ISSN 2278-3091
Volume 10, No.4, July - August 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse031042021.pdf
https://doi.org/10.30534/ijatcse/2021/031042021

A Secure and Verifiable Color Visual Cryptography Scheme with LSB Based Image Steganography

D. R. Somwanshi[1], Dr. Vikas T. Humbe[2]
[1] Department of Computer Science, College of Computer Science and Information Technology (COCSIT) Latur, Maharashtra, India, somwanshi1234@gmail.com
[2]School of Technology, Swami Ramanand Teerth Marathwada University Nanded, Sub-CenterLatur, Maharashtra, India, vikashumbe@gmail.com

ABSTRACT

A secure and verifiable color visual cryptography has becoming an important field of study in recent development of visual cryptography. In recent era there is a need of security and verifiability of shares.This research paper introduce the new secure and verifiable color secrete sharing scheme which identifies and analyses cheating while presenting the share. Integrity and reliability of share is identified before superimposition of share to revel the original secrete image. Secrete and verification image of size n x n are used for creating two shares then created shares are embedded into two cover images using LSB (Least Significant Bit) based stenography to create the meaningful and stenographic shares. Color channel decomposition and Jarvis half toning method is applied on each color channel of RGB secrete and verification image for creation of shares. Method proposed eliminates the problem such as explicit requirement of codebook design, pixel expansion, and poor visual quality of reconstructed images. Structural Similarity(SS) and Mean Square Error(MSE) measures of original verification image with revealed verification image verifies the soundness and originality of the secrete. The method also compares the result with previously proposed method; experimental results and statistical analysis are used to prove the efficiency of the method proposed.

Key words: Color Half-tone Images, Verification image, Least Significant Bit Stenography Stenographic shares,Pixel Expansion, optimal contrast, Secure and verifiable Secrete Sharing.

1. INTRODUCTION

Color visual cryptography scheme is a technique of encrypting or sharing color visual secretes information such as images, written materials, handwritten notes, drawing etc. in a perfectly secure way. In general secrete sharing scheme the secret information that is to be secure from unauthorized access is divided into *n* numbers of parts or shares. Then each part or share is distributed among *n* participant or user of the information. To recover the secret information, all the *n* numbers of participant or we can specify any *k* out of *n* numbers of participant have to provide their share. Provided shares are superimposed together to reconstruct the original secret information. The most important characteristics of secrete sharing scheme is that staking, superimposition of shares or decryption of shares and getting the secret information from the shares is performed by human visual system without any computation, only the computation is required for creation of shares or encryption of secret information [1]-[4].

The idea of visual cryptography scheme is presented as below in figure 1. The secret image is divided into two components share and superimposition of shares return original secret image.

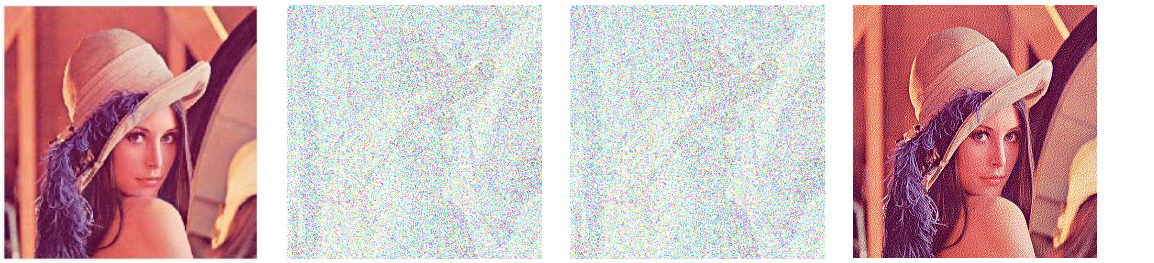


Figure 1: Idea of Visual Cryptography

While creating and combining the shares some problems such as pixel expansion, alignment problem, flipping Issues, and share distortion, cheating of shares may arise [5], [6]. In pixel expansion numbers of pixel in share are increased, due to that size of share increases and alignment problems may occurs. Due to alignment problems combined secrete image looks different. If image is not superimposed in proper direction flipping issue may arise. With this most of past secret sharing scheme presented are based on binary images and very few of them are based gray and color images. Again in case of cheating issue one of the dishonest participants of secrete sharing scheme may tamper or damage the shares, therefore the secrete recovery process will generate the unambiguous resultant image means the secrete recovery is negotiated and that is not accepted. Sometimes the dealer who creates shares for distribution among the participant may create the inaccurate shares. While designing the scheme of secretes sharing, one should aware of these attacks because cheating problem may be the important issue. Most of the scheme developed in the past creates additional shares or authentication shares only for verification purpose which requires additional overheads. Wang et.al [12] proposed such (2,2) secret sharing scheme but the scheme is time consuming and share generated by this scheme are meaningless**.** If the shares are meaningless it may create doubt that, something is hidden inside the image**.** Also most of the past developed scheme only operates the binary and gray level image. In this paper color image processing with verification image for verification of shares and creation of meaningful share with the help of LSB based steganography are handled efficiently.Color components decomposition and half-toning technique is applied on both secrete image and verification image. The scheme proposed also verifies the accuracy or integrity on the secrete image before the recovery based on the SS (Structural Similarity) and MSE (Mean Square Error) of the recovered image and with verification image Method proposed also eliminated the entire problem discussed above.

2. RELATED WORK

Naor and Shamir generalized basic secrete sharing scheme into k out of n visual cryptography scheme [1]. In *k* out of *n* visual cryptography scheme, *n* shares of the original image are generated and given to *n* participant. Minimum *k* of those *n* participant have to provide theirs share for reveling the secrete image. Contrast of the recovered image is poor and pixel expansion is double in this scheme.

To provide the security to this scheme, G. Ateniese et al. further modified *(k, n)* model to general access structure model of visual cryptography [7]. According to them number of share *n*, created are divided into two parts or subsets as per the importance and need. First part of the subset is called qualified subset and second is forbidden subset. Any *k* shares from qualified subset can recover the secret image. From the forbidden set *k* or more shares cannot recover the secret image. AbhishekParakh et.al.proposed "Recursive threshold visual cryptography" [8]. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to *(n-1)/n* bit of secret which is nearly *100%*again to maintain the good contrast and improve the security, Zhi Zhou, et.al. proposed halftone visual cryptography [4], [9].In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the *n* shares. Mahmoud E. Hodeish et.al proposed an optimized half tone visual cryptography using error diffusion. They works on binary and gray scale image and improves the pixel expansion, elements the code book requirement but they only works on binary half tone images[6]. Mahmoud E. Hodeish et.al proposed a new efficient TKHC-based image sharing scheme over unsecured channel they proposed the method of RGB and gray scale images encrypted and decrypted by means of TKHC and providing strong security to transmit all the generated shares via one public channel [9]. Chang-Chou Lin et.al.proposed visual cryptography for gray level images [10]. The scheme uses the dithering technique for conversion of gray level image into approximate binary image. Then they have applied existing Visual cryptography schemes for binary images to create the shares. To reduces the pixel expansion F.Liu, etal. proposed a new approach for colored visual cryptography scheme [11]. They proposed three different approaches for color image representation in which they separate three color channels Red, green and blue. Any one channel can be used in half toning process but quality of image gets degraded due to half-toning process. Wang et al. [12] proposed the Sharing a Secret Image in Binary Images with Verification. In this scheme, it is difficult to manage and process the meaningless shares and it also consumes time to scramble the images.Kalyan Das et al. [21] suggested a novel visual secret sharing technique that is based on pixel intensity adjustment function and some basic binary operations for providing the confidentiality and integrity of the transmitted visual image. The scheme proposed by them provides time efficient solution.

Some of the verifiable and securevisual cryptography schemes developed recently allow the user to authenticate only the shares received by them instead of revealed image, but most of them have the problem such as lessrevealing

quality, pixel expansion, complexity in computational, accuracy and security of the image.

3. PRELIMINARY CONCEPTS

In this section essential concepts necessary for the proposed scheme is discussed

3.1. Color channel decomposition techniques

This paper uses RGB color model, secret RGB image to encrypt is decomposed into R, G and B component image. Four shares of each components image are created and finally shares are concatenated to form RGB shares.

3.2. HVC scheme and Error Diffusion:

The proposed scheme convert each components image into half-tone image, Half tone is atype of image which is made up of a series of dots instead of continuous tone, these dots can be of varying size, shape and color. Smaller dots are used to represent lighter area of image and larger dots are used to represents more dense area in the image. Such scheme of visual cryptography is called Half- tone Visual Cryptography (HVC) [4].

Each color components image represented here can be a separate gray level image. Error diffusion is a technique of converting gray level image (color components image) to binary image form in such a way that picture in binary image form looks similar to gray level image with somewhat better quality image.This is the efficiency and simplicity of binary image. The process of error diffusion diffuses or minimizes the error in binary image. To diffuse the error at each pixel, the quantization error is filtered andfeedback to the input. The error filter process diffuses the quantization error on one pixel away tothe neighboring gray pixels. In nature, the error diffusion noise is of high frequency or bluenoise and for human vision; it can provide pleasing halftone images [4, 5]. Zhongmin Wang et al. [13] havealso proposed the half toning with error- diffusion.

4. PROPOSED METHODOLOGY

For proposed method one original secrete image, one verification image, and two covers images, all are color RGB images are taken as an input. Method produces the output as two RGB meaningful shares and after superimposition of shares it produces the original image and verification image. The method proposed consists of four phases:

1. Share generation,
2. Meaningful share generation or share hiding using LSB steganography,
3. Un-hiding of shares or reverse steganography and
4. Reveling the original secrete and verification of the result

The detailed explanation and the algorithms developed for the each phase is described in the following subsections:

4.1: Share Generation Phase:

In a share generation phase, Original RGB color secrete image and verification image is first decomposed/converted into *R*, *G*and*B*components image, then each components image is then converted into halftone image using Jarvis halftone algorithm. For each halftone image, twoshares are generated using original image and verification image component (R, G, and B) using the equation 1 and 2 [5],

$$(R\_SA_{ij}) = \left\lfloor \left(\left(R\_OI_{ij}^{hft} \times 2 + R\_VI_{ij}^{hft} + 1 \right) mod\ 4 \right) / 2 \right\rfloor \quad eq(1)$$

$$(R\_SB_{ij}) = \left\lfloor \left(\left(R\_OI_{ij}^{hft} \times 2 + R\_VI_{ij}^{hft} + 1 \right) mod\ 2 \right) \right\rfloor \quad eq\ (2)$$

Where

$R_{OI_{ij}}^{hft}$ *is halftone R Component image of original image*

$R_{VI_{ij}}^{hft}$ *is the halftone R Component image of verification image*

$R_{SA_{ij}}$ *and* $R_{SB_{ij}}$ *are the share A and share B of R Componenet image*

And the same is calculated for both green and blue component of original and verification image. Arnold transformation on each share generated above is calculated and converted to becoming random share images

Arnold transformation on each share generated above is applied for becoming truly random share images. Finally R, G, B component are concatenated and two RGB noise like shares are created. The detailed steps are presented in Algorithms I developed and presented in 4.1.1.

4.1.1 Algorithm I: Algorithm for share generation

Input: 1. Original RGB Secrete Color Image $OI = (OI_{ij})$
2. Verification color RGB Image $VI = (VI_{ij})$

Output: Twomeaningful RGB share images$SA = (SA_{ij})$,$SB = (SB_{ij})$ where *i= 0* to *H-1* and j=0 to *W-1*

Begin

1: Resize the Verification color image *VI*, to the size of original secrete image *OI* if not the equal size.

2: Separate original RGB secrete imageOI_{ij} into *R, G, and B* components image as $R\_OI = (R\_OI_{ij})$,$G\_OI = (G\_OI_{ij})$ and$B_OI = (B_OI_{ij})$.

3: Separate original RGB verification image VI_{ij} into *R, G, and B* components image as $R\_VI = (R\_VI_{ij})$,$G\_VI = (G\_VI_{ij})$ and$B_VI = (B_VI_{ij})$.

4: Convert each component *R_OI, G_OI* and *B_OI*of original image into half-tone image using Jarvis Half-toning algorithms as $R\_OI_{ij}^{hft}$, $G\_OI_{ij}^{hft}$, $B\_OI_{ij}^{hft}$

5: Convert each component *R_VI, G_VI* and *B_VI*of Verification image into half-tone image using Jarvis Half-toning algorithms as $R\_VI_{ij}^{hft}$, $G\_VI_{ij}^{hft}$, $B\_VI_{ij}^{hft}$

6: Extract the width and height of the original Secrete image as *h* and *w*

7: Initialize the output share images *R_SA, G_SA, B_SA*of size *h X w as zero* for each R,G,

B halftone image of original secrete image.

8: Initialize the output share images *R_SB, G_SB, B_SB* of size *h X w as zero* for each R, G,

B halftone images of verification image.

9: For*i=0* to *H-1*

For *j=0* to *W-1*

1. $(R\_SA_{ij}) = \left\lfloor \left(\left(R\_OI_{ij}^{hft} \times 2 + R\_VI_{ij}^{hft} + 1 \right) mod\ 4 \right) / 2 \right\rfloor$
2. $(R\_SB_{ij}) = \left\lfloor \left(\left(R\_OI_{ij}^{hft} \times 2 + R\_VI_{ij}^{hft} + 1 \right) mod\ 2 \right) \right\rfloor$
3. $(G\_SA_{ij}) = \left\lfloor \left(\left(G\_OI_{ij}^{hft} \times 2 + G\_VI_{ij}^{hft} + 1 \right) mod\ 4 \right) / 2 \right\rfloor$
4. $(G\_SB_{ij}) = \left\lfloor \left(\left(G\_OI_{ij}^{hft} \times 2 + G\_VI_{ij}^{hft} + 1 \right) mod\ 2 \right) \right\rfloor$
5. $(B\_SA_{ij}) = \left\lfloor \left(\left(B\_OI_{ij}^{hft} \times 2 + B\_VI_{ij}^{hft} + 1 \right) mod\ 4 \right) / 2 \right\rfloor$
6. $(B\_SB_{ij}) = \left\lfloor \left(\left(B\_OI_{ij}^{hft} \times 2 + B\_VI_{ij}^{hft} + 1 \right) mod\ 2 \right) \right\rfloor$

End

End

10: Apply the Arnold transformation on each share generated above for becoming random share images.

11: Concatenate Red, Green and Blue components share to produce two noise like final RGB sharesas:RGB_SA_{ij} = Concatenate $(255 * R\_SA_{ij}, 255 * G\_SA_{i,j}, 255 * B\_SA_{i,j})$,and GB_SB_{ij} = Concatenate $(255 * R\_SB_{ij}, 255 * G\_SB_{i,j}, 255 * B\_SB_{i,j})$

End

4.2 Meaningful share generation or share hiding using LSB steganography

Two noise like shares generated using Algorithms 4.1.1 are, hidden using Least Significant Bit (LSB) based image stenography for construction of meaningful shares. As we know pixel value in gray scale image range from 0 to 255. The main idea of LSB based steganography is that if the last bit value of pixel is changed then there will not be much change in color of image[14]. The shares image that is to be hiding inside the cover image is converted into binary images, then the each bit of share images are hidden inside Least Significant bit of cover image. Means the Least Significant Bit of cover image is changed as per the bits in share image. Algorithms II presented in 4.2.1 illustrate the detailed steps of meaningful share generation or share hiding using LSB stenography.

4.2.1 Algorithm II: Algorithm for LSB Based Stenography for Meaningful share Generation

Input: 1: Two RGB Secrete Share Images $RGB\_SA = (RGB\_SA_{ij})$ and $RGB\_SB = (RGB\_SB_{ij})$

2: Two RGB Cover Images $CI\_1 = (CI_{1_{ij}})$ and $CI\_2 = (CI_{2_{ij}})$

Output: Two RGB Meaningful Shares $RGB\_CI\_SA = (RGB\_CI\_SA_{ij})$ and $RGB\_CI\_SB = (RGB\_CI\_SB_{ij})$

Begin

1: Resize the RGB cover image equal to the RGB share image if they are not equal size

2: Separate *R, G and B* component of RGB_SA and RGB_SBas R_RGB_SA, G_RGB_SA, $B_RGB_SA$and R_RGB_SB, G_RGB_SB, B_RGB_SB.

3: Convert each *R, G and B* component to binary in step 2.

(Like$R_RGB_SA_{ij} = R_RGB_SA_{ij}/255$)

3: Separate *R, G and B* component of CI_1 and CI_2as $\_CI\_1, G\_CI\_1$, B_CI_1 and R_CI_2, G_CI_2, B_CI_2

4: Initialize the output cover share images $R\_CI\_1\_OUTPUT_{ij}$,$G\_CI\_1\_OUTPUT_{ij}$

$B_CI_1_OUTPUT_{ij}$and $R\_CI\_2\_OUTPUT_{ij}$, $G\_CI\_2\_OUTPUT_{ij}B\_CI\_2\_OUTPUT_{ij}$ of size $h\times w$ *as zero*

5: For *i=0* to *H-1*

For *j=0* to *W-1*

1: Extract the LSB bit value of R_CI_1 image as *R_LSB*

2: Extract the binary pixel value of $R\_RGB\_SA_{ij}$

3: Compare whether the *R_LSB and* $R_RGB_SA_{ij}$bit is same or needs to change and find the value as *temp (0 or1)*

4: $R\_CI\_1\_OUTPUT_{ij} = R\_RGB\_SA_{ij} + temp$

5: Repeat the steps 1 to 4 inside loop for G_CI_1 and B_CI_1 and for R_CI_2 , G_CI_2, B_CI_2 and calculate $G\_CI\_1\_OUTPUT_{ij}$, $B\_CI\_1\_OUTPUT_{ij}$, $R\_CI\_2\_OUTPUT_{ij}$, $G\_CI\_2\_OUTPUT_{ij}$, $B\_CI\_2\_OUTPUT_{ij}$

End

End

6: Concatenate Red, Green and Blue components share to produce two meaningful final

RGB shares as:

RGB_CI_SA = Concatenate($R\_CI\_1\_OUTPUT_{ij}$, $G\_CI\_1\_OUTPUT_{ij}$, $B\_CI\_1\_OUTPUT_{ij}$)

RGB_CI_SB = Concatenate($R\_CI\_2\_OUTPUT_{ij}$, $G\_CI\_2\_OUTPUT_{ij}$, $B\_CI\_2\_OUTPUT_{ij}$)

End

4.3 Un-hiding of shares or reverse steganography

Two noise like share hidden using algorithms 4.2.1 are extracted using reverse LSB steganography steps presented in algorithms III which are in section 4.3.1. First we need to extract LSB of each component image and create Binary share images from all RGB components image. Then RBG image will be created from all component images to produce the two final shares images which are in hidden form.

4.3.1 Algorithm III: Algorithm for Reverse Steganography for Extracting Shares from Meaningful shares

Input: 1: Two RGB Meaningful Images contains the Two Secrete Share Images $RGB\_CI\_SA = (RGB\_CI\_SA_{ij})$ and $RGB\_CI\_SB = (RGB\_CI\_SB_{ij})$

Output: Two RGB Shares $RGB\_SA = (RGB\_SA_{ij})$ and $RGB\_SB = (RGB\_SB_{ij})$

Begin

1: Separate the *R, G, and B* Components images form RGB_CI_SA and RGB_CI_SB as:

$R\_RGB\_CI\_SA$, $G\_RGB\_CI\_SA$,$B\_RGB\_CI\_SA$ and $R\_RGB\_CI\_SB$, $G\_RGB\_CI\_SB$, $B\_RGB\_CI\_SB$

2: For *i=0* to *H-1*

For *j=0* to *W-1*

1: Extract LSB of each component image and Create Binary share images from all components images in Step 1 (as like for *R*Component($R\_SA_{ij=}(R\_RGB\_CI\_SA_{ij}\ mod\ 2)$

End

End

3: Create RGB Share images from R, G, and B Components $(R\_SA_{ij}, G\_SA_{ij}, B\_SA_{ij}, R\_SB_{ij}, G\_SB_{ij}\ and\ B\_SB_{ij}$ generated in Step 2

4: Concatenate Red, Green and Blue components share to produce two final

RGB shares as:

RGB_SA = Concatenate ($255 * R\_SA_{ij}, 255 * G\_SA_{ij}, 255 * B\_SA_{ij}$)

RGB_SB = Concatenate ($255 * R\_SB_{ij}, 255 * G\_SB_{ij}, 255 * B\_SB_{ij}$)

4.4 Reveling the original secrete and verification of the result

Reveling the original secretes and verification of the result is the most important phase of the proposed algorithm. Two noise like RGB shares generated using algorithms III presented in section 4.3.1 are used to revel the original secrete image. After extraction of R, G, B components from two noise like shares, reverse Arnold transformation is applied. Finally the original secrete image and verification is extracted by using the equation 3 and 4 [5].

1. $(R\_OI_{ij}) = \left|\left(\left(R\_SA_{ij} \times 2 + R\_SB_{ij} + 3 \right) mod\ 4 \right) / 2\right| \quad eq.3$

2. $(R\_VI_{ij}) = \left\lfloor \left(\left(R\_SA_{ij} \times 2 + R\_SB_{ij} + 3 \right) mod\ 2 \right) \right\rfloor \quad eq.4$

Where

$(R_{OI\,ij})$ *and* $(R_{VI\,ij})$ *are red componets image original image and verification image.*

And the same is calculated for both green and blue component of original and verification image.

Algorithm IV presented in section 4.4.1 illustrate the detailed steps of reveling the original secrete image. The image quality of the reconstructed image and the original secrete image is same and there is no distortion of pixels. The method also helps us to verify the reconstructed image using the verification image.

The image extracted can be verified using MSE (Mean Square Error) and SS (Structural Similarity) Index value. If the SS value is 1and the MSE value is 0 then the revealed image is the same image as the hidden image and there is not cheating by the user.

4.4.1Algorithm IV: Algorithm for Secrete Recovery

Input: Two noise like RGB share images $RGB\_SA = (RGB\_SA_{ij})$, $RGB\_SB = (RGB\_SB_{ij})$, where *i= 0* to *H-1* and j=0 to *W-1*

Output: Original RGB Secrete Color Image $OI = (OI_{ij})$and Original Verification Image $VI = (VI_{ij})$of Size *H X W* where *i= 0* to *H-1* and *j=0* to *W-1*

Begin

1: Separate twonoise like RGB share imagesRGB_SA_{ij} , RGB_SB_{ij}into R, G, and B components image and convert these into binary image as below

$(R\_SA = (R\_SA_{ij})/255, G\_SA = (G\_SA_{ij})/255$ and$B_SA = (B_SA_{ij})/255)$, $(R\_SB = (R\_SB_{ij})/255, G\_SB = (G\_SB_{ij})/255$ and$B_SB = (B_SB_{ij})/255)$

2: Apply Reverse Arnold transformation on each of the *R, G, and B* components image generated in step 1.

3: For *i=0* to *H-1*

For *j=0* to *W-1*

3. $(R\_OI_{ij}) = \left\lfloor \left(\left(R\_SA_{ij} \times 2 + R\_SB_{ij} + 3 \right) mod\ 4 \right) /2 \right\rfloor$
4. $(R\_VI_{ij}) = \left\lfloor \left(\left(R\_SA_{ij} \times 2 + R\_SB_{ij} + 3 \right) mod\ 2 \right) \right\rfloor$
5. $(G\_OI_{ij}) = \left\lfloor \left(\left(G\_SA_{ij} \times 2 + G\_SB_{ij} + 3 \right) mod\ 4 \right) /2 \right\rfloor$
6. $(G\_VI_{ij}) = \left\lfloor \left(\left(G\_SA_{ij} \times 2 + G\_SB_{ij} + 3 \right) mod\ 2 \right) \right\rfloor$
7. $(B\_OI_{ij}) = \left\lfloor \left(\left(B\_SA_{ij} \times 2 + B\_SB_{ij} + 3 \right) mod\ 4 \right) /2 \right\rfloor$
8. $(B\_VI_{ij}) = \left\lfloor \left(\left(B\_SA_{ij} \times 2 + B\_SB_{ij} + 3 \right) mod\ 2 \right) \right\rfloor$

End

End

4: Concatenate Red, Green and Blue components share generated in step 3 to produce Original and Verification images as:

OI = Concatenate $(255 * R\_OI_{ij}, 255 * G\_OI_{ij}, 255 * B\_OI_{ij})$

VI = Concatenate $(255 * R\_VI_{ij}, 255 * G\_VI_{ij}, 255 * B\_VI_{ij})$

5: Display *OI and VI* with using colormap.

End

5. EXPERIMENTAL RESULTS

The results obtained using the Algorithm I, II, III, and IV are presented in table 2: and discussed as below.

To illustrate how the scheme proposed overcomes the various security constraints of visual cryptography such as expansion of pixel in secrete image, cheating while presenting shares and contrasts loss of shares we used the four images as presented in table 2 (a, b, c, and d). All the images used and generated using experiments that are shows in table2 are 512 X 512 color images so there is no pixel expansion. Lena image (a) and Gold Hill Image (b) is used as original image and verification image. Peppers image (e) and monkey image (f) is used as a cover image for LSB based steganography. The images (c) and (d) are the color RGB share image generated using algorithm II and images (g) and (h) are the unhidden and reveled shares images from the cover images (e) and (f) generated using algorithms III. Finally image (i) and (j) are the original image and verification image revealed using Algorithms IV. In Table 2 the original image and the reconstructed images are exactly of same clarity and size means there is no pixel expansion. Flipping issues and also share distortion is not arising. Cheating while presenting the shares is discussed in section 4.4 and contrasts loss of shares is discussed in section 6.

6. DISCUSSION AND PERFORMANCE ANALYSIS

The performance analysis of the above method is also performed using the statistical method presented below.

a. Pixel expansion:

Pixel expansion problem is 100% reduced in the scheme proposed in this paper because the share size and the generated image size after superimposing the share is exactly equal which is shown in table 2 (a) original image, Share Images *(c), (d)* and recovered image*(i).*

b. Contrast and statistical analysis:

As shown in table. 2(a), and *(i)* the recovered image is obtained without any pixel distortion. To evaluate the quality of recovered image and to prove that the recovered image is of same quality of the original image, different statistical metrics of image restoration are used as below.

I. Mean Square Error (MSE)

Mean Square Error (MSE) [13] can be mathematically computed using the formula

$$MSE = \frac{1}{MX\,N}\sum_{i=1}^{M}\sum_{j=1}^{N}(h_{ij} - h'_{ij})^2 \qquad eq.5$$

Where $h_{ij}\ and\ h'_{ij}$ are the pixel values of original image and reconstructed image respectively.

II. Peak-Signal-to-Noise Ratio (PSNR)

Peak-Signal-to-Noise Ratio (PSNR) [14] is also and mathematical or engineering formulations calculated using *MSE* with the help of following formula.

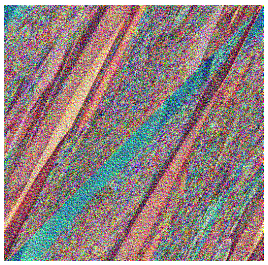
$$PSNR = 10 * \log\frac{R^2}{MSE} \qquad eq.6$$

Statistically, when the value of PSNR=1, it indicates that the scheme provides a maximum visual quality.

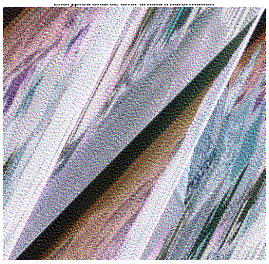
Table 2: a. Original RGB Image b Verification Image, c and d are RGB Color shares e and f are meaningful steganography shares; g and h are extracted shares from steganography shares, i. original share image, j. verification share.

a

b



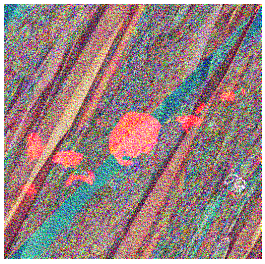
c



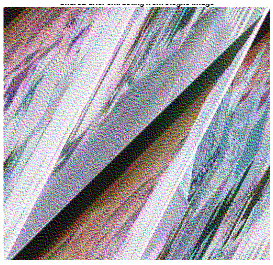
d

e

f



g



h

i

j

III. Universal Index Quality (UIQ)

Universal Index Quality (UIQ) [15] can be calculated with the help of following equation

$$UIQ = \frac{4\sigma_{zy}\,\overline{xy}}{\sigma_x^2 + \sigma_y^2\,[\,(\bar{x})^2 + (\bar{y})^2\,]} \qquad eq.7$$

This is used to modeling the image distortion as combination of three factors these are

1. Loss of correlation,
2. Luminance distortion, and
3. Contrast distortion

The UIQ between two images varies from *-1* to *+1*. The two images X and Y have strong positive linear correlation, if UIQ is close to *+1*. The *-1* value of UIQ indicates a negative relationship between the two images and the zero value indicates that there is no relationship between the two images [16].

c. Maximum Difference (MD)

Maximum Difference (MD)measure is used to calculate the error between original image and reconstructed image. MD is directly proportional to contrast giving an image dynamic range and which can be calculated with the expression [17]

$$MD = max|x_{ij} - y_{ij}| \qquad eq.8$$

d. Average Difference (AD)

Average difference is method of calculating the difference in two images; original image and recovered image. Average Difference (AD) between original image and recovered image is calculated with the average difference metrics as below [17].

$$AD = \frac{1}{M\ X\ N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij}) \qquad eq.9$$

Where, X and Y denote the original image and calculated recovered image. The values of all the metrics discussed above are presented in table 3.Table 3 represents the value of MSE, MD, AD is zero, PSNR value is infinite ∞ and UIQ value is 1 represents and assures that the original images have been completely recovered without any damage or loss of any meaningful information of the recovered image.

Table 3: Value of Difference Statistical Metrics Obtained in experiment

Statistical Metrics	Value Obtained in Experiments
MSE	0
PSNR	∞
UIQ	1
MD	0
AD	0

We compare our method with previously known method the result obtained using different statistical measures are presented in table 4:

Table 4: Results of comparison between the previously known methods and the proposed method using statistical measures

Scheme	Secrete Image	Pixel Expansion	Decoding Method	Aspect Ratio	Reconstructed Image
Zhou et al.'s scheme [4]	Binary(m x n)	*p=4*	OR Operation	Changed	Better quality
Zhongmin Wang et. al. 's [12]	Binary(m x n)	*P=4*	OR Operation	changed	Lossless
Mahmoud E. Hodeish et. al. 's [6]	Binary Halftone	P=1	XOR Operation	unchanged	Lossless
Mahmoud E. Hodeish et. al. 's [6]	Binary Halftone	P=2	XOR Operation	changed	Lossless
Chang-Chou Lin [10]	Grey Level	P=4	OR Operation	changed	Lossy
F. Liu et. al [11]	Color	*P=4*	OR operation	changed	Lossy
The Proposed Scheme	Color	*p=1*	Reconstruction Algorithm	unchanged	Lossless

7. CONCLUSION

In this paper novel approach for secure and verifiable color visual cryptography Scheme with LSB based image steganography is proposed. Secure and verifiable scheme is most suitable for securing the sensitive and important data. The proposed method overcomes the various security constraints of visual cryptography such as expansion of pixel in secrete image, codebook requirement for creating shares, cheating while presenting shares and contrasts loss of shares. The approach presented is an 2 out of 2 secrete sharing scheme and generate meaningful color shares using Least Significant Bit (LSB) steganography so it don't invite the attention of cheaters.

Performance evaluation of this method is also performed with existing method and using some statistical metrics and we found better results in terms of quality and security of the image. The scheme proposed is capable for detection of originality of the shares means cheating is made of not. The scheme can be extended to identify the exact location of tempered region in case the share presented is damaged. Further the scheme can also be extended for (k, n) secrete sharing scheme and can be used for different images.

REFERENCES

1. MoniNaor and Adi Shamir, "**Visual Cryptography",**Eurocrypt, 1994
2. Young-Chang Hou**"Visual cryptography for color images",**Pattern Recognition Journal of the Pattern Recognition Society Volume 36, pp. 1619–1629,2002
3. Jonathan weir and weiQi, Yan **"Visual Cryptography and its Application"**, Ventus Publishing Aps, eBook, pp.1-144, 2012.
4. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo**, "Halftone Visual Cryptography",** IEEE Transactions On Image Processing, Vol. 15, No. 8, Pp. 2241-2453, August 2006
5. Mahmoud E. Hodeish, LinasBukauska,Vikas T. Humbe,**"An Optimal (k,n)Visual Secret Sharing Scheme**

for Information Security", Elsevier- Procedia Computer Science 93, pp.760 – 767, 2016.

6. Mahmoud E. Hodeish and Vikas T. Humbe, **"An Optimized Half tone Visual Cryptography Scheme Using Error Diffusion"**, Springer, Multimed Tools Application pp1-17, January 2018.
7. G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, **"Visual cryptography for general access structures"**, Proc.ICAL96, Springer, Berlin, 1996, pp. 416-428, 1996
8. AbhishekParakh and SubhashKak**"A Recursive Threshold Visual Cryptography Scheme"**, CoRR abs/0902.2487, 2009
9. Mahmoud E. Hodeish, LinasBukauskas , Vikas T. Humbe, **"A new efficient TKHC-based image sharing scheme over unsecured channel"**, Journal of King Saud University Computer and Information Sciences, 3 August 2019.
10. Chang-Chou Lin, Wen-Hsiang Tsai, **"Visual cryptography for graylevel images by dithering techniques"**, Pattern Recognition Letters, v.24 n.1-3, 2003.
11. F. Liu, C.K. Wu, X.J. Lin, **"Colour Visual Cryptography Schemes"**, IET Information Security, vol. 2,No. 4, pp 151-165, 2009.
12. Zhi-hui Wang, **"Sharing a Secret Image in Binary Images with Verification"**, Journal of Information Hiding and Multimedia Signal Processing, Ubiquitous International, 2011
13. Zhongmin Wang, Student Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Giovanni Di Crescenzo, **"Halftone Visual Cryptography via Error Diffusion"**,IEEE Transactions On Information Forensics And Security, VOL. 4, NO. 3, pp. 383-396, September 2009
14. Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, **"Steganography in Images Using LSB Technique"**, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1, pp. 426-430. January 2015
15. Chen, C.Y., Chen, C.H., Chen, C.H., Lin, K.P., 2016. **"An automatic filtering convergence method for iterative impulse noise filters based on PSNR checking and filtered pixels detection**". Expert Syst. Appl. 63, 198–207.
16. Shankar, K., Eswaran, P., February 2017. **"RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography**". China Commun. 14 (2), 118–130. https://doi.org/10.1109/CC.2017.7868160.
17. Wang, Z., Bovik, A.C., "**A universal image quality index"**, IEEE Signal Process Lett.9 (3), 81–84, 2002
18. Rajkumar, S., Malathi, G., 2016. **"A comparative analysis on image quality assessment for real time satellite images"**. Indian J. Sci. Technol. 9, 1–11
19. Ece, C., Mullana, M.M.U., 2011. **"Image quality assessment techniques in spatial domain"**, IJCST 2 (3).
20. Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, **"Steganography in Images Using LSB Technique",** International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1, pp. 426-430. January 2015
21. Kalyan Das, AromitaSen and Samir Kr. Bandhopadhyay, **"A Robust Visual Cryptography Scheme for Imperceptible Distribution of Secret Message without Pixel Expansion"**,International Journal of Advanced Trends in Computer Science and Engineering(**IJATCSE**)Available Online at http://www.warse.org/IJATCSE),Volume 6, No.4, pp.62-70 August 2017