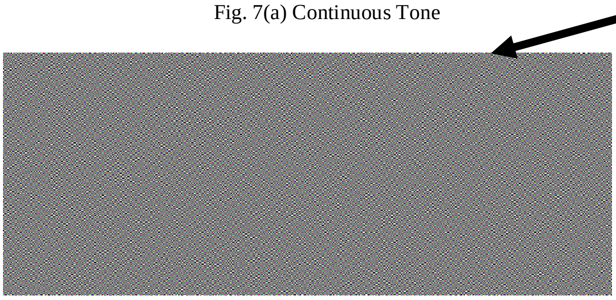


Fig. 8(a) Share-1

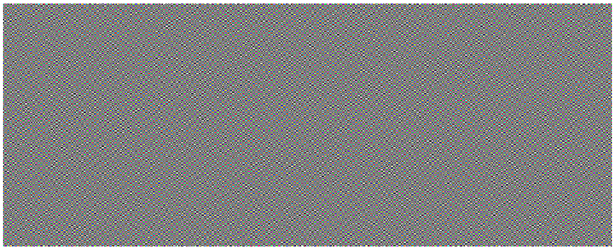
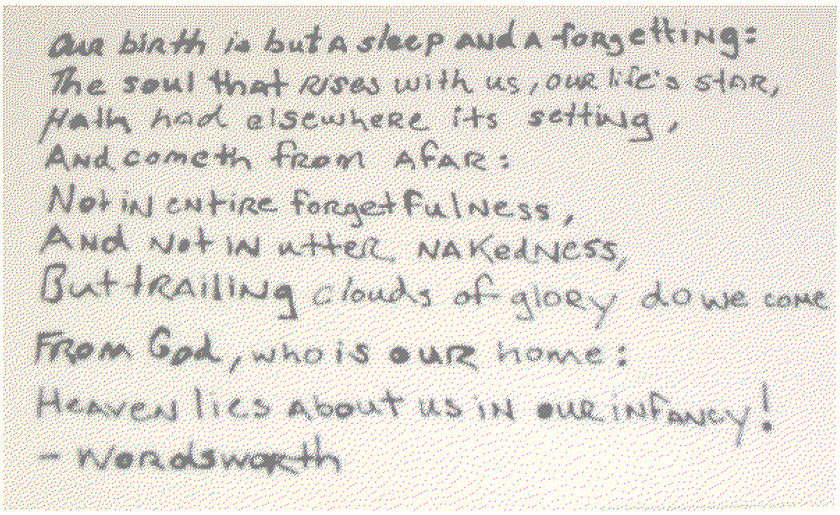


Fig. 8(b) Share-2



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

2) Example-3:

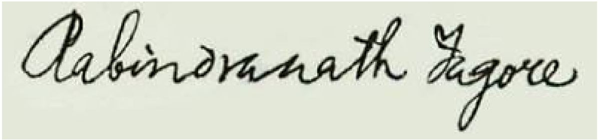


Fig. 9(a) Continuous Tone

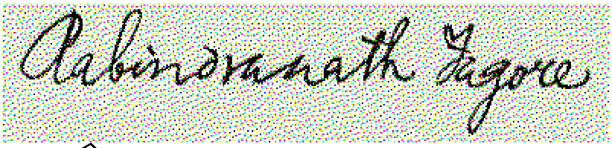


Fig 9(b) Halftone

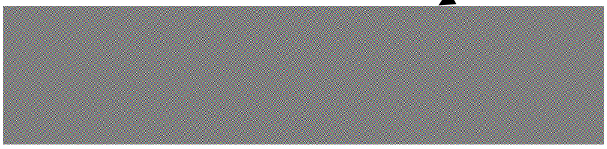


Fig. 10(a) Share-1

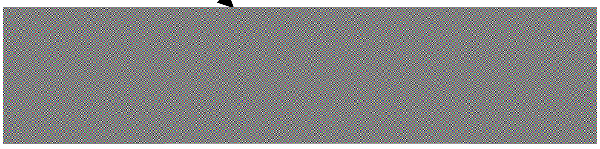


Fig. 10(b) Share-2

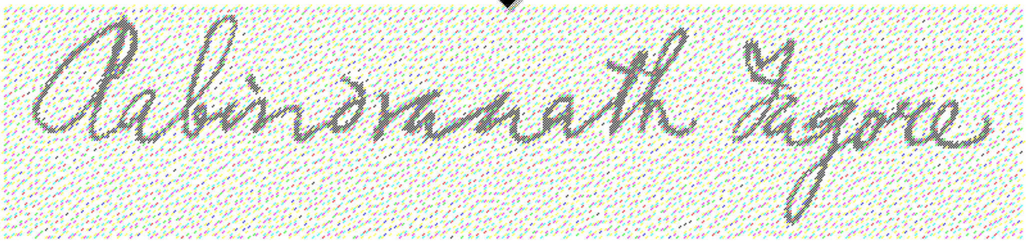


Fig. 10(c) Decrypted Image

IV. Conclusion & Future Scope

There is lot of scope in Visual cryptography for encrypting color images. The present method can be further improved by improving the contrast and to produce clearer resultant image. Visual cryptography may be further extended in encoding and decoding data in QR^{TM} code. The present method may be further extended in 3D images for creating the shares that have partial secret and reveal that secret by stacking to each other. In reality, however, such ideal color mixture is unlikely due to the properties of ink, transparencies, etc. It needs to establish a sophisticated color mixing model for the extended visual cryptography with better color quality.

Acknowledgment

The authors are very much grateful to faculty members of Department of Computer Science. One of the authors AN is extremely grateful to Dr. Fr. John Felix Raj, Principal of St. Xavier's College (Autonomous), Kolkata for inspiring all time to do research work in the department.

References

[1] 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).

[2] 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).

[3] 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).

[4] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath , A Challenge in hiding encrypted message in LSB and LSB+1 bit positions in any cover files : executable files, Microsoft office files and database files, image files, audio files and video files, JGRCS, Vol-2,No.4,Page:180-185,April (2011)

[5] Agniswar Dutta, Abhirup Kumar Sen, Sankar Das, Shalabh Agarwal and Asoke Nath : New Data Hiding Algorithm in MATLAB using Encrypted secret message: Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 262-267(2011).

[6] Joyshree Nath, Meheboob Alam Mallik , Saima Ghosh and Asoke Nath : An efficient data hiding method using encrypted secret message obtained by MSA algorithm: Proceedings of the International conference Worldcomp 2011 held at Las Vegas(USA), 18-21 Jul(2011), Page 312-318, Vol-1(2011)

[7] Rishav Ray, Jeeyan Sanyal, Tripti Das, Kaushik Goswami, Sankar Das and Asoke Nath , A new randomized data hiding algorithm with encrypted secret message using modified generalized Vernam Cipher Method: RAN-SEC algorithm, , Proceedings of IEEE International conference : World Congress WICT-2011 held at Mumbai University 11-14 Dec, 2011, Page No. 1215-1220 (2011).

[8] Rishav Ray, Jeeyan Sanyal, Debanjan Das and Asoke Nath, A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file : RJDA Algorithm, Proceedings of IEEE CSNT-2012 conference held at Rajkot May 11-13, 2012, Page:889-893(2012).

[9] Sayak Guha, Tamodeep Das, Saima Ghosh, Joyshree Nath, Sankar Das, Asoke Nath, A new data hiding algorithm with encrypted secret message using TTJSA symmetric key crypto system, Journal of Global Research in Computer Science, Vol 3, No.4, Page-11-16(2012).

[10] Joyshree Nath, Saima Ghosh and Asoke Nath,, Advanced Digital Steganography using Encrypted Secret Message and Encrypted Embedded Cover File, International Journal of Computer Applications(IJCA 0975-8887), Vol 46, No-14, May ,(2012).

[11] Somdip dey, Kalyan Mondal, Joyshree Nath, Asoke Nath, Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded with Any Encrypted Secret Message : ASA_QR Algorithm International Journal of Modern Education and Computer Science, No.6, Page 59-67, 2012.

[12] Joyshree Nath, Saima Ghosh and Asoke Nath, Data hiding algorithm using two-way encryption and embedding in a cover file – A new method for sending password or confidential message. Proceedings of International Conference World comp 2012 held at Las Vegas, USA, IPCV-12, Page-414 – 420(2012).

[13] Somdip Dey, Joyshree Nath and Asoke Nath, A New Technique to Hide Encrypted Data in QR Codes^{TM}, Proceedings of International Conference Worldcomp 2012 held at Las Vegas, USA, ICOMP-12, Page-94 – 101(2012).

[14] 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.

[15] 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 Computer Science, Vol. 1189, Springer, Berlin, 1997, pp. 197–202.

[16] D.R. Stinson, An introduction to visual cryptography, presented at Public Key Solutions ’97, Toronto, Canada, April28–30, 1997.

[17] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform.Comput.129 (1996) 86–106.

[18] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended schemes for visual cryptography.

[19] C. Blundo, A. De Santis, D.R. Stinson, On the contrast invisual cryptography schemes. J. Cryptology, Vol. 12, 1999, 261–289.

[20] M. Naor, B. Pinkas, Visual authentication and identification, in: B. Kaliski, Jr. (Ed.), Advances in Cryptology—CRYPTO’97, Lecture Notes in Computer Science, Vol. 1294,Springer, Berlin, 1997, pp. 322–336.

[21] V. Rijmen, B. Preneel, Efficient color visual encryption forshared colors of Benetton, Eurocrypto’96, Rump Session,Berlin, 1996.

[22] A. D. Rubin, Independent one-time passwords, Computer Systems9 (1996) 15–27.

[23] A. Shamir, Visual cryptanalysis, Proceedings of the Eurocrypt’98, Espoo, 1998.

[24] C.A. Poynton, Frequently asked questions about color, http://www.inforamp.net/~poynton.

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

[26] Y.C. Hou, F. Lin, C.Y. Chang, Improvement and implementation of the secret color image sharing technique, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 592–597.

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

[28] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November1999, pp. 584–591.