ISSN 2278-3091
Volume 6, No.4, July - August 2017
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01642017.pdf

A Robust Visual Cryptography Scheme for Imperceptible Distribution of Secret Message without Pixel Expansion

Kalyan Das [1], Aromita Sen [2], Samir Kr. Bandhopadhyay [3]
[1]Information Technology, St. Thomas' College of Engg and Technology
[2]Computer Science & Engineering, St. Thomas' College of Engg and Technology
[3]Computer Science and Engineering, University of Calcutta

ABSTRACT

The high speed advancement of Computer network and internet has hiked the chance of data snooped during the time of transmission. In this issue, Cryptography plays a vital role, which hides the actual information using some secret key and thereby converts it into an alternative equivalent multimedia file like image, video or audio in such a way that only the intended recipient can retrieve back the original data. To achieve that goal the secret image has been divided into several shares and distributed among individuals in such a way that only when all the shares has been combined, the original secret image can be revealed. Here in this paper, a novel visual secret sharing technique has been suggested, which uses the pixel intensity adjustment function and basic binary operations, ensuring the confidentiality and integrity of the transmitted data. The proposed scheme has advantage of being very time efficient and also able to hide more secret information providing higher imperceptibility.

Key Words: Visual Cryptographic System, Modified LSBR, Secret Sharing, Pixel Expansion, Intensity adjustment, Visual distortion, Steganography, Security through obscurity

1. INTRODUCTION

A sender always wants to send a message in a secured way to the intended receiver. Cryptography is the art and science of achieving security by encoding messages(e.g. printed text, handwritten notes, and picture) in such a way, that decipher can be performed by an authorized user with the help of human visual system (HVS) without any complex process. It also provides high security, so that hackers cannot observe any clues about a secret image from individual cover images. To deal with the security problems of secret images, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography which would require less computation and less storage.

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, gray or color) and number of secret images(either single or multiple) encrypted by the scheme.

The basic model of Visual Cryptography was introduced by Naor and Shamir [5] in 1994 accepts binary image I(x, y) as secret image, which is divided into 'n' number of shares. Each pixel of image I(x, y) is represented by 'm' black and white sub pixels in each of the 'n' shared images. Naor and Shamir proposed a k out of n scheme and assumed that the image or message is a collection of binary data 0 and 1displayed as black and white pixels. According to their algorithm, the secret image is turned into n shares and the secret is revealed if any k of them are stacked together. So the image remains hidden if less than k shares are stacked. Decryption is achieved by stacking the shares and thus introduces noise. It is impossible to get any information about the secret images from individual shares. But the main disadvantage is, if someone get all the shares he/she can easily retrieve the secret message by stacking the shares.

The first form of visual cryptography is also known as secret sharing. The simplest form of visual cryptography separates a secret image into two parts so that either part by itself conveys no information. When these two parts are combined together by means of superimposition, the original secret can be revealed. These parts are called as shares. There are several advantages of visual cryptography. Basically it is simple to use and no mathematical computations are required to reveal the secret. Secondly, the individuals who do not have knowledge of cryptography are indirectly getting involved in decryption.

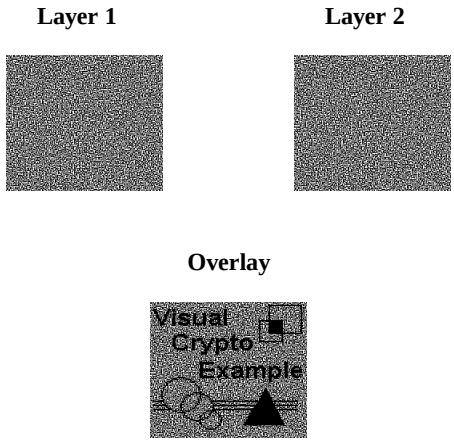

Figure1: Example of traditional (2, 2)-VCS with image size 128x128.

We can achieve this by one of the following access structure schemes.

- (2, 2)- Threshold VCS scheme- This is the simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.
- (n, n) -Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when all n of the shares are combined will the secret image be revealed.
- (k, n) Threshold VCS scheme- This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

Here our proposed scheme provides a visual cryptography scheme that is time-efficient and has high capacity to hide the secret information with higher imperceptibility.

This paper is organized as follows. In Sect 2, the related ideas to this problem are discussed. In Sect 3 the preliminaries dealing with the basic concepts are discussed. Sect 4 describes about the proposed method along with the methodology mentioned in Sect 5. Sect 6-7 deals with the implementation Details and the result generated. At the conclusion is written in Sect 8 followed by the References.

2. PRELIMINARIES

2.1 Image: Digital images are of three different types- binary, grayscale and color image. Binary images consist of only two different colors black and white, which are represented using 0 and 1. In grayscale image each pixel is represented in 8bpp format where intensity values starts from 0 to 255 representing black and white and the intermediate values represents different shades of gray.

In additive model or RGB model, every color image is composed of pixels where each pixel is a series of bits composed of RGB values with 24bit depth. 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.

2.2 Input Image: Both the grayscale and color images are used as input image in this scheme. Here a grayscale image is represented as a square matrix M with dimensions as RXC, where R & C denotes the row and column count of the matrix respectively. Each element in the matrix denotes a pixel in the image.

$M=[m_{i,j}]_{RXC}$ where i={1,2,3,……..,R} and j={1,2,3,……,C}

Here $m_{(i,j)}$denotes the intensity value of the pixel at position (i,j) and the value lies within 0 to 255.

For color image each of the RGB (R=red, G=green, B=blue) layer is represented using different matrices of same size e.g. MR, MG and MB.

$R=[MR_{i,j}]_{RXC}$ $G=[MG_{i,j}]_{RXC}$ $B=[MB_{i,j}]_{RXC}$

Here we have used Grayscale images and Color images for the experimental purpose.

2.3 Output Image: Here the output images are the secret shares S1,S2,S3….Sn where each of the share is a meaningful image of the same size and same type as of the corresponding input image.

2.4 Bitwise Operator: Here for mathematical computation purpose bitwise operators has been used, which are OR, AND and Exclusive OR operations. The respective mathematical functions are as follows:

AND: $i \wedge j == -1 - ((-1 - i) | (-1 - j))$ ..(Eq. 1)
OR: $i | j == -1 - ((-1 - i) \wedge (-1 - j))$ ..(Eq. 2)
XOR: $i \oplus j == (i | j) \wedge (-1 - (i \wedge j))$ ..(Eq. 3)

3. LITERATURE SURVEY

Many authors have published different Visual Cryptography Schemes for different applications. Each scheme has its own advantages and disadvantages. Few such schemes are mentioned below.

A. BLACK and WHITE VISUAL CRYPTOGRAPHY SCHEME

a) Single Secret Sharing Scheme

The concept of visual cryptography was first proposed by Naor and Shamir [5] in 1994. Naor and Shamir proposed a k out of n scheme where for a given message, n transparencies will be generated and it is impossible to get any information about the secret images from individual shares. The original message is visible if any k (or more) of them are stacked together, but totally invisible if fewer than k transparencies are stacked together (or analyzed by any other method).

The original encryption problem can be considered as a 2 out of 2 secret sharing problem. In (2, 2) Visual Cryptography Scheme each pixel P is split into two pixel in each of the two shares (each such pixel in the shares is called sub pixel) by following any one row of the corresponding pixie in Figure 1. If P is white, then a row is chosen randomly from one of the first two rows in the Figure 1. If P is black, then a row is chosen randomly from one of the last two rows in the Figure 2.

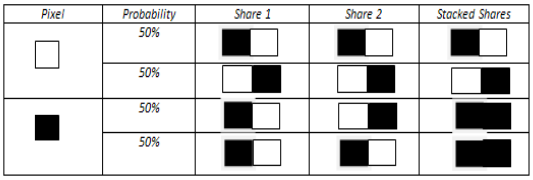

Figure2. Naor and Shamir's scheme for encoding a binary pixel into two shares

Now when two shares are superimposed the black pixels in the secret image we will get two black pixels whereas the white pixels will result in one white and one black pixel as shown in the last column of Figure1. Thus we can say that in this particular case the reconstructed pixel has grey level of 1 if P is black and a grey level of 1/2 if P is white. The advantage of the above scheme is that the decoding can be performed without any cryptographic computations in a simple way. But it lacks in balancing the contrast of the decoded image with respect to the original one, so the recovered image can't be reused.

Fig 3a. Original Image

Fig 3b. Share1

Fig 3c. Share 2

Fig 3d. Output of the Superimposed Shares

Figure3. Illustration of a 2-out-of-2 VCS scheme with 2-subpixel construction

b) Multiple Secrets Sharing Scheme

All the previous researches in visual cryptography, only one image can be secured at a time. Wu and Chen [6] were first researchers to present the visual cryptography schemes to share two secret images in two shares. In this scheme, two secret binary images can be hidden into two random shares. They are denoted as A and B. By stacking the two shares can be seen in the first secret denoted by A⊗ B. For rotating A by Θ anti-clockwise the second secret can be obtained. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦.

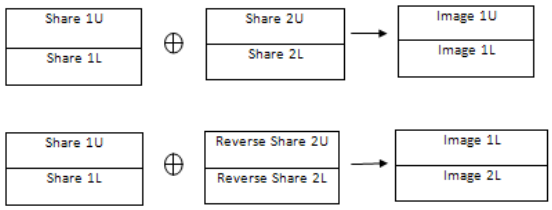

Figure4. Block diagram of the scheme suggested by Wu and Chen

To overcome the angle restriction of Wu and Chen's scheme, Hsu et al [7] proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles.

Wu and Chang [8] also refined the idea of Wu and Chen [6] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed.

B. COLOR IMAGE SHARING SCHEMES

a**) Single Secret Sharing**

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [9]. Colored secret images can be shared with the concept of arcs to construct a colored visual cryptography scheme. In the c-colorful visual cryptography scheme one pixel is transformed into the m sub pixels, and each sub pixel is divided into the c color regions. In each and every sub pixel, there is exactly one color region is colored, and all the other color regions are black. The color of one pixel depends on the inter relationships between the stack sub pixels. In this colored visual cryptography scheme with c colors, the pixel expansion m is c*3.

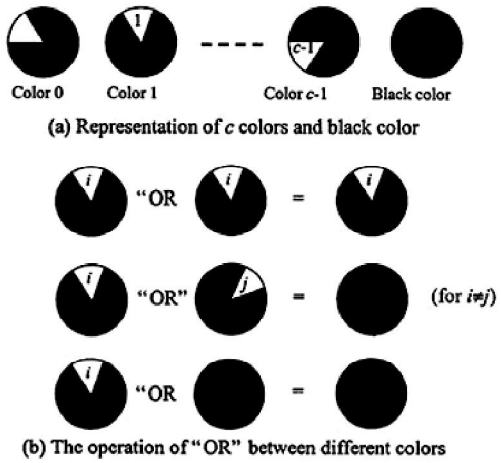

Figure5. Infrastructure of colored subpixels and its OR operations in Verheul-Van Tilborg Scheme

Yang and Laih [10] proposed a scheme which improves the pixel expansion to c*2. The scheme was implemented on basis of a black & white VSS scheme and got much better block length than the Verheul-Van Tilborg scheme .But in both of these schemes share generated were meaningless.

For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai [11] anticipated color visual cryptography scheme. For a secret color image two effective color images are chosen as cover images which are the exactly same size of the secret color image. Then according to a predefined Color Index Table, the secret color image will be concealed into two disguise images. In this scheme also number of sub pixels is in proportional to the number of colors in the secret image as in the previous schemes. The only disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

b) **Multiple Secrets Sharing Scheme**

Tzung-Her Chen et al [12] anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional (2,2) VSS is used to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

In this paper, a new share generation technique is proposed which generates meaningful shares and gives a better result compared to the information density of the previous well known algorithms and also 100% retrieval of the secret image, without any pixel expansion.The proposed method is flexible enough to be applied on Grayscale as well as Color Secret Images.

4. PROPOSED METHOD

Most of the secret sharing scheme is based on the concept of dividing a pixel into subpixels and thus causing pixel expansion, which not only increases the storage requirement but also degrades the quality of the retrieved image.

All those schemes generating meaningless shares may suffer from transmission risk problem because holding noise like shares will cause hacker's suspicion and share may be intercepted. To fill upthis security gap, in our proposed scheme consider security of image in terms of using cover images and generate meaningful shares.

Here the flowchart of the proposed method is given below:

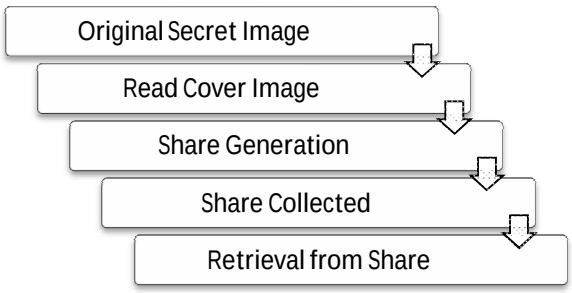

Figure6. Block Diagram of the Proposed Scheme

Here the original secret grayscale image has been partitioned into 3 different parts and then each part is been hidden into 3 different meaningful Grayscale Cover Images which has been taken as input. The number of shares generated may be controlled as per the quality requirement of the decrypted image.

For 100% retrieval we need atmost 3 cover images for hiding a grayscale image. Accordingly a number of shares will be generated in case of color images i.e. maximum 6 grayscale shares or 3 color shares. For black-white image only one cover is sufficient.

The image steganography technique takes the advantage of limited power of human visual system (HVS). It uses image as cover media for embedding secret message.

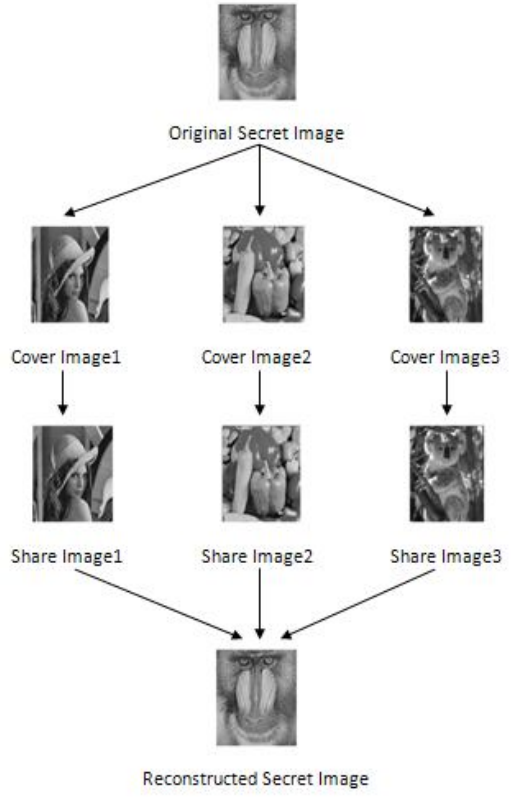

Figure7. Share Generation using the proposed method

5. METHODOLOGY

Let, the secret image is a grayscale image M of size R*C. For each pixel $m_{(i,j)} \in M_{(R*C)}$ divide the intensity value into three bit streams named B_1, B_2 and B_3 where $B_1B_2B_3$ ->$m_{(i,\ j)}$. Here the original secret image pixels (8 bpp) have been divided in 3:3:2 ratio.

Now take three meaningful grayscale cover image of same size as of the secret image, as inputnamed C_1, C_2 and C_3, which will be used to hide the information B_1, B_2 and B_3 respectively.

C_1: image for share 1
C_2: image for share 2
C_3: image for share 3

For each binary stream, depending on the value in the LSB i.e. 0 or 1, a higher bit of the respective pixel in the cover image will be modified and then the pixel adjustment will be performed in the following manner.

Table1. Bit Level Operations Performed

Sl. No.	Replacement Criterion	Operation performed
1	c=0 && b=0	No Change
2	c=0 && b=1	Set all lower bits in the cover image to 0
3	c=1 && b=0	Set all lower bits in the cover image to 1
4	c=1 && b=1	No Change

Here c and b denotes the cover image bit and the binary stream bit of the secret image respectively.

If the information is been hidden by only using replacement rule, then that would have created much disturbance in the cover image and that will cause a chance for the intruder to intercept the presence of the secret information. For that reason pixel intensity adjustment method has been applied to reduce the error.

The higher order bits with respect to the bit replaced in the cover image, remain unchanged.
For all c_i where $i<n$ (n^{th} bit is used for the replacement, chosen as the optimized solution regarding less visual disturbance)

$$r_i == c_i \quad \text{…… (Eq. 4)}$$

and

$$r_n == b \quad \text{…… (Eq. 5)}$$

where r denotes the resultant matrix after performing the proposed operations, which is of the same size of the input cover image.

And for other lower order remaining bits the following function will be used ---

For all i>n,

$r_i = ((\sim(c \oplus b)) \wedge c_i) + ((c \oplus b) \wedge (\sim b))$ …..(Eq. 6)

So the resultant mathematical representation of the proposed algorithm is-

$$ri = f(c,b) = \begin{cases} ci & i < n \\ b & i = n \\ (\sim(c \oplus b))\wedge ci + (c \oplus b)\wedge(\sim b) & i > n \end{cases}$$ …… (Eq. 7)

r: Output Intensity
b and c denotes the corresponding secret bit and the n^{th} bit in the cover image.

After performing the suggested steps, now the remaining higher order bits present in the bit stream, will perform simple mathematical operation, with the lower order bits of the corresponding cover image.

Let $b_3b_2b_1$ denotes the bit stream Bi of a pixel in the secret image and $c_8c_7c_6\ldots c_2c_1$ denotes the pixel intensity value of the corresponding pixel in a cover image.

$r_8r_7r_6\ldots.r_2r_1 = c_8c_7c_6\ldots c_2c_1 \oplus b_3b_2$ …… (Eq. 8)

Where $c_8, c_7, c_6, \ldots c_2, c_1, b_3, b_2, b_1 \in \{0,1\}$

Thus in each pixel in the Cover Image maximum 3bit information of the corresponding pixel in the Secret Image (8 bpp) is been hidden without any visible distortion, maintaining the quality of the cover image. Here by generating 3 shares for the Grayscale Secret Image.

For the Color Secret Image, in each pixel in the Cover Images maximum 9bit of the corresponding pixel in the Secret Image (24bpp) has been successfully hidden in the similar process, where each layer in the Cover Image (R, G and B layer) was holding maximum of 3bit information.

6. RESULT AND DISCUSSION

6.1 Experimental Results

This section presents the simulation results illustrating the performance of the proposed Method. The above mentioned scheme is implemented into "MATLAB R2009a and IrfanView have been used as the basic image editing software. In this process we have taken some well-known benchmark images for the experimental purpose. Then the Original Secret Images has been operated using the proposed method and then the generated shares are used to retrieve back the original image. The retrieved image is exactly of the same size & having the same quality as of the Original Secret Image. The same method can be applied on grayscale as well as on color images providing good quality result. After testing on many different images the results are as our expectation and the shares are clear without any visual abnormality.

6.2 Performance Analysis

The following section shows various performance metrics considered to demonstrate the quality of generated shares. The two main parameters considered are the PSNR (Peak Signal to Noise Ration) and MSE (Mean Square Error), for measuring the quality between two images.
In PSNR quality measurement one of the images are compared provided the other image is regarded as of perfect quality. The formulae used are given below:

$$MSE = \frac{1}{N*M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2$$ …… (Eq. 9)

$$PSNR = \log_{10}\left(\frac{Imax^2}{MSE}\right)$$ ….. (Eq. 10)

[X is the original image and Y is the output image; I is the dynamic range of pixel values normally 255; (M, N) are the dimensions of the image]

The quality measures are calculated between the original image and retrieved image along with the execution time. Table2 shows the quality measures of the images after encryption / decryption process.

Table2. PSNR and MSE values for various test cases

Image(s)	MSE values	PSNR index for Grayscale Secret	MSE values	PSNR index for Color Secret
Original Secret Image	0	inf	0	inf
Cover Image 1	0	inf	0	inf
Cover Image 2	0	inf	0	inf
Cover Image 3	0	inf	0	inf
Share Generated 1 (w.r.t Cover1)	10.7313	37.8243	{3.5871, 3.5865, 3.6098}	{42.5834, 42.5841, 42.5560}
Share Generated 2 (w.r.t Cover2)	10.4698	37.9314	{3.4403, 3.6337, 3.6491}	{42.7648, 42.5273, 42.5090}
Share Generated 3 (w.r.t Cover2)	2.4923	44.1648	{0.8349, 0.8299, 0.8381}	{48.9142, 48.9405, 48.8981}
Retrieved from Shares	0	inf	0	inf

Table3. Comparative result of the proposed and the existing method

Authors Year	Pixel Expansion (m)	No. of Secret Images	Image Format	Type of Share generated
Naor and Shamir [5] 1995	4	1	Binary	Random
Wu and Chen [6] 1998	4	2	Binary	Random
Hsu et al [7] 2004	4	2	Binary	Random
Wu and Chang [8] 2005	4	2	Binary	Random
E. Verheuland [9] 1997	C*3	1	color	Random
Yang and Liah [10] 2000	C*2	1	Color	Random
Chang and Tsai [11] 2000	C*2	1	Color	Meaningful
Tzung-Her Chen et al [12] 2008	4	2	Gray	Random
Proposed Method	1	1	Gray, Color	Meaningful

6.3 Comparative Analysis

A. Visual Quality Comparison

Fig8 and Fig9 show the Original image, and its generated shares along with respective cover images. Theproposed algorithm works for the graycode model along with color code models. Theproposed method yields, perfect share generation as wellas ends in good reconstruction of the secret images with theirdesired quality.By implementation of the proposed algorithm, the userneed not pre-process the image that degrades the visualquality. The generated shares do not differ much from the cover images, avoiding visual distortion. Hence, thesecurity of the data is considerably increased.In our proposed algorithm the original secret image can be retrieved in totality without any data loss. Thefollowing table shows a comparative analysis of theproposed method with existing methods.

Figure8. Share Generation of a Grayscale Secret Image

Figure9. Share Generation of a Grayscale Secret Image

B. Performance Based Comparison

The values in table3 give the performance evaluation with respect to the required execution time for different set of data. The time required can be represented using the following expression-

$$t = O(r * c * bpp) \quad \text{…… (Eq. 11)}$$

t : time
[rc] : dimension of the input data set
bpp: bit depth

Table4. Details of the Benchmark Images used in the experiment and its execution time

Image	Size	Type	Execution Time
monalisa.jpg	256*256	Color	-
satellite.jpg	256*256	Color (Secret Image)	1.092478 seconds
			1.011067 seconds
			0.324485 seconds
peppers.jpg	256*256	Color	-
koala.jpg	256*256	Color	-
Lena.bmp	256*256	Grayscale	-
Mandrill.png	256*256	Grayscale (Secret Image)	0.297684 seconds
			0.307329 seconds
			0.094087 seconds
Koala.jpg	256*256	Grayscale	-
Pepper.png	256*256	Grayscale	-

7. CONCLUSION AND FUTURE WORK

As conclusion it can be said that; visual information where size and security is more concerned, the proposed visual sharing scheme is undoubtedly fine and fantastic to use and it has a simple, lossless implementation module. This visual sharing procedure is totally new and can't be disguised easily by the intruder as it don't effects the base(cover) image that much as the message is hidden as a part of it. So from the shares generated there is no chance of any visual disturbance. It is already confirmed that proposed method gives a lossless way of cryptography where the generated shares are meaningful images and has been able to hide a high amount of information with higher imperceptibility.

There is no pixel expansion and hence storage requirement per encrypted image is same as original image without pixel expansion. The quality of the image recovered is same as the original image. The same technique can be used on color or gray scale images also without any change in the algorithm. The proposed method is simple enough and thus requiring less time for the share generation and the regeneration of the original secret. Our future work would be to suggest some more secure algorithm providing greater level of hiding in the area of visual sharing.

8. REFERENCES

[1] Amit B. Chougule, NilamNisar Shaikh, '**A Secure Keyless Colored Image Encryption'**, International Journal of Advanced Technology in Engineering and Science ,Volume No.02, Issue No. 12, December 2014 ISSN (online): 2348 – 7550

[2] P.S.Revenkar, AnisaAnjum, W .Z.Gandhare, "**Survey of Visual Cryptography Schemes**", International Journal of Security and Its Applications,Vol. 4, No. 2, April, 2010

[3] ShyamalenduKandar, Arnab Maiti, Bibhas Chandra Dhara, "**Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking**", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011, ISSN (Online): 1694-0814

[4] RenuPoriye, Dr S. S Tyagi, "**Secret Sharing Using Visual Cryptography**", 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)

[5] Moni Naor and Adi Shamir, "**Visual Cryptography**", advances in cryptology–Eurocrypt, 1995, pp 1-12

[6] C.C. Wu, L.H. Chen, "**A Study On Visual Cryptography**", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998

[7] H. C. Hsu, T.S.Chen, Y.H.Lin, "**The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing**", In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 2004, pp. 996–1001

[8] H.-C.Wu, C.-C.Chang, "**Sharing Visual Multi-Secrets Using Circle Shares**", Comput. Stand. Interfaces 134 (28), pp.123–135, (2005)

[9] E. Verheuland H. V. Tilborg, "**Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes**.", Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.

[10] C. Yang and C. Laih, "**New Colored Visual Secret Sharing Schemes**", Designs, Codes and cryptography, 20, 2000, pp. 325–335

[11] C. Chang, C. Tsai, and T. Chen. "**A New Scheme for Sharing Secret Color Images in Computer Network**", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000

[12] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "**Multi-Secrets Visual Secret Sharing**", Proceedings of APCC2008, IEICE, 2008

[13] M.Karolin1, Dr.T.Meyyapan, "**RGB Based Secret Sharing Scheme in Color Visual Cryptography**", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[14] Mousumi Ghanti, Prof. Samir Kumar Bandyopadhyay, "**A Proposed Method for Cryptography using Random Key and Rotation of Text**", hanti et al., International Journal of Advanced Trends in Computer Science and Engineering, 6(2), March - April 2017, 18

[15] Kshyamasagar Mahanta, Hima Bindu Maringanti, "**An enhanced Advanced Encryption Standard Algorithm**", International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 28 - 33