Information Security using Visual Secret Sharing Scheme and Solution to Potential Attacks

Jesalkumari Varolia
Assistant Professor,
Department of Computer Engineering,
Thakur College of Engineering and
Technology,Mumbai,India

R.R. Sedamkar
Professor,
Department of Computer Engineering,
Thakur College of Engineering and
Technology,Mumbai,India

ABSTRACT

Recently images are used almost everywhere as an information transfer. As growing call for of protection, user authentication resides in earlier in records protection and performs an important position in shielding customers privacy. On-line transactions have become very usual place In this virtual era and numerous attacks are concerns. This paper discusses many potential attacks on visual secret sharing system and offering more safety than current method. In the proposed method, secret image is divided into many shares and distributed among the participants. The method used is recursive visual cryptography so many shares can be concealed in one share which gives better manageability. The main focus is on better image quality of reconstructed Image and protection from potential attacks on generated shares. At the decryption end super resolution is used to improve image quality and this paper achieved 92% accuracy and 95% SSIM The suggested method can be useful in many applications like online voting system, online banking and any other system where authentication is essential.

Keywords

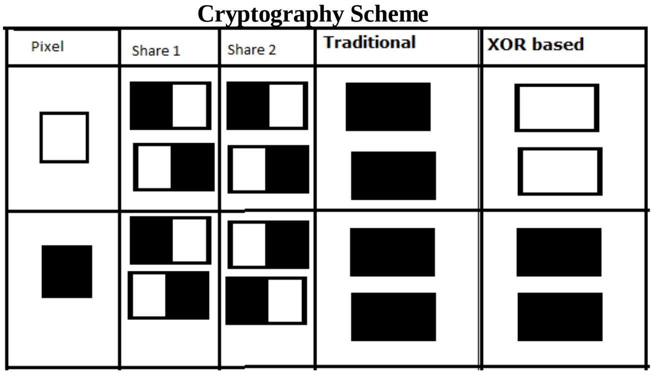
Visual Secret Sharing, Information Security

1. INTRODUCTION

Internet has turn out to be a totally vital in nearly in every one’s life. Internet banking, E-Commerce and online document transaction has received extensive acceptance the world over and looks to be short catching up in digital India. Online banking permits the clients to apply all the banking offerings from a computer which has internet, then the clients can carry out monetary transactions on steady sites operated beneath Neath banks. The visual cryptography is a technique, which provides security to digital documents by dividing the secret image into multiple shares. These shares are then transmitted over a network to respective participants. To reconstruct the original secret image, all shares must be stacked their shares together at the receiver end. For n participants, all n shares are to be stacked in order to revelation of the original image. No single participant is responsible if secret image is leaked, in fact all are equally responsible as it is almost impossible to retrieve secret image from random noised image. There are many advantages of Visual cryptography method and one of the most prominent is share can’t reveal secret image (SI) as it looks random noisy image. The proposed Visual Secret Sharing scheme is mainly for sharing binary images and to reconstruct the original secret binary image ‘or’ operation is used.[1] The proposed scheme was restricted to binary images only and pixel expansion was major problem. Pixel expansion changes the resolution of the image which depends on which method is used. To recover gray-scale and color images Hou et al. [19] proposed the scheme as block-based progressive visual secret sharing scheme. The VSS scheme proposed by [19] recovered SI with none pixel expansion. The secret image was recovered progressively block by block just like jig-Saw-puzzle .The recovered secret image was in halftone format not in multitone format which degrades the contrast quality of image. Visual cryptography proposed with XOR operation which gives better contrast of a reconstructed image. Itzkovitz [2] presented XOR based Visual Cryptography to share a binary image.

Traditional v/s XOR Based Visual Cryptography

Table I. (2, 2) XOR-based 1x2 Resolution Visual Cryptography Scheme


Pixel
Share 1
Share 2
Traditional
XOR based

A (2,2) visual cryptography scheme S = (C0, C1) consists of two matrices C0 and C1 of n x m binary matrices. To generate a share for white (black) pixel, random matrix (C0 or C1) is chosen from Table I is chosen and given to the rows for both participants as encrypted data. XOR-based

Encryption of image is same as traditional but decryption can not be done by human eye system. It requires computation for decryption. Table 1 compares the outcome of Traditional and XOR-based (2,2) Visual cryptography Scheme. It also shows that 2 subpixels (one white and one black) are generated from an original pixel. If the original pixel is white than one of the row from table I is selected randomly for share generation and that changes resolution of reconstructed image to 1x2.

Work done for transmission of document images’ securely is not done much using Visual Secret scheme in our best knowledge. In today’s era the document photos(i.e. image of Aadhar Card, Check, Passport photo etc) are transferred via social media commonly. The security of such documents are crucial and paramount for the customers. The major contribution is: We have proposed a novel approach- Deep Learning based VSS Which transmits document images securely over a network and improves the quality of reconstructed image.

The Visual Secret Sharing (VSS) is a scheme first proposed by Naor and Shamir [1] to share secret image among n users. They have designed basis matrices in order to generate multiple shares. Basis matrices are the collection of ones and zeros, which are used to mask secret image pixels into multiple shares. Many researchers were successful in recovering the secret image with the contrast of up to 50% have proposed VSS based techniques which recover the secret image with the contrast of up to 50%. Hou et al. [19] proposed the scheme Block-based Progressive Visual Secret Sharing. The scheme recovers the gray-scale and color images with the contrast of 50% and 25% for noise-like and meaningful shares. Although BPVSS achieves the contrast of 50%, scheme suffers from drawbacks like 1) It recovers the secret image as a monotone image. 2) Recovers the secret image with the maximum contrast of 50%.

2. PROPOSED METHODOLOGY

We have proposed a novel VSS scheme which enhances the visual quality of the reconstructed secret image due to CNN-based architecture. The model deals with the attacks like scaling, missing share, passive attack, unauthenticated share. All of these attacks are discussed in following section. Although the visual quality of reconstructed image is better, it is not able to sharpen the edge of an image. This paper contributes to reduce some of the noise as upscaling makes

picture more clear. The proposed architecture is shown in Fig. 1. The proposed architecture contains three steps such as (1)Train the model for super resolution, (2) generate the temporary image using decryption method, and 3) generate the final output image after upscaling.We not working with true colors but with halftoned image. Input an RGB colored image and then split the image in CMY model. The main purpose of using CMY is it is compatible with printers .RGB and CMY are complementary colors, in the true color model, (R, G, B) and (C, M, Y) has the following relationships: C =255−R, M = 255−G, Y = 255−B;

In CMY model white pixel is represented by (0; 0; 0) and black pixel (255; 255;255) represents . So first we split RGB model of original image. Then using above equation RGB is converted to CMY model.

Halftone algorithm is to be applied on R, G and B images separately. Among many halftones algorithms error diffusion algorithm is used. The coefficients are modified and compared with floyd's algorithm, stucki's algorithm and proposed algorithm for halftoning. The coefficients for the same are given in Table 2. The dark spot depicts current pixel, which is the threshold. The filter coefficients in Error Diffusion filter determines what percentage of quantization error indexed relative to the current pixel, which, is to pass to the pixel at that location, relative the current pixel.

Table 2 Coefficients for Halftone

		*	8/24	0
	2/24	4/24	00	2/24
1/24	0	4/24	2/24	1/24

It gives three halftoned images one for each Cyan, Magenta and Yellow. Here, threshold (T=127) is checked for each pixel is and if value is greater than T converts it to 255 otherwise 0.

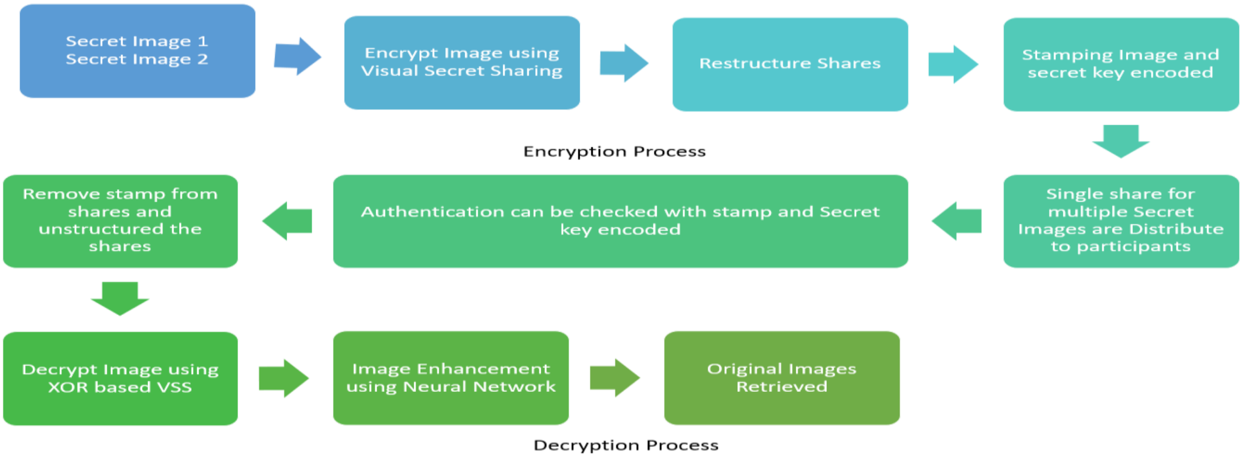

Secret Image 1
Secret Image 2
Encrypt Image using Visual Secret Sharing
Restructure Shares
Stamping Image and secret key encoded
Encryption Process
Single share for multiple Secret Images are Distribute to participants
Authentication can be checked with stamp and Secret key encoded
Remove stamp from shares and unstructured the shares
Decrypt Image using XOR based VSS
Image Enhancement using Neural Network
Original Images Retrieved
Decryption Process

Fig 1. Architecture for Image Security using VSS

2.1 Procedure for Encryption

1. Input RGB color image.

2. Conversion of RGB to CMY model.

3. Apply Halftone on each (C,M,Y).

4. Pass through Visual Cryptography and generate shares for each C,M and Y .

5. Generate share 1' by Combining all the share 1 and generate share 2' by Combining share 2

6. Read encrypted colored image shares.

7. Restructure (Scramble the shares for further security) by rotating blocks in clockwise direction.

8. Stamp a share with cover image

9. Shares are ready is to be shared with participants.

At decryption end XOR operation is applied on the shares which are superimposed to reconstruct the image.

This method is Modified Visual Cryptography scheme for colored images. Fig.1 expresses the same procedure

2.2 Recursive Visual Cryptography for multiple interrelated secret information

Recursive cryptography is a technique to hide more than one secret images in single of the shares of the original image. We can hide participants Aadhar card, pan card and driving license in one image. The first secret image is Aadhaar card, second secret image is driving license and third driving license. The constraint is images have to be of specific size of (nXn ; 2nX2n; nX2n) to get merged in one share. The first step is to apply VC to the smallest secret image is divided into different shares. These shares are used to generate one share of next image with resolution double at columns whereas number of rows remains same. The final shares are distributed among participants and at the decryption end three images can be revealed.

Fig. 2 explains the concept of recursive visual cryptography where three images are considered with in original image of size 256 X 256, Secret image 1 of 256X128 and secret image 2 of 128X128 is patient's personal detail. First Visual cryptography is e applied on Lowest resolution image which is secret message 1 and two shares are generated of 128X256 which are further used for generating share 1 of secret message 2. Share 2 of secret message is generated from secret image 2 and share 1. These two shares are used to generate share 1 of Secret original message.

Both the shares of secret message 2 are concatenated which makes share1 of size 256X 512 and share 2 is generated with respect to share 1 such that by applying XOR based VC at decryption end Secret image 2 is revealed. As decoding is total reverse process of encryption process, using two shares of secret image 2, share 1 of original secret is generated. For decryptions shares must be broken from center and stacked onto to reveal original message of size 256x512 by decrypting shares using XOR based Visual Cryptography. To decrypt the original message of the size as its original ones which is 256x256 here, size reduction algorithm is used, which is mentioned below, reconstructed image is achieved. Both the shares of secret message 2 are concatenated which makes share1 of size 256X 512 and share 2 is generated with respect to share 1 such that by decryption is done by XOR based. Now using these two shares of secret image 2, share 1 of original secret is generated. For that both the shares are combined and share1 of size 256x512 is generated and share 2 of original message is generated such that it can reveal the original message of size 256x512 by decrypting shares using XOR based Visual Cryptography. To decode the original message of same size as its original size which is 256x256 here, size reduction algorithm is used, which is mentioned below, reconstructed image is achieved.

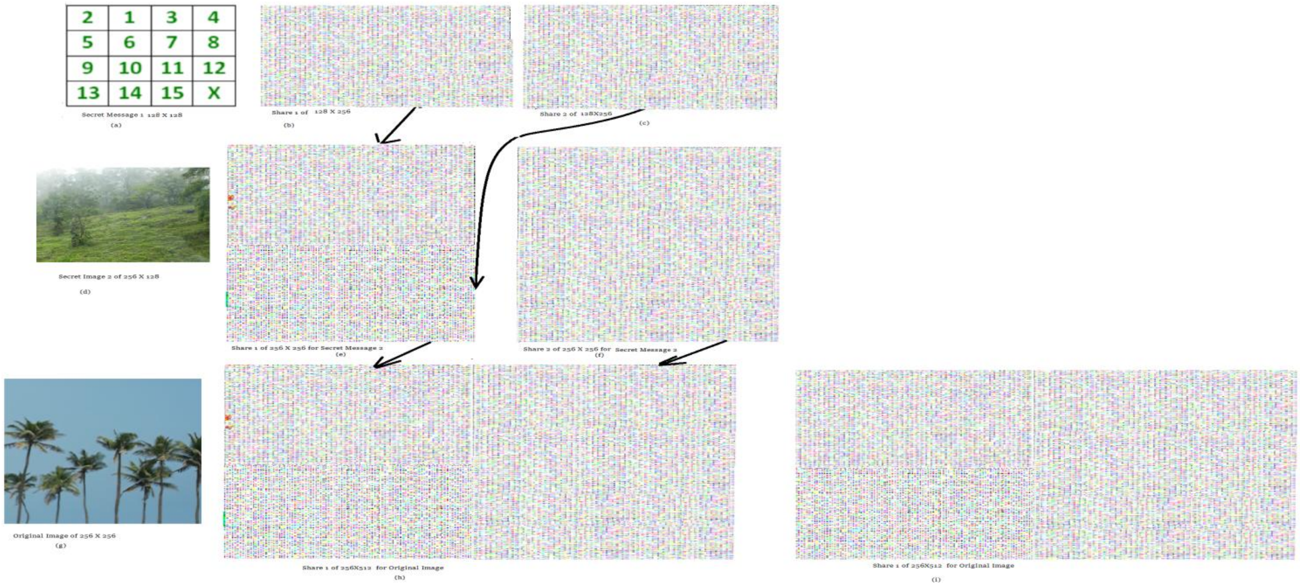

2 1 3 4
5 6 7 8
9 10 11 12
13 14 15 X
Secret Message 1 128 X 128
(a)
Share 1 of 128 X 256
(b)
Share 2 of 128X256
(c)
Secret Image 2 of 256 X 128
(d)
Share 1 of 256 X 256 for Secret Message 2
(e)
Share 2 of 256 X 256 for Secret Message 2
(f)
Original Image of 256 X 256
(g)
Share 1 of 256X512 for Original Image
(h)
Share 1 of 256X512 for Original Image
(i)

Fig. 2 (g)Original Message (256X256) (a) Secret Message 1(128X128) (d) Secret Message 2 (256X128) (b) Share 1 of Secret Message 1(128X256) (c) Share 2 of Secret Message 1(128X256) (e) Share 1 of Secret Message 2 (256X256) (f) Share 2 of Secret Message 2 (256X256) (h) Share 1 of Original Message (256X512) (i) Share 2 of Original Message(256X512)

Sized reduction algorithm.

1. Consider decrypted image and one image with the size of original message with all pixels white.
2. if 2i-1 and 2i both pixels are black for same row then Color black to the ith pixel (because number of rows are same) in decrypted image.
3. Repeat above steps for all the remaining pixels.

In this method, first share of original image acts as Cipher (which contains hidden message) and second share acts as a key to decrypt original message. Share 1 can reveal secret message 1 and secret message 2 by alone but to decrypt original message share 2 is needed. Share 1 can be divided in two part from the center (of same size 256X256) and by applying XOR based VCS on them we can reveal Secret image 2 and further if we divide the first part of that division horizontally then we can reveal secret image 1 using XOR based VCS.

2.3 Artificial Neural Network

The brain's biological neural network has 100 billion neurons, the prominent processing unit of the brain. Neurons has synapses to perform their functions through their massive interconnections. The human brain consists of 100 trillion synapses per neuron 1,000. Similarly, the nodes work in parallel and each node collects input from some other. The nodes then process these inputs and pass on the output to the next neighbor node. Neural networks perform task by experience and analyzing pre-defined data. Convolutional Neural Network (CNN) is Neural Networks algorithm mostly used to analyze images. Deep Learning algorithms are designed in such how that they mimic the function of the human cerebral mantle. These algorithms are representations of deep neural networks i.e., neural networks with many hidden layers. Convolutional neural networks are deep learning algorithms which will train large datasets with many parameters, in sort of 2D images as input and convolve it with filters to supply the specified outputs. during this article, CNN models are built to guage its performance on image recognition and detection datasets.

Convolutional Neural Network consists of Convolutional layers with mathematical operation called convolution which is a specific kind of linear operation that involves the multiplication of weights and input.

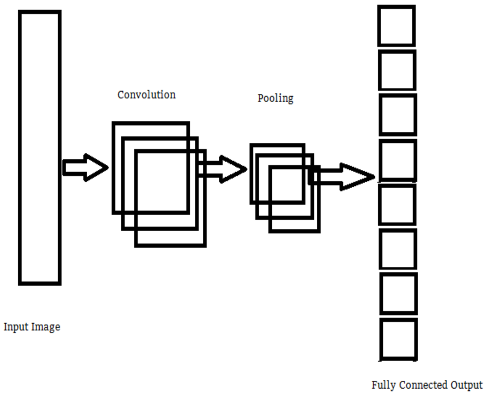


Fig. 3. CNN Architecture

Fig. 3 shows the CNN Architecture with all internal main processes. CNN automatically extracts features of an image. It uses information of neighbor pixel to effectively down sample the image initially by convolution and then uses a prediction layer at the end. Deep neural network can predict good patterns of natural images effectively. The network can make better judgments on redundant area and so can hide more pixels. More data can be hidden by saving the space on unwanted area of an image. Because of the structure and random weights, the network will succeed in hiding from ones who don't kno weights. The output image helps the model to learn and genera a residual image for a given secret image. The output of t convolution will be given to the ReLU activation function. T pooling layer is to reduce the dimensionality so parameters c be reduced and cost of computation too. This will lead to sh training time and manages overfitting. The most frequent type pooling is max pooling, which takes the maximum value in ea window.

Image Enhancement using Enhanced Deep Residual Networks

An enhanced deep super-resolution network (EDSR) has better performance in super resolution. The learning is supervised learning. The improvement in the model is mainly because of removal of unnecessary modules in conventional residual networks. Before starting with training or testing the network, the input images should be of same size. All images

\should be resized by cropping to 256 × 256 before giving into the network. To train a model for increasing the spatial size by a factor of 2. However, the convolution operation downscales the size of the input. So, we have to apply a deconvolution so that the output image size increases by 2 times compare to input. Training data is done on high resolution (HR) images from the internet, then down-size them by a factor of 2 that will be the low resolution(LR) images. This low-resolution image is fed to the network and trained it to generate the high-resolution image.

3. EXPERIMENTAL RESULTS

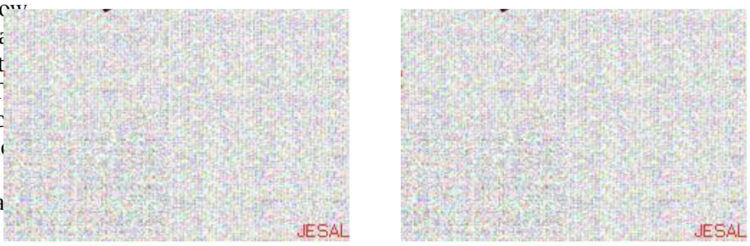
Configuration Anaconda 2.6.0 is used. Spyder is currently in the β phase is used. Tensorflow 2.4.3 with keras were pre-installed Many other essential machine learning libraries were imported. Model has used libraries like Matplotlib, Tensorflow, Matplotlib, Numpy, Keras, Scipy, etc. The system used was RAM 16 GB, Intel core i5-8300H CPU @2.30 GHz, 64-bit Operating System. The model is trained for Image Enhancement using super resolution. This is the most crucial and rewarding stage of new and Improved Visual Secret Sharing. The quality is reconstructed image is being improved with this method compared to traditional VSS.

This proposed method hides two secret messages with one additional message using recursive visual cryptography as discussed in above part. Fig 2 shows the process for the same. After this step, single Share is ready for more than one secret message as shown in Fig. 2 (h)(i). These shares are restructured by any random number which is passed with the share for decryption purpose. For example, if shares are restructured by 4 then image is divided in 4 and blocks are rotated in clockwise direction. Example is shown in Fig. 4(a) and (b) where both the shares are restructured

(a) (b)

Fig. 4(a) Share 1 (b) Share 2

Now , stamping is imposed on these shares as to identify which share is used for what purpose and it is kind of identification of share. Following Fig. 5(a) (b) shows stamped shares for participants.



(a) (b)

Fig. 5(a) Share 1 stamped (b) Share 2 stamped

These stamped shares are given to participants which has to be kept secured as to retrive the secret messages.It can be stored on cloud or on personal machine that is upto particpant but to retrive original message these share are required.

At the decryption end secret messages are retrived but the image quality is to be further enhanced that is done by Convolution Neural Network based super resolution of the retrived image.

3.1 Image Quality Measurement

Evaluation of reconstructed image is to be done so as the evaluate the proposed method. Image quality is checked by two parameters: 1) Subjective and 2) Objective. Evaluation done with human visual system is known as subjective.

We have evaluated reconstructed image's qualtity with human visual system and the findings are: the image size has increased and that helps in better visibility of minor detailing.

Then for objective evaluation We have used parameters like self-similarity index (SSIM), mean square error (MSE) and normalized absolute error (NAE).

Self-similarity index (SSIM)

Earlier SSIM is to be calculated for grayscale structures only by converting colored image into greyscale but it wasn't giving actual image quality of colored image.

‘The new index is proposed by improving the grayscale Structural Similarity index (SSIM) to include color information. This is done by modeling any image distortion as a combination of four local comparison functions namely luminance comparison, contrast comparison, structure comparison, and color comparison.’[25] The proposed quality index is defined as:

CSSIM =l (x, y) C (x, y) S (x, y) Cr (x, y)

Where l(x,y) ,C(x,y), and S(x,y) are the luminance, contrast, and structure comparisons between the original and distorted images. Cr(x,y) is the color comparison which is defined as: Cr (x, y)=1-1/k Delta(E(x,y))

Where Delta (E(x,y)) is the color fidelity value [25] with is calculated as

$$\Delta E = \sqrt{(L_1^* - L_2^*)^2 + (a_1^* - a_2^*)^2 + (b_1^* - b_2^*)^2}$$

Mean square error (MSE)

Mean Squared Error (MSE) is a way of measuring this similarity to compute an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal. The mean-squared-error (MSE) is the simplest, and the most widely used, full-reference image quality measurement.

This metric is frequently used in signal processing and is defined as follows:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x(i,j) - y(i,j))^2$$

Where x(i, j) represents the original (reference) image and y(i, j) represents the distorted (modified) image and i and j are the pixel position of the M×N image.MSE is zero when x(i, j) = y(i, j) .

ii) Peak Signal to Noise Ratio (PSNR): The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation :-

$$PSNR = 10 \log_{10} \frac{(2^n - 1)^2}{\sqrt{MSE}}$$

Normalized absolute error (NAE)

NAE is the measure of error between the original image and the reconstructed image. NAE of one means the reconstructed image is of poor quality. Similarly, NAE being Zero indicates the better reconstruction quality of the SI. The formula used to compute the NAE is given in Eq. 11.

$$NAE = \sum_{i=1}^{m} \sum_{j=1}^{m} \frac{\mathbf{I}(i,j) - \mathbf{R}(i,j)}{\mathbf{I}(i,j)}$$

Result Analysis:

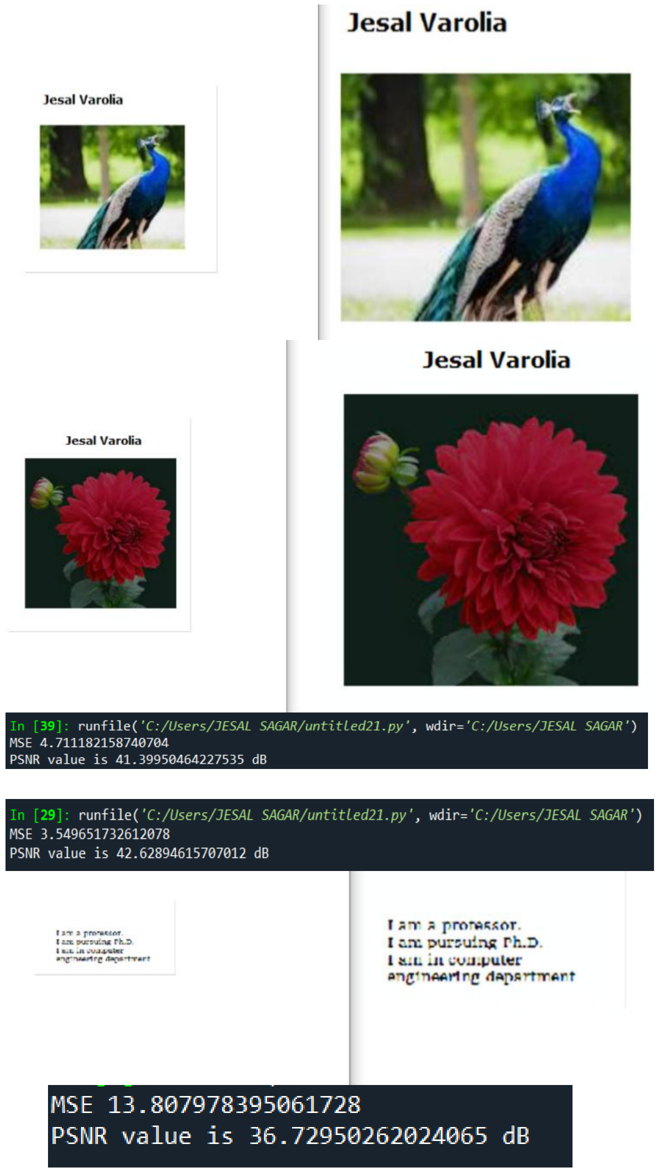
As the following table shows the comparison of proposed system with our own proposed system in earlier paper[4] and with secure visual secret sharing methodology[23]. The results shows that the recovered image with proposed method has an advantage of better visual quality. The quality is measured with respect to MSE,PSNR,SSIM and NAE for about 32 images.

	MSE	PSNR	SSIM	NAE
VC for Secret Image Sharing [4]	8.27	29.89	0.814	0.38
Secure VSS[23]	13.69	32.58	0.886	0.57
Proposed method	4.71	41.399	0.926	0.241

Figure 6 shows the output image with its original image and its MSE and PSNR values are also being displayed. The visual quality is better improved as the upscaling with super resolution gave better quality.

Figure 6(c) has reconstructed the image with text where the original document text is little distorted so the reconstructed image is not of that good readable good quality Image Histogram.

An image histogram is a graphical representation of the intensity range in a digital image. It plots for each intensity and the total number of pixels. The y-axis represents number of pixels and X axis represents intensity tone for Red color/Green Color/ Blue Color.



```
In [39]: runfile('C:/Users/JESAL SAGAR/untitled21.py', wdir='C:/Users/JESAL SAGAR')
MSE 4.711182158740704
PSNR value is 41.39950464227535 dB
```

```
In [29]: runfile('C:/Users/JESAL SAGAR/untitled21.py', wdir='C:/Users/JESAL SAGAR')
MSE 3.549651732612078
PSNR value is 42.62894615707012 dB
```

```
MSE 13.807978395061728
PSNR value is 36.72950262024065 dB
```

Figure 6(a) Secret Image 1(b) Secret Image 2 c) Original message

Figure 7(a) shows the histogram for R-plane of original image and (b) is the histograom of R -Plane of Reconstructed image . That shows the intensity remained almost same for the recovered image so the quality of image was intact as per human visual system.

3.2 Potential Attacks handling

The first possible attack is deletion of one of the shares of an information whereas other shares are there. For example, if individual shares are stored for each PAN card, Aadhar card and Driving license then participant has to always keep a track of all the shares which is quite inconvenient. As a solution to the same a single share stores the data of variety documents so participant has to only keep track of single share for all his data files.

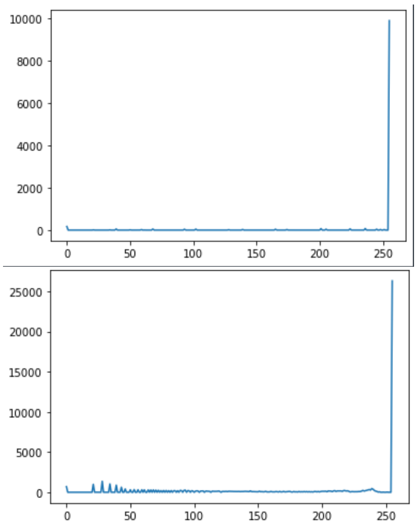


Figure 7(a) Histogram of Original Image (b) Histogram of reconstructed image

The second attack considered is, if share is leaked then also no secret message will be revealed as it is only random dots like image and because of restructuring the share the superimposed two shares also won't give any details.

The third attack is unauthorized share received by decryption end. The stamp on the Shares are compared before starting with decryption and if they don't match then the received share is not from authorized user.

Next few attacks are regarding active attack by intruders. If share is modified in size or content then it will be identified at decryption end either by no message revealed or wrong message revealed. In this case the outcome has to be notified to owner of the share so that attack is been Identify. Scaling and rotation can be taken care of because the size of the share is fixed and stamping will prevent rotation attack as the stamping is meaningful on the share.

4. CONCLUSION

The image contains many essential information and are communicated securely over the internet. Recursive Visual secret sharing (VSS) is a cryptographic method, which encodes multiple shares into a single share and these shares shared with participants. To reconstruct the secret image, participant has to stack all the share together. Secret message 1 and secret message 2 can be revealed by the share 1 but original secret message can be revealed only if share 2 is there. In this paper, we proposed Super resolution based Recursive VSS scheme that reconstructs multiple secret images with better quality. The results depicted that the recovered secret image is of with a better PSNR, MSE and SSIM. Although the proposed method gives better image quality but when it comes to image document it suffers from many artifacts and needs improvement. However, the colored image quality is improved as compared with traditional Recursive Visual Cryptography, the major drawback is the size of the share has increased 3 times as compared to original image. Furthermore, Image quality assessment became efficient with Color-based Structural Similarity (CSSIM). The encryption part provides more security by restructuring the share because it is arduous to find the number of divisions of a share and how they are rearranged. At the decryption end super resolution gives better visual quality of a reconstructed image with fine detailing. The accuracy of almost 92% is achieved for an image reconstructed which is way more than traditional method. Another major advantage of using Deep learning is consistency in outcome which is clearly measured. In future better image can be reconstructed for image of a text document and CNN can help in the same by correct prediction of information.

5. REFERENCES

[1] Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology { EUROCRYPT '94", A.DeSantis, ed., Lecture Notes in Computer Science 950 (1995), 1-12

[2] E. Biham and A. Itzkovitz, "Visual cryptography with polarization," in *RUMP Session of CRYPTO'98*, 1997.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] College of Engineering, Aurangabad, M.S., India"Survey of Visual Cryptography Schemes" International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[4] Mrs.Jesalkumari Varolia , Dr.R.R.Sedamkar, Recursive Visual Cryptography for Multiple Secret Image Sharing, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-X, Issue-X

[5] A Verifiable Visual Cryptography Scheme Using Neural Networks Deng Yuqiao1,a , Song Ge2,

[6] Dian, R., Li, S., Guo, A., Fang, L.: Deep hyperspectral image sharpening. IEEE Trans. Neural Netw. Learn. Syst. 99, 1–11 (2018)

[7] Dong, C., Deng, Y., Change Loy, C., Tang, X.: Compression artifacts reduction by a deep convolutional network. In: Proceedings of the IEEE International Conference on Computer Vision, pp. 576– 584 (2015)

[8] Dong, C., Loy, C.C., He, K., Tang, X.: Image super-resolution usingdeep convolutional networks. IEEE Trans. Pattern Anal. Mach.Intell. 38(2), 295–307 (2016)

[9] Duarte, A., Codevilla, F., Gaya, J.D.O., Botelho, S.S.: A dataset to evaluate underwater image restoration methods. In: OCEANS 2016-Shanghai, pp. 1–6. IEEE (2016)

[10] Eskicioglu, A.M., Fisher, P.S.: Image quality measures and their performance. IEEE Trans. Commun. 43(12), 2959–2965 (1995)

[11] Fan, D.P., Lin, Z., Zhang, Z., Zhu, M., Cheng, M.M.: RethinkingRGB-D salient object detection: models, data sets, and large-scalebenchmarks. IEEE Trans Neural Netw Learn Syst (2020)

[12] Fu, K., Fan, D.P., Ji, G.P., Zhao, Q.: Jl-dcf: Joint learning and densely-cooperative fusion framework for rgb-d salient object detection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3052–3062 (2020)

[13] He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for imagerecognition. In: Proceedings of the IEEE Conference on ComputerVision and Pattern Recognition, pp. 770–778 (2016)

[14] Hou, Y.C., Quan, Z.Y., Tsai, C.F., Tseng, A.Y.: Block-based progressive visual secret sharing. Inf. Sci. 233, 290–304 (2013)

[15] Martin, D., Fowlkes, C., Tal, D., Malik, J.: A database of humansegmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics. In:Proceedings of 8th International Conference Computer Vision,vol. 2, pp. 416–423 (2001)

[16] Mhala, N.C., Jamal, R., Pais, A.R.: Randomised visual secretsharing scheme for grey-scale and colour images. IET ImageProcessing 12, 422–431(9) (2018). http://digitallibrary.theiet.org/content/journals/10.1049/iet-ipr.2017.0759

[17] Mhala, N.C., Pais, A.R.: Contrast enhancement of progressivevisual secret sharing (PVSS) scheme for gray-scale and colorimages using super-resolution. Sig. Process. 162, 253–267 (2019)

[18] 26. Naor, M., Shamir, A.: Visual cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques, pp. 1–12. Springer, Berlin (1994)

[19] Nocedal, J., Wright, S.J.: Numerical Optimization, 2nd (2006) 28. Shivani, S.: VMVC: verifiable multi-tone visual cryptography. Multimedia Tools Appl., pp. 1–20 (2017)

[20] Timofte, R., De Smet, V., Van Gool, L.: Anchored neighborhood regression for fast example-based super-resolution. In: Proceedings of the IEEE International Conference on Computer Vision, pp. 1920–1927 (2013)

[21] Hou, Y.C., Quan, Z.Y.: Progressive visual cryptography with unexpanded shares. IEEE Trans. Circuits Syst. Video Technol. 21(11),1760–1764 (2011)

[22] Timofte, R., De Smet, V., Van Gool, L.: A+: Adjusted anchored neighborhood regression for fast super-resolution. In: Asian Conference on Computer Vision, pp. 111–126. Springer, Berlin (2014)

[23] Wang, R.Z.: Region incrementing visual cryptography. IEEE Signal Process. Lett. 16(8), 659–662 (2009) 32. Wang, R.Z., Lee, Y.K., Huang, S.Y., Chia, T.L.: Multilevel visual secret sharing. In: Innovative Computing, Information and Control, 2007. ICICIC’07. Second International Conference on, pp. 283– 283. IEEE (2007)

[24] Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error diffusion. IEEE Trans. Inf. Forensics Secur. 4(3), 383–396 (2009).

[25] Mohammed Hassan, Chakravarthy Bhagvati ‘Structural Similarity Measure for Color Images’, April 2012 International Journal of Computer Applications.