Secret Image Sharing using Visual Cryptography Shares with Acknowledgement

Chandra Sekhar Sanaboina, Srinivasa Rao Odugu, Girish Vanamadi

Abstract*— *Visual Cryptography is an encryption technique in which the secret image is encoded and divided into n meaningless images called shares. The shares look like black and white dots embedded randomly in an image. These shares don't reveal any information about the original image. Every share was printed on transparent paper and decrypted through the superimposition of shares without any computer decryption algorithm. When all n shares were overlapped, the original picture would appear. A (k, n)-threshold visual cryptography is a technique in which n is the maximum number of shares that are to be generated and k is the minimum number of shares that are required to decrypt the original image. If the insufficient number of shares, which are less than the k value is given to the decryption function, the decryption function will generate the output, which doesn't reveal any clue to the original image. This paper presents how the Entropy, Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR) values varies with respect to given same image of different sizes.

Index Terms*— *shares, visual cryptography, visual secret sharing

I. INTRODUCTION

The model of entropy is related to the amount of disorder in a physical system. Shannon redefined the entropy as a degree of the amount of information (uncertainty) in a source [1]. If the source is an image, it can be seen as a 2D array of data. PSNR and MSE are the error metrics used to compare image compression quality. MSE represents the cumulative squared error between the compressed and the original image. Peak Signal to Noise Ratio is often used as a quality measurement between the original and a compressed image. The quality of the image increases with the increase in PSNR value.

In the Secret Sharing scheme, a secret message which is in text form is encrypted and randomly distributed to the *n* number of the participants which are called shares. The secret shares that are distributed to the participants look like a randomly generated text and don't provide any clue to the secret message. To get the original message, all the *n* participant's shares are required or at least *k* number of participant's shares are required. The value of *k* and *n* are determined at the time of encryption. The value of *n* should be greater than or equal to *k*. Any qualified combination of shares whose value greater than or equal to *k* can reconstruct the secret. .

The set that consists of qualified combinations of shares is called a qualified set. The set that consists of forbidden combinations is called forbidden set respectively, and the access structure is a pair of the qualified and forbidden sets [2]. An example of Secret sharing schemes is the (k, n) visual Secret Sharing scheme [3] in which a secret picture is encoded into n meaningless shares so that any k-1 shares cannot reconstruct the secret picture, while shares greater than or equal to k will reveal the secret.

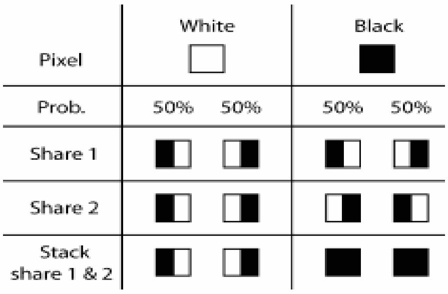


Fig.1. (2, 2) Visual cryptography model

In (2, 2) visual cryptography two shares are generated and all the two shares are required to reconstruct the original image [3]. The size of the decrypted image with respect to the height and width of the original image is doubled because of the pixel expansion. One pixel in the original image is replaced with two pixels in the share images and also in the decrypted image. The pixel expansion in this model is two. Initially, the original image is converted into a binary image. In Matlab im2bw() is a function that converts an image into a binary image. The white pixels and black pixels are represented by zeros and ones in a binary image. In (2, 2) Visual cryptography model base matrix S_1 is for black pixel expansion and S_0 is for the white pixel expansion. The matrices C_{11} and C_{12} are obtained by column permutation of S_1. The matrices C_{01} and C_{02} are obtained by column permutation of S_0.

For (2, 2) visual secret sharing scheme, S_0 and S_1 are defined as follows:

$$S_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

As such, therefore, C_{01}, $C_{02,}$ C_{11} and C_{12} will be as follows:

Manuscript published on 30 September 2019.
***Correspondence Author(s)**
Chandra Sekhar Sanaboina, Department of Computer Science and Engineering from JNTU-K, Kakinada.
Srinivasa Rao Odugu, Department of Computer Science and Engineering from JNTU-K, Kakinada.
Girish Vanamadi, Department of Computer Science and Engineering from JNTU-K, Kakinada.

Retrieval Number: K25620981119/19©BEIESP
DOI: 10.35940/ijitee.K2562.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

$$C_{01}=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} C_{02}=\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$$

$$C_{11}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} C_{12}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Two zeros array of size twice than the original image with respect to height and width are created for generating shares. Zeros array is an array that contains all zeros. Original image pixels are needed to be traversed when a white pixel is found one of the matrices from C_0 is selected that is either C_{01} or C_{02} is selected. The first row from the selected matrix is substituted in the share1 and the second row from the selected matrix is substituted in share2. When a black pixel is found one of the matrices from C_1 is selected that is either C_{11} or C_{12} is selected and substituted in shares. This process is repeated for all the pixels in the original image. Both column-wise and row-wise column expansion is to be done. If only the column expansion is done the quality of the decrypted image will be reduced and looks like a stretched image. In (2, 2) model if both column and row expansion is done, then one pixel got replaced with four pixels. OR operation is performed between the shares to reconstruct the original image.

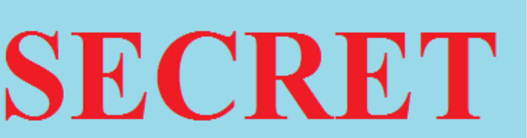


Fig.2. Original Image

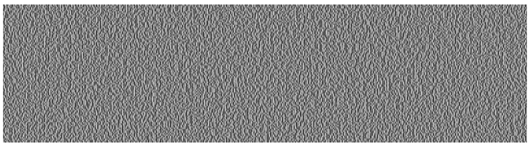


Fig.3: Share1

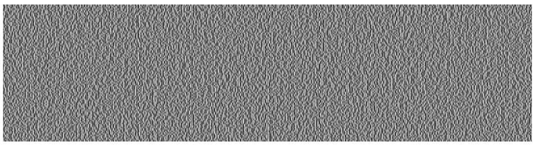


Fig.4. Share2

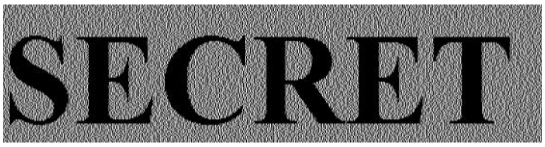


Fig.5. Decrypted Output

In (2, n) Visual cryptography model *n* shares will be generated and any two of the *n* shares are required to reconstruct the original image [4]. In (2, n) visual cryptography base matrix S_0 should have (n-1) columns of weight 'n'. All the Remaining columns are assigned with zeros. Here 'n' is the maximum number of shares that are to be generated. Number of rows and columns are determined by the value *n*. Base matrix S_1 should have $S_{ij}=0$ if i=j and $S_{ij}=1$ if i≠j. C_0 and C_1 are obtained by column permutation of S_0 and S_1. Eliminate the matrices that are having the same values. Exchanging the column one with three and three with one yield the same result.

For (2, 3) visual secret sharing scheme, S_0 and S_1 are defined as follows:

$$S_0=\begin{pmatrix}0 & 1 & 1\\ 0 & 1 & 1\\ 0 & 1 & 1\end{pmatrix} S_1=\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}$$

As such, therefore, C_0, C_1 will be as follows:

$$C_0 = \{\begin{pmatrix}0 & 1 & 1\\ 0 & 1 & 1\\ 0 & 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 0 & 1\\ 1 & 0 & 1\\ 1 & 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1 & 0\\ 1 & 1 & 0\\ 1 & 1 & 0\end{pmatrix} \begin{pmatrix}0 & 1 & 1\\ 0 & 1 & 1\\ 0 & 1 & 1\end{pmatrix}\}$$

$$C_1 = \{\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{pmatrix} \begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 0\end{pmatrix} \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\end{pmatrix} \begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}\}$$

In (n, n) Visual cryptography model *n* shares will be generated and all of the *n* shares are required to reconstruct the original image. The size of matrices S_0 and S_1 should be n*2^{n-1}(if n=3 then 3rows x 4cols). All 2^{n-1} columns should have an even number of one's in S_0. All 2^{n-1} columns should have an odd number of one's in S_1. No two rows should be the same in both S_0 and S_1 .C_0 and C_1 is obtained by column permutation of S_0 and S_1. For (3, 3) visual secret sharing scheme, S_0 and S_1 are defined as follows

$$S_0=\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 0 & 1 & 1 & 0\end{pmatrix} \quad S_1=\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\end{pmatrix}$$

As such, therefore, C_0, C_1 will be as follows:

$$C_0 = \{\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 0 & 1 & 1 & 0\end{pmatrix} \begin{pmatrix}0 & 0 & 1 & 1\\ 1 & 0 & 0 & 1\\ 1 & 0 & 1 & 0\end{pmatrix}$$

$$\begin{pmatrix}1 & 0 & 1 & 0\\ 1 & 1 & 0 & 0\\ 0 & 1 & 1 & 0\end{pmatrix} \begin{pmatrix}0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\\ 0 & 1 & 1 & 0\end{pmatrix}$$

$$\begin{pmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 0 & 1\\ 1 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\end{pmatrix}\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\\ 0 & 1 & 0 & 1\end{pmatrix}\}$$

$$C_1 = \{ \begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\end{pmatrix} \begin{pmatrix}0 & 0 & 1 & 1\\ 1 & 0 & 0 & 1\\ 0 & 1 & 0 & 1\end{pmatrix}$$

$$\begin{pmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\end{pmatrix} \begin{pmatrix}1 & 0 & 1 & 0\\ 1 & 1 & 0 & 0\\ 1 & 0 & 0 & 1\end{pmatrix}$$

$$\begin{pmatrix}0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\\ 1 & 0 & 0 & 1\end{pmatrix} \begin{pmatrix}0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 1 & 0 & 0\end{pmatrix} \begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\end{pmatrix}\}$$

II. RELEATED WORK:

Nakajima [5] proposed Extended visual Cryptography with meaningful shares. The shares in this scheme look like meaningful images rather than the ordinary shares with black and white pixels. He developed a system that will take three images as input and generates the two meaningful shares as output. The generated meaningful shares look similar to two of the three images given as input. When the two meaningful shares are given to the decryption function, the original image will be revealed, that is the third image.

Lukac and plataniotis [6] introduce Bit-level cryptography for both grey and color images. Grey or color pixels in an image are converted into binary bits, and then traditional visual cryptography is applied. The algorithm is capable of reconstructing the original secret image correctly.

Nerella[7]used wavelet transformation as a pre-processing to convert color images into grayscale. Instead of the color decomposition technique, the color picture was transformed to grey using a wavelet, and then halftoning was applied to convert it into binary images. Finally, a traditional 2 out of 2 visual cryptography scheme was implemented for encryption. Their solution does not address the need for visual cryptography in color because the revealed secret is a binary image

Duo Jin [8] suggested a progressive visual cryptography system. The authors propose visual cryptography techniques for both color and greyscale. In this scheme, lossless decryption is achieved by performing the XOR operation between the shares.

In 2012 Tripta Deendayal [9] developed Enhanced Visual Cryptography using color Error diffusion and Digital Watermarking. It is a new visual cryptography scheme in which the user may hide the secret data in a secret image, and the secret image is divided into shares. Error diffusion technique is used to enhance the quality of the image concerning the size. The original image can be regained by stacking the shares which are higher than the *k* value.

III. PROPOSED SYSTEM

We have developed the (k, n) Visual scheme using K out of K scheme[10]. In the proposed model a maximum of four shares will be generated and minimum of two shares are required to decrypt the original image .The proposed system provides acknowledgement to the sender after the receiver has decrypted the image.

Consider a starting n × l matrix SM (n,1, k) whose entries are elements of a ground set {a1, a2,..,ak} with the property that ,for any subset of k rows, there exists at least one column such that the entries in the k given rows of that column are all distinct, where l is the whiteness of a black pixel. If there exists a SM(n,1, k) , then there exists a k-out-of- n VCS with pixel expansion m =1*2k −1 . The n×m basis matrices S_0 and S_1 are constructed by respectively replacing the symbols a1,a2,...,ak with the 1st, …, kth rows of the corresponding basis matrices of the k out-of-k VCS.

Algorithm for Encryption

Input: Image
Output: 'n' number of shares
Step 1: Convert the input image into a binary image and store the pixel values in a two-dimensional array.
Step 2: Construct the base matrices S_0 and S_1 concerning 'k' and 'n'values.
Step 3: Construct the C_0 which contains all the combinations of white pixels and $C_{1,}$ which contains all the combinations of black pixels from the base matrices.
Step 4: When a white pixel is found in an array, one of the matrices from the C_0 is taken and substituted in the shares.
Step 5: When a black pixel is found in an array, one of the matrices from the C_1 is taken and substituted in the shares.
Step 6: Repeat step4, step5 for all pixel values in the two-dimensional array.
Step 7: Finally, shares are generated and sent to the receiver.

Algorithm for Decryption

Input: 'k' or more number of shares, less than the value of 'n.'
Output: Decrypted Image.
Step 1: Convert the shares into binary images and store the pixel values in two-dimensional arrays.
Step 2: Apply OR operation between the pixel values of different shares.
Step 3: Decrypted Image.
Step 4: Acknowledgement to the receiver through email.

Modules:

A) User Authentication
B) Image encryption and shared to user
C) Image decryption by the receiver
D) Acknowledgement to the receiver

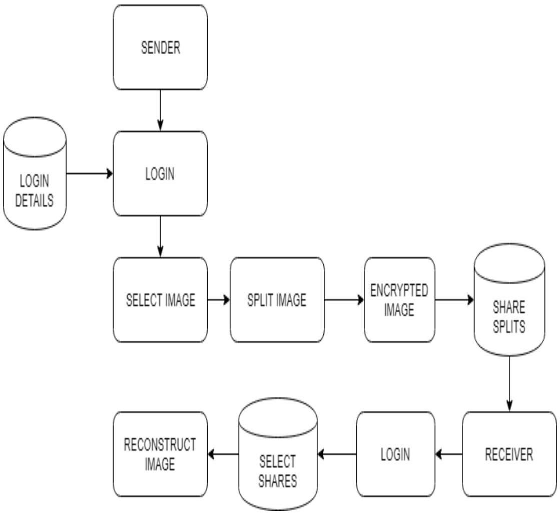
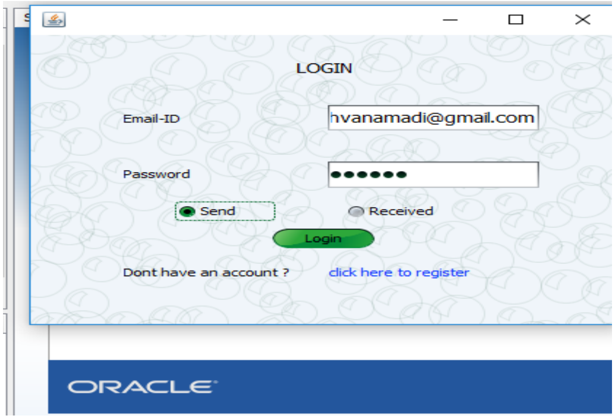


Fig.6. Proposed Architecture

A. User Authentication

Ownership of the user is authenticated here. If the user is new, then the user has to register his details. In the login page, there will be two options, one is the sender, and another is the receiver. If the user selects the sender option and gets logged in, a list of all users is displayed, the user may choose one of the users from the list, and he can send the image to the selected user.

If the user selects the receiver option and gets logged in, the list of messages in the form of encrypted shares that are sent from different users are displayed and he can decrypt the image with the received shares.



LOGIN

Email-ID: hvanamadi@gmail.com

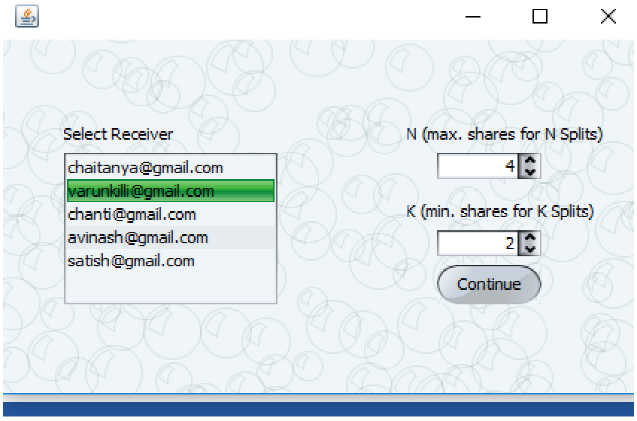
Password: ●●●●●●

● Send ○ Received

Fig.7. Login Page

B. Image encryption and shared to user

In this phase, the original image is split into shares, and that shares are shared to intended receivers. The user should specify the value of *k* and *n* before encrypting the image. The maximum number of shares the user can generate here is four. The value of *k* should be greater than or equal two.



Select Receiver

- chaitanya@gmail.com
- varunkilli@gmail.com
- chanti@gmail.com
- avinash@gmail.com
- satish@gmail.com

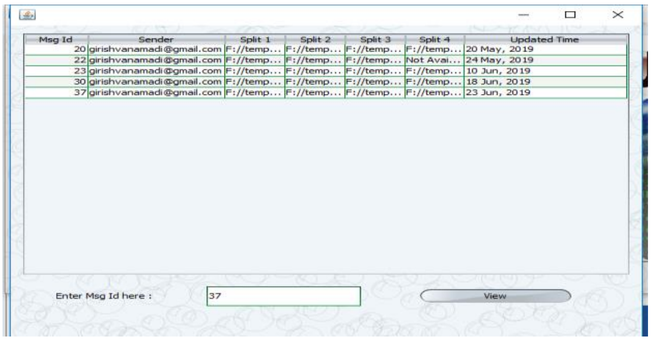
N (max. shares for N Splits): 4

K (min. shares for K Splits): 2

Fig.8. Sender Page

C. Image decryption by the receiver:

After sending splits by the sender, the encrypted images have sent to the shared user's account. The receiver will receive the shares. If the receiver has given the correct number of splits to decryption function, then the image is decrypted, and the user will get the original image.



Msg Id	Sender	Split 1	Split 2	Split 3	Split 4	Updated Time
20	girishvanamadi@gmail.com	F://temp...	F://temp...	F://temp...	F://temp...	20 May, 2019
22	girishvanamadi@gmail.com	F://temp...	F://temp...	F://temp...	Not Avai...	24 May, 2019
23	girishvanamadi@gmail.com	F://temp...	F://temp...	F://temp...	F://temp...	10 Jun, 2019
30	girishvanamadi@gmail.com	F://temp...	F://temp...	F://temp...	F://temp...	18 Jun, 2019
37	girishvanamadi@gmail.com	F://temp...	F://temp...	F://temp...	F://temp...	23 Jun, 2019

Enter Msg Id here : 37

Fig.9. Decryption Page

D. Acknowledgement to the receiver

After decrypting the image by the receiver, the sender who has sent the image to the receiver will get acknowledgment through email that the receiver has decrypted the image.

IV. EXPERIMENTAL EVALUATION & RESULTS

ENTROPY:

If a probability density p is known then entropy can be used to estimate image information content irrespective of its interpretation. Entropy refers to the quantity of uncertainty associated with a specified distribution of probability about an event. It's a measure of disorder. If the level of disorder increases, entropy increases and events are less predictable. Entropy increases when level of disorder increases.

The original image is transformed in to different sizes like 10, 20...100. At each size, the original image is given to encryption function and shares are obtained. Entropy values for the shares at different sizes are calculated.

Table- I: Entropy values for shares obtained at different sizes

image size	Original image	share1	share2	share3	share4
10	7.738829	0.811278	0.811278	0.811278	0.811278
20	7.748898	0.811278	0.811278	0.811278	0.811278
30	7.75577	0.811278	0.811278	0.811278	0.811278
40	7.759799	0.811278	0.811278	0.811278	0.811278
50	7.758768	0.811278	0.811278	0.811278	0.811278
60	7.750169	0.811278	0.811278	0.811278	0.811278
70	7.75382	0.811278	0.811278	0.811278	0.811278
80	7.753571	0.811278	0.811278	0.811278	0.811278
90	7.753019	0.811278	0.811278	0.811278	0.811278
100	7.750197	0.811278	0.811278	0.811278	0.811278

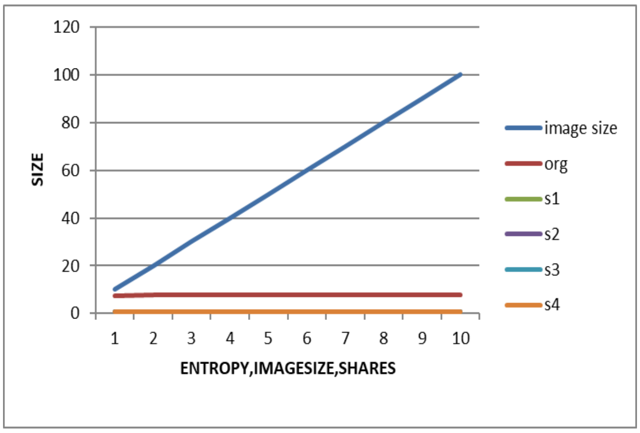


Fig.10. Graph illustrates Entropy values for shares at different sizes.

In Table-I, the entropy value for the shares obtained at different sizes is calculated. The entropy values for the shares remains constant at all sizes, but the entropy value for the original image slightly increases with the increase in size. The entropy value for the original image at size 10 is 7.738829.

The Entropy value of the original image at size 100 is 7.750197. The k value is two, and n value four is taken four for generating the shares.

Table- II: Entropy values for decrypted output obtained by combing different shares at different size

image size	share 1&2	share 1&3	share 1&4	share 2&3	share 2&4	share 3&4	share 1&2&3	share 2&3&4	share 1&2&3&4
10	0.541745	0.541745	0.541745	0.541745	0.541745	0.541745	0.541745	0.541745	0.541745
20	0.543429	0.543429	0.543429	0.543429	0.543429	0.543429	0.543429	0.543429	0.543429
30	0.546206	0.546206	0.546206	0.546206	0.546206	0.546206	0.546206	0.546206	0.546206
40	0.544984	0.544984	0.544984	0.544984	0.544984	0.544984	0.544984	0.544984	0.544984
50	0.545489	0.545489	0.545489	0.545489	0.545489	0.545489	0.545489	0.545489	0.545489
60	0.546176	0.546176	0.546176	0.546176	0.546176	0.546176	0.546176	0.546176	0.546176
70	0.54841	0.54841	0.54841	0.54841	0.54841	0.54841	0.54841	0.54841	0.54841
80	0.548268	0.548268	0.548268	0.548268	0.548268	0.548268	0.548268	0.548268	0.548268
90	0.548548	0.548548	0.548548	0.548548	0.548548	0.548548	0.548548	0.548548	0.548548
100	0.551231	0.551231	0.551231	0.551231	0.551231	0.551231	0.551231	0.551231	0.551231

In table-II, share1 & 2 is the output obtained by combining the share1 and share2. The entropy remains constant at a particular size, for all the images decrypted by combining the different shares. The entropy value for the decrypted output by combining share1 and share2 at size 10 is 0.541745. The entropy value for the decrypted output by combining share1, share2, and share3 at size 10 is 0.541745. So, the quality of the image is the same, even in both cases. The entropy value of the decrypted output by combining share1 and share2 at size 100 is 0.5512310. The entropy value of the decrypted image increases with the increase in the image size.

Mean squared error: MSE is calculated to check if two images are similar or not. MSE values for shares obtained at different sizes are compared and analysed.

$$\text{MSE}=\frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[I(x,y)-I'(x,y)\right]^{2}$$

Table- III:MSE between the shares obtained at different sizes

Image size	share1 & share2	share1 & share3	share1 & share4	share1 & share3
10	16340.41695	16340.41695	16340.41695	16340.41695
20	16262.5217	16262.5217	16262.5217	16262.5217
30	16133.6034	16133.6034	16133.6034	16133.6034
40	16190.39714	16190.39714	16190.39714	16190.39714
50	16166.94097	16166.94097	16166.94097	16166.94097
60	16134.99711	16134.99711	16134.99711	16134.99711
70	16030.8489	16030.8489	16030.8489	16030.8489
80	16037.50141	16037.50141	16037.50141	16037.50141
90	16024.40141	16024.40141	16024.40141	16024.40141
100	15898.80896	15898.80896	15898.80896	15898.80896

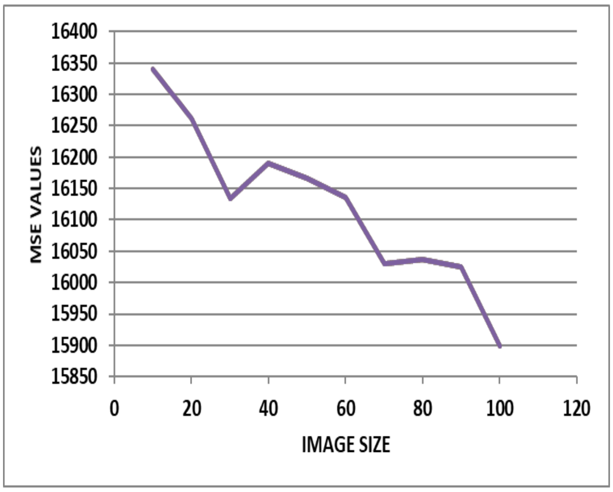


Fig.11. Graph illustrates how MSE value varies between shares at different sizes

In table-III, MSE between different shares at different sizes is calculated. The MSE value between share1 and share2 at size 10 is 16340.41695. The MSE value between share1 and share3 at size 10 is 16340.41695. The MSE value between the share1 and share4 at size 10 is 16340.41965. The MSE value between the share1 and share3 at size 10 is 16340.41965. The MSE value remains constant between the different shares at a particular size.

The MSE value between shares at size 10 is 16340.41695. The MSE value between the shares at size 100 is 15898.80896. The MSE between the different shares decreases when the size of the image increases.

Table- IV :MSE values between decrypted outputs generated by combining different shares at different sizes

image size	org & org	share12 & share13	share12 & share14	share12 & share23	share12 & share24	share23 & share24	share23 & share34	share123 & share234	share123 & share1234	share123 & share34
10	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0

In table-IV, share12 is the decrypted output obtained by combining share1 and share2. Share 13 is the output obtained by combining share1 and share3.Share123 is the decrypted output obtained by combining share1, share2 and share3. Share1234 is the decrypted output obtained by combining share1, share2, share3 and share4. The MSE between the share12 and share13 at size 10 is 0. The MSE remains zero between the different shares at all the different sizes. If the MSE value between the two images is zero; then, the images are identical.

PSNR – Peak signal to noise ratio (PSNR) is better test because it considers the signal strength. The quality of the image increases with the increase in PSNR value. If the PSNR value between the images is Infinity then both the images are identical images.

$$PSNR = 20 * \log10 (255 / \text{sqrt} (MSE))$$

Table- V: PSNR values between shares at different sizes

Image size	share1 & share2	share1 & share3	share1 & share4	share2 & share3
10	5.998172	5.998172	5.998172	5.998172
20	6.018925	6.018925	6.018925	6.018925
30	6.05349	6.05349	6.05349	6.05349
40	6.038229	6.038229	6.038229	6.038229
50	6.044525	6.044525	6.044525	6.044525
60	6.053115	6.053115	6.053115	6.053115
70	6.081238	6.081238	6.081238	6.081238
80	6.079437	6.079437	6.079437	6.079437
90	6.082985	6.082985	6.082985	6.082985
100	6.117158	6.117158	6.117158	6.117158

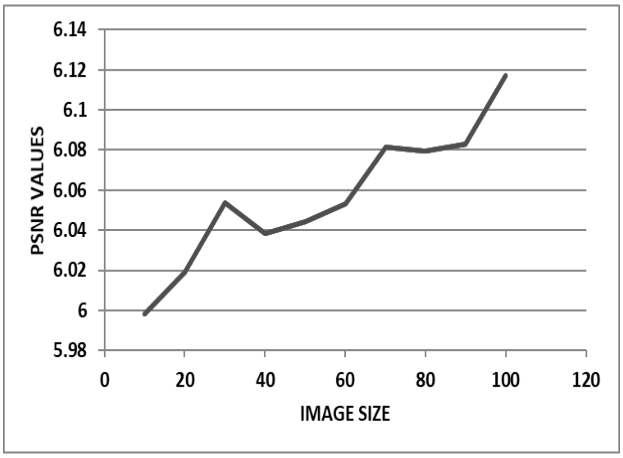


Fig.12. Graph illustrates how PSNR value varies between shares at different sizes

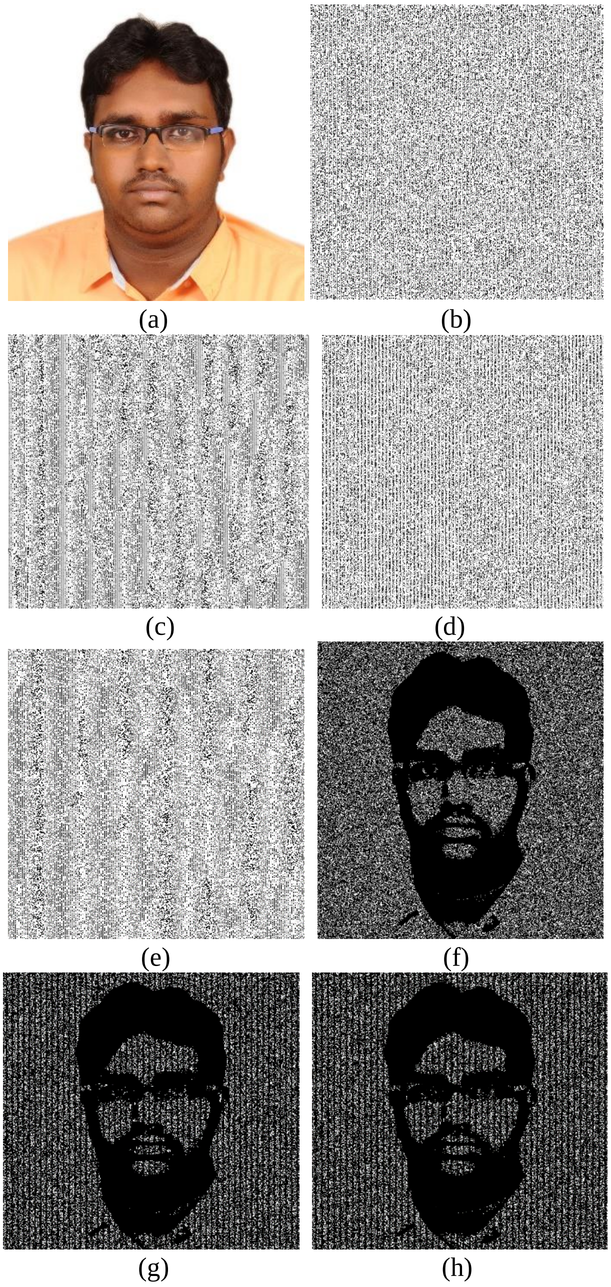
In table-V, PSNR value between different shares at different sizes are analyzed .The PSNR value between share1 and share2 at size 10 is 5.998172.The PSNR value between share1 and share3 at size 10 is 5.998172. The PSNR value between share1 and share4 at size 10 is 5.98172. The PSNR value between share2 and share3 at size 10 is 5.998172.The PSNR value remains constant between different shares at a particular size. The k value is two, and n value four is taken four for generating the shares.

In table-VI, PSNR values between different decrypted outputs is analyzed, which are obtained by combining different shares at different sizes. The PSNR value between the share12 and share 13 at size 10 is Infinity (INF). The PSNR value between the share12 and share 14 at size 10 is Infinity. From this, we can conclude that the outputs obtained in both the case are similar images. The PSNR values remain constant between the shares at all the different sizes.

Table- VI: PSNR values between decrypted outputs obtained by combining different shares at different sizes

Image size	org & org	share12 & share13	share12 & share14	share12 & share23	share12 & share24	share23 & share24	share23 & share34	share123 & share234	share123 & share1234	share123 & share34
10	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
20	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
30	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
40	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
50	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
60	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
70	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
80	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
90	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞
100	∞	∞	∞	∞	∞	∞	∞	∞	∞	∞

Below are the some of the output’s obtained at image size 100 in (2, 4) scheme.



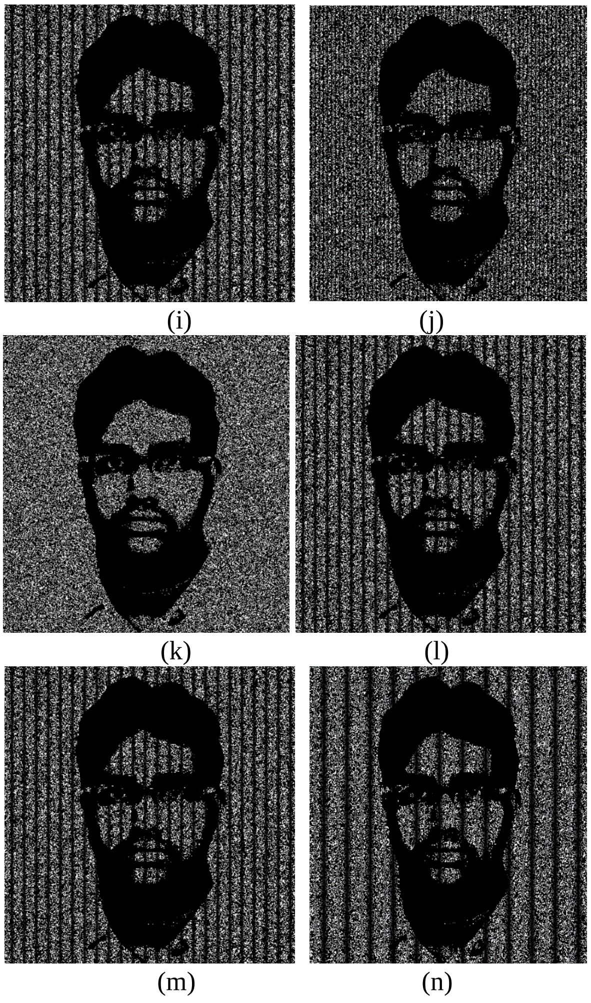


Fig. 12. 2-out-of-4 VCS (a) Original image (b) Share1,(c) share2, (d) share3,(e) share4, (f) share1 +share2, (g)share1+share3, (h)share1+share4, (i)share2+share3, (j)share2+share4, (k)share3+share4, (l)share1+share2+share3, (m)share1+share2+share3+share4, (n)share2+share3+share4

V. CONCLUSION

The security of the visual secret sharing schemes depends up on the column permutation of the base matrices. The shares may reveal the information of the original image if less number of column permutations are taken for the encryption of the image. Both row and column-wise pixel expansion need to be done. If only the row-wise pixel expansion is done, the decrypted output look like the stretched one which reduces the quality of the original image. After the receiver decrypts the shares, the sender will get an acknowledgment through email that the receiver has decrypted the shares. From table-I, for different sizes of the same image, entropy remains constant. From table-IV for different sizes of the same image MSE between decrypted images which are obtained by combining different shares is zero. From this, we can conclude that all decrypted images which are generated are by combining different shares are identical images. From table-VI for different sizes of the same image PSNR between decrypted images is infinity, which are obtained by combining different shares.From this, we can conclude that all decrypted images which are generated by combining different shares are identical.

REFERENCES

1. Shannon, C.E.: The Mathematical Theory of Communication. The Bell System Technical Journal 27, 379–423, 623–656 (1948)
2. Manami Sasaki and Yodai Watanabe, "Visual Secret Sharing SchemesEncrypting Multiple Images."
3. M. Noar and A. Shamir, "Visual cryptography," Advances in Cryptology - EUROCRYPT'94, pp. 1-12, 1995.
4. Doug Stinson, Visual cryptography and threshold schemes, Dr.Dobb’s Journal, pp. 36-43, April 1998.
5. Mizuho Nakajima and Yasushi Yamaguchi, “Extended Visual Cryptography for Natural Images”.
6. Lukac, R & Plataniotis, KN 2005, 'Bit-level based secret sharing for image encryption', Pattern Recognition, vol.38, no.5, pp.767-772
7. Nerella, SK, Gadi, KV & Chaganti, R 2012, 'Securing images using colour visual cryptography and wavelets', International Journal of Advanced Research in Computer Science and Software Engineering,vol.2, no.3
8. Duo Jin, Weiqi Yan, Mohan S. Kankanhalli “Progressive color visualcryptography” Journal of Elecronic Imaging,Vol 14, Issue 3,2005
9. Duo Jin, Weiqi Yan, Mohan S. Kankanhalli “Progressive color visualcryptography” Journal of Elecronic Imaging,Vol 14, Issue 3,2005
10. Abul Hasnat, Dibyendu Barman, Satyendra Nath Mandal.” Implementation K out of N Visual Cryptography using K out of K Scheme.”