Secured Sharing of Digital Images Via Diverse Media

Richu Shibu
PG Student, Dept. CSE.
Christ Knowledge City, Mannoor

Meekha Merina George
Asst. Professor , Dept.CSE
Christ Knowledge City, Mannoor

Leya Elizabeth Sunny
Sr. Grade Assistant Professor
KMEA Engineering College

***Abstract*--Visual Cryptography (VC) is a technique that is gaining its importance in the modern era for sharing secret images. In conventional visual cryptography schemes, secret shares are generated from secret image itself. The proposed work initially creates a cover image based on a key. Feature images are extracted from these cover images. Secret color image is divided into n shares. Each of these n shares is encrypted using the extracted feature image. It is then encoded into Quick Response code for additional security and send to the receiver. We can retrieve the secret image using k secret encrypted shares since we use (k,n) secret sharing algorithm. The method is most useful in sharing passwords in joint bank accounts.**

Index Terms – Visual Cryptography, Shares, Cover Image, Encryption,Quick Reponse Code

I. INTRODUCTION

Data security over internet has been an important challenge for researches and computer engineers for decades. Internet is a great convenience which offers secure data communication of important messages, secret information, variety of images, and documents. In order to prevent unauthorized access of important messages and images from malicious fraudsters, one need to make it more secure by sending encrypted messages over the network. To accomplish and build such secret systems, many data hiding and encryption methods have been proposed. Both data hiding and encryption are found main mechanism in security.

Visual cryptography (VC) is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Moni Naor and Adi Shamir were the developers of this idea in 1994. The basic idea of a visual secret sharing scheme is that an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. The secret images in VCC can be of various types. It can be images, hand written documents, photographs and others. Sharing and delivering secret images is called Visual Secret Sharing (VSS) scheme. Conventional shares consist of many random and meaningless pixels. They satisfy the security requirement for protecting secret contents Shares do not provide any information to identify secret image. The secret image can be retrieved successfully by stacking sufficient number of shares. Shares can even be printed on perforated (transparent) papers. These printed shares when kept correctly over the other will reveal the secret hidden in them. Figure 1.1 shows the basic model of visual cryptography.

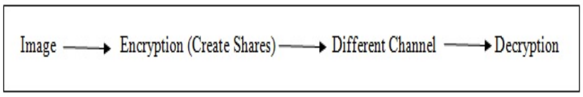
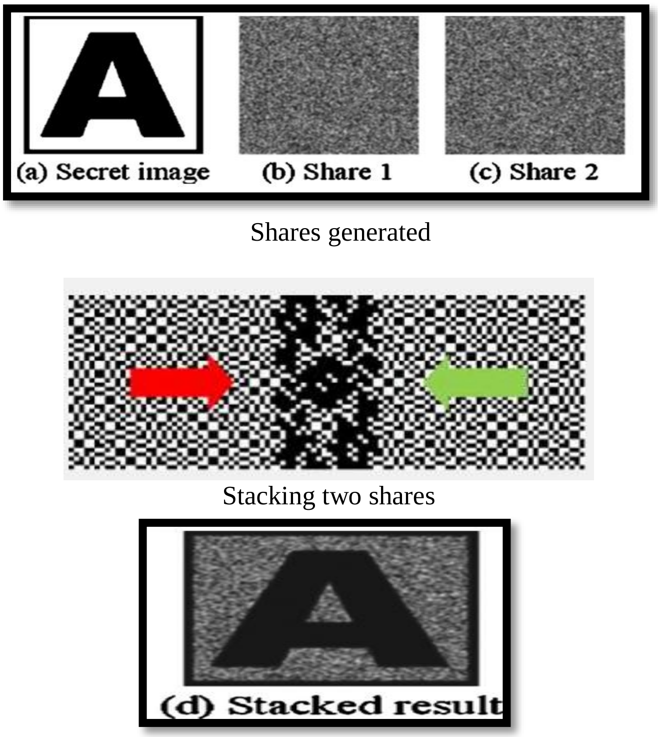


Fig 1. Basic model of Visual Cryptography

Shares generated and the secret image retrieved is shown in the below figure 2.



Shares generated

Stacking two shares

Resultant Image after stacking the shares.

Fig2: Sharing process in visual cryptography.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Applications of Visual Cryptography include

1. Secret data communication
2. Biometric Security.
3. Water Marking.
4. Remote Electronic Voting.
5. Bank Customer Identification.

II RELATED WORKS

Moni Naor and Adi Shamir proposed “Visual Cryptogrphy” [2] in the year 1995 which addresses the problem of communicating secret information via computers over the internet. Paper proposes the method of sharing secret image by dividing the secret into n shares. Only if n shares are stacked together we will be able to decode the message. (n,n) and (k,n) Visual secret sharing scheme is proposed. This is the simplest method of sharing binary secret images. This method assumes that the secret image consist of black and white pixels. Each pixel here is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white sub pixels. The resulting structure can be described by an n x m Boolean matrix S = [Sij] where Sij = 1 if the jth subpixel in the i th transparency is black.Otherwise it is interpreted as white. When transparencies are overlaid together in a way which properly aligns the sub pixels, we see a combined share whose black subpixels are represented by the Boolean "or" of rows i_1 ,i_2,.. in S. The grey level of this combined share is directly proportional to the Hamming weight H(V) of the "or"ed m-vector V. This grey level is interpreted by the visual system of the users as black if hamming weight H(V)> d and as white if H(V) < d - am for some fixed threshold 1 < d < m and relative difference a>0 .

Zhi Zhou, Gonzalo R. Arce et.al proposed paper titled “Halftone Visual Cryptography” in the year 2006 [3]. A novel technique named halftone visual cryptography is proposed to achieve visual cryptography via halftoning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date. Method uses general access structures which is a set of qualified subsets and a set of forbidden subsets. The participants of any qualified subset can jointly decode the secret image, but those from a forbidden subset cannot decode the secret successfully. Both subsets together as a pair is called the access structure. In halftone VC a secret binary pixel is encoded into an array of Q1* Q2 sub pixels, that is referred to as a halftone cell, in each of the shares. Q1*Q2 is thus the pixel expansion in halftone VC. To encode a secret pixel into a halftone cell in each of the two shares, only two pixels, referred to as the secret information pixels, in each halftone cell need to be modified. The secret information pixels should be at the same positions in the two shares. The other pixels in the halftone cell which were not modified are referred to as ordinary pixels. They maintain the halftone information. Selection of the secret information pixels in a halftone cell is important since it affects the visual quality of the resultant halftone shares. To obtain better visual results, the void and cluster algorithm is applied to select these pixel locations. We first apply a low-pass finite-impulse response (FIR) filter to obtain a measure of minority pixel density (m.p.d.) at each minority pixel location. The minority pixel is black/white and the majority pixel is white/black, if the halftone cell contains more white/black pixels. Minority pixel with the highest density is replaced with a majority pixel. The dither pattern is then filtered again by the same low-pass FIR filter to obtain a measure of m.p.d. at each majority pixel location. Majority pixel (different from pixel) with the lowest density, is then replaced with a minority pixel. The void and cluster algorithm, in effect, identifies the minority pixel with the highest m.p.d. and the majority pixel with the lowest m.p.d., and switches their positions. This, in effect, spreads the minority pixels as homogeneously as possible leading to an improved blue noise halftone cell in each share.

Ran-Zan Wang proposed paper titled “Region Incrementing Visual Cryptography” in the year 2009 [4]. This method shares visual secrets with multiple secrecy levels in a single image. Here the entire secret image is divided into n secret levels. In n layer region incrementing VC (RIVC) , the secrecy level of a region has a value ranging from 1 to n ,where the first-level secret is the least significant and the nth level secret is the most significant. The dealer can assign each region of S to a secrecy level according to the specification of her or his application, which represents the degree of secrecy of that region. Unlike all previous VC schemes that adopt a single encoding rule, the basic idea of our RIVC scheme is applying encoding rules called level kernels kernels - one for each secrecy level to encode the secret image. Each level kernel is used to encode the regions belonging to a certain secrecy property.

Thomas Monoth and Babu Anto proposed paper ” Recursive Visual Cryptography Using Random Basis Column Pixel Expansion “ [5] in 2007. The method encodes the secret image into n share images in a recursive manner, that have dimensions of the secret image. The secret image is encoded into n shares such as S1,S2...Sn . The shares S1,S2...Sn are further encoded into subshares as S11,S12...S1p,S21,S22...S2q ... Sn1,Sn2...Snr respectively, where p, q and r be the number of subshares for each share in secret image. Here k out of n scheme, the k is the total number of shares required to recover the SI. Similarly k1,k2...kn be the total number of subshares required to recover the shares such as S1,S2...Sn respectively.A ‘visual recovery’ of the secret image is possible by stacking together the k shares or by xeroxing the k shares onto transparencies, and then stacking them. But the k shares are obtained by overlaying together the subshares associated to k1,k2...kn

Young-Chang Hou introduced Visual Cryptography Using Color Images [6] in the year 2003 The additive and subtractive models are commonly used to describe the constitutions of colors. In the additive system, the primaries are red, green and blue (RGB), with desired colors

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

being obtained by mixing different RGB components. When we control the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. More the mixed colored-lights, the higher is the brightness of the light. When mixing all red, green and blue components with equal intensity, it will result in white color.

Zhongmin Wang and Gonzalo R. Arce prposed “Halftone Visual Cryptography Through Error Diffusion” in the year 2006 [7]. Halftone VC is built upon the basis matrices and collections available in conventional VC.A secret binary pixel p in halftone VC is encoded into an array of Ql x Q2 sub-pixels, which is referred to as a halftone cell, in each of the n shares. The pixel expansion in halftone VC is thus Ql x Q2. Void and cluster algorithm is used for selecting secret information pixels. Using error diffusion the quantization error at each pixel is filtered and fed back to the input. The quantization error on one pixel is diffused away to the neighboring grayscale pixels through a error filter. The error diffusion noise is high frequency or "blue noise" in nature and it produces halftone images with better image quality.

Young-Chang Hou and Zen-Yu Quan proposed paper titled “Progressive Visual Cryptography with Unexpanded Shares” in the year 2011 [8]. It makes use of 2 n*n matrices denoted by C0 and C1 which represents the sharing matrix for white and black pixels of the secret image, respectively. Each row in matrix C0 or C1 represents a sharing method, and each column represents the value assigned to every participant In matrix C0 , the first row is assigned to 1, and other rows are all 0. On the contrary, matrix C1 is a diagonal matrix, which means 1 is assigned to the diagonal line and the rest elements are all 0. During the dispatching process, random numbers ranging from 1 to n are needed to create shares. To share a white pixel of the input image, we choose a random number l, and distribute the values of the lth row vector of C0 to every share. Same is carried out with C1 to share black pixel. With the increase of the numbers of shares being overlaid, the contrast between white and black regions will be increased, hence the content of the secret image is revealed progressively.

Rezvan Dastanian and Hadi Shahriar Shahhoseini proposed “Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares” in the year 2011 [9]. In the case of traditional visual cryptographic scheme one secret image is divided between two shares so that by stacking the two shares secret image appears. One drawback of this scheme is the size of the shares is 4 times the size of the main secret image and transmission of the shares through internet needs too storage space and more bandwidth. In this work a new visual cryptography scheme is proposed which transmits the two secret image with the use of two shares. By stacking two shares, secret image I appears and with by rotating one of the shares in 90 degrees in clockwise direction and then stacking the shares will reveal the second secret image II.
Gopi Krishnan S and Loganathan D proposed “Color Image Cryptography Scheme Based On Visual Cryptography in the year 2011 [10]. In proposed scheme the technique of Visual Cryptography is used to securely transmit a color image.A binary image is used as a key to encrypt and decrypt the secret image. The binary image is created using binary image key generation algorithm. Secret image is decomposed into three components based on YCbCr color space. YCbCr indicates brightness,blue-Y and red-Y. Each of these secret image components are then converted into binary images and are then encrypted using binary key image by the XOR operation. This is share1. Now each of these encryptd share is combined which results in share2. This share2 is send to the reciever side. On the reciever side the shares are decrypted and inverse half toning is done to the retrieved binary images to get the monochrome images. Finally all of them are combined to get the secret image back.

Kai Hui Lee and Pei Ling Chiu proposed “Digital Image Sharing By Diverse Image Media” in the year 2014 [11]. This method used multiple cover images and QR code to generate and send the secret share.Cover Images could be digital images or printed images. A feature image matrix was crated from the selected cover images. Encryption was done by the XOR operation of the secret image and the feature image created. Only a single secret share was created. This secret share was then encoded into the Quick Response code. QR code is send to the receiver side along with the cover images. On the receiver side the feature images are again created and is XOR ed with the secret share that is decoded from the QR code. After the XOR operation we get the secret image back.

III PROPOSED METHOD

In the proposed method a new technique for secure image transmission is discussed, which creates cover images within the system at first with a secret key. Cover images are not directly used for encryption. But we extract feature matrices from the cover images used. This feature matrix is used for encryption of secret image. Color secret image uses (k,n) secret sharing scheme to generate shares. Each of the n shares are xor ed with the feature images created to generate the encrypted secret share. The generated share is concealed with QR codes. This increases the security level during transmission phase. QR code is then to receiver side along the required keys to generate the feature image and to create cover images. Only if sufficient QR codes are available we will be able to retrieve the secret image back. On the receiver side first the QR code is decoded. Using the same key we can create the cover images. Then feature images can be created. Feature images and the encrypted shares are xord to get the secret shares. We use (k,n) secret recovery scheme to retrieve the secret image back. We need k encrypted secret shares here. Thus this method becomes an efficient method to share the secret successfully with multiple participants.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

The overall system encryption is shown in the figure below:

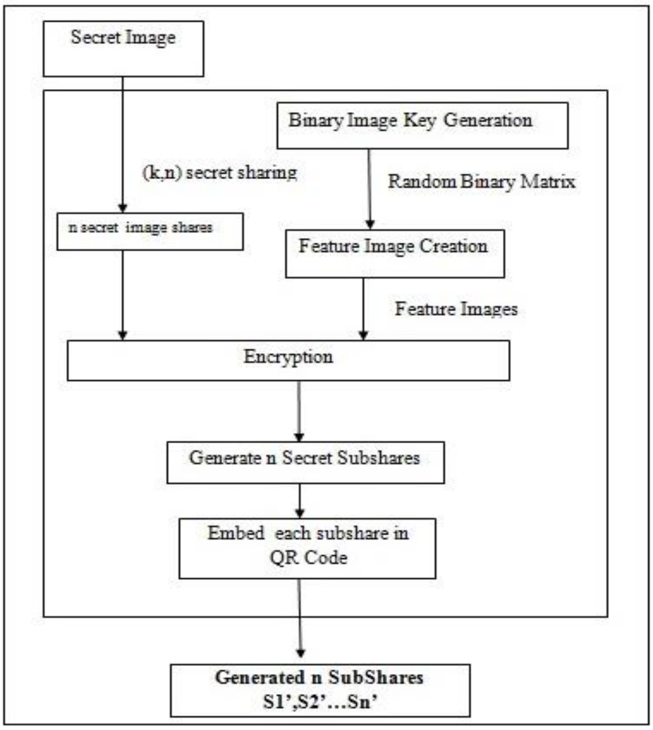

Secret Image
Binary Image Key Generation
(k,n) secret sharing
Random Binary Matrix
n secret image shares
Feature Image Creation
Feature Images
Encryption
Generate n Secret Subshares
Embed each subshare in QR Code
Generated n SubShares S1',S2'...Sn'

Fig2: Sharing process in visual cryptography.

A. *Cover Image Generation*

Initially we generate a cover image by randomly distributed 4x4 matrices with equal number of zero's and one 's. To generate a random matrix image we make use 6 4 x 4 matrices. These 6 matrices are different combinations of zeros and ones. These matrices are stored as arrays. Each time the function is called it will randomly pick any one of the available six matrices. Since each time it is generating a 4 x 4 matrix, therefore it needs to be called only half the times the total height and width of the entire secret image. To generate a color cover image matrix, we call this algorithm for each of the RGB color 8 times.

Cover Image Generation Algorithm

```
Input h,w,key
Output Cover Image N
Initailise an array m as below:
  m[1]={00;11} m[2]={11:00} m[3]={10;10}
  m[4]={01;01} m[5]={10;01} m[6]={01;10}
CurRows[]={}; N={}
for i=1 to h/2
  for j=1 to w/2
    CurRows={CurRows m [rand(6)]}
  end
  N={N; CurRows}
  CurRows={};
end
end
Output N
```

B. *Feature Extraction from Cover Image*

Unlike many other methods known we are not directly using the cover image as such to encrypt secret. The cover image is left untouched. First we take each cover image and divide it into blocks of size b x b. Main steps in feature image creation or feature extraction (FE) are binarization, stabilisation and chaos. A binary matrix is first created from the cover image using binarization. For this we find the median of the pixel values in each block. Those pixel values greater than or equal to that median value is considered 1 and all others are considered 0. For this first we need to calculate $H^{x,y}$ which denotes the sum of red green blue values of each pixel in the entire image.

$$H^{x,y} = P^{x,y}{}_R + P^{x,y}{}_G + P^{x,y}{}_B \qquad (1)$$

$P^{x,y}{}_R$, $P^{x,y}{}_G$, $P^{x,y}{}_B$ in the above equation is the pixel intensity values for red , green and blue components of the image. The threshold function used to convert image into binary form $f^{x,y}$ is defined below where M denotes median of all pixel values in a block.

$$f^{x,y} = F(H^{x,y}) = \begin{cases} 1, H^{x,y} >= M, \\ 0, \text{Otherwise.} \end{cases} \qquad (2)$$

Stabilization balances the number of 1s and 0s. This step improves the appearance probability of the extracted image. Number of unbalanced black pixels is given by the equation:

$$Q_S = \sum_{\substack{\forall x1 \le x \le xb \\ \forall y1 \le y \le yb}} f^{x,y} - (b^2/2) \qquad (3)$$

Chaos process eliminates the texture that may appear on the extracted feature image. Chaos selects randomly Q_c pixels which are 1s and 0s and interchange their values. The value of Q_c with noise P_{noise} will be as calculated using equation below.

$$Q_c = (b^2 / 2) \times P_{noise} \qquad (4)$$

Feature Extraction Algorithm (FE)

```
Input N, b, $P_{noise,}$ sd
Output F
1. Divide N into b*b blocks
2. For each block repeat steps 3-11
3. For each pixel in a block calculate $H^{x,y}$
4. Calculate M
5. Determine $f^{x,y}$ for each pixel.
6.  Calculate Qs
7.  Randomly select Qs pixels where $f^{x,y} = 1$ & $H^{x,y} =M$ and
    let  $f^{x,y} =0$
8.  Calculate Qc
9.  Randomly select Qc pixels where $f^{x,y} =0$
10. Randomly select Qc pixels where $f^{x,y} =1$
11. Alter the values of pixels selected in step 9 & 10
12.  Output F
```

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

C. (k,n) Secret Sharing Scheme

(k,n) secret sharing method is used for very securely transmitting the secret images. System allows a secret image to be shared among multiple participants. Here each participant gets only a part of the entire secret image. Only if sufficient number of secret image sub shares is used we will be able to retrieve the secret correctly. So nobody alone can break the secret. This is achieved by using (k,n) secret sharing scheme to transmit the secret. It is a form of secret sharing, where a secret is divided into different parts, giving each secret holder his own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Combining sub shares from all participants together to retrieve the secret might be impractical always, and therefore sometimes the threshold scheme is used where k of the parts are sufficient to reconstruct the original secret. The goal is to divide secret share S into n pieces of data S1,S2..Sn in such a way that knowledge of k pieces of secret makes the computation of the secret image easy. But knowledge of k-1 or fewer secret sub share (secret) pieces leaves S completely undetermined. If k=n , then all participants are required to reconstruct the secret.

Secret Sharing Algorithm

Input Secret Image S, number of participants n, threshold k≤ n
Output n secret shares sh.

1. Divide each pixel value of secret image into two halves d and c.
2. Choose a number p which is larger than d.
3. Select n distinct real values $x_1, x_2 \ldots x_n$
4. Use the following (k-1) degree polynomial to compute n function values $F(x_i)$ called partial shares for i=1, 2, ..n.

$$F(x_i) = \left(d + cx_i + c\,x_i^2 + \cdots + c\,x_i^{k-1}\right) mod\ p \qquad (5)$$

5. Deliver (x_i, $F(x_i)$) as share to ith participant where I= 1,2..n.

$F(x_i)$ is the pixel value that will appear in ith share. This is calculated for all shares.

D. Encryption

Each of the n shares is separately encrypted with the feature image created before. The encryption is done by xor operation of the corresponding bits. Each of the encrypted shares is compressed using Huffman compression. Then it is embedded into a Quick Response code. This is done to ensure additional protection .

Secret Encryption Algorithm

```
Input: Share,cover image Nh,w,n,t, Pnoise,sd
Output: S'
1: Initialize random number generator G by seed sd
2. For all RGB components initialize FI←0
3. For each cover image
       for each RGB components
          for 0<=i<=7 repeat 4-5
4. f(x,y)=Call Procedure FE(N,b, Pnoise,sd,F)
5. p(x,y)=p(x,y)+f(x,y)*2^i
6. Randomly selects (x1; y1) from feature image;
10: Randomly selects (x2; y2) from feature image;
11. Exchange values of p(x1, y1) and p(x2, y2)
12. For each RGB components S'← Share xor FI1 xor...FI n-1
13: Output S'
```

Here FI1 denotes the feature image created from first cover image FI2 from second cover image and so on.

E. Decryption

In the decryption side we need at least k shares created out of n to successfully retrieve the secret image back. First step is to decode the secret share from the QR code and decompress to get the secret encrypted share. Cover images are create d using the keys and feature images are extracted on the receiver side too. We do the xor operation again between the available k shares and feature images.This gives original secret shares.

k shares can be combined to get retrieve the secret image using the secret recovery algorithm.

Secret Recovery Algorithm

Input: k shares, p
Output: Secret image S

1. Read each of k shares available.
2. Divide each pixels in all k shares into d and c.
3. Use the k shares (x_i, $F(x_i)$) to set up the following equations:

$$F(x_j) = \left(d + c\ x_j + c\,x_j^2 + \cdots + c\,x_j^{k-1}\right) mod\ p \quad (6)$$

Where j = 1, 2, ..., k.

4. Solve the k equations above by Lagrange's interpolation to obtain d as follows:

$$d = ((-1)^{k-1} \begin{bmatrix} F(x_1)\dfrac{x2x3 \ldots xk}{((x1-x2)(x1-x3)\ldots(x1-xk)} \\ + \cdots . + \\ F(x_1)\dfrac{x2x3 \ldots xk}{((xk-x1)(xk-x2)\ldots(xk-xk-1)} \end{bmatrix} mod\ p \quad (7)$$

5. Substitute value of d step 4 and using trial and error find value of c for all pixels.
6. Combine the value of d and c for all pixels to obtain value of each pixel of the original secret image S

The overall system encryption is shown in the figure 3:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

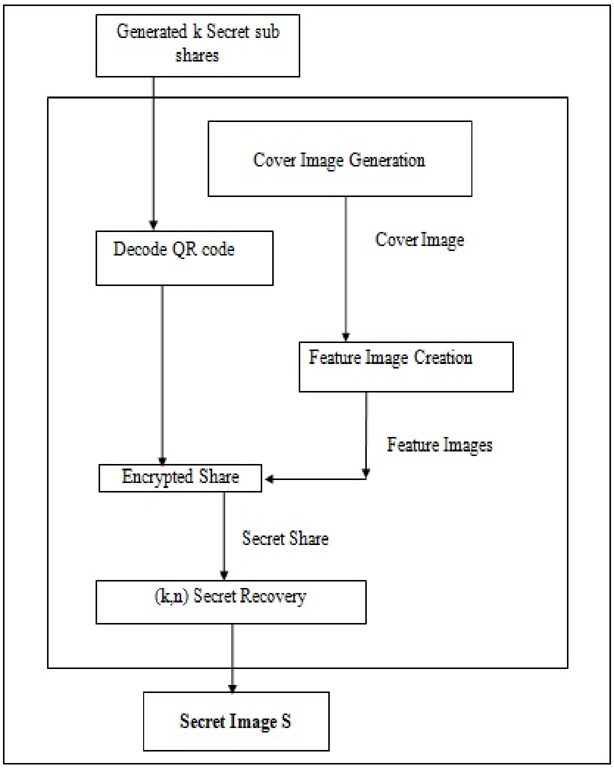


Fig3: Secret Recovery process in visual cryptography

IV EXPERIMENTAL RESULTS

The system implements a very secure method to share the secret or confidential images. Use of (k,n) secret sharing Scheme has increased the security of the entire system. Since the system creates the cover image automatically, therefore the user need not carry them. Method also retrieves the secret image with good clarity.

Entire system is analyzed based on factors like PSNR, correlation analysis and SSIM

Encryption Analysis

Image	Key1	Key2	Key3	Cor.Sh 1	Cor. Sh2	Cor.Sh3
Lena	ab123	bvg45	54321	.001	.008	.006

Decryption Analysis

Image	Key1	Key2	Key3	PSNR	SSIM
Lena	ab123	bvg45	54321	Inf	1

Peak Signal-to- Noise Ratio (PSNR)

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the idelity of its representation. PSNR is an approximation to human perception of reconstruction quality. A higher PSNR generally indicates that the reconstruction is of higher quality. The PSNR value of the decrypted secret image with respect to the original secret image is checked and it is above 30 which indicates that the decrypted secret image is similar to the original secret image.

$$\text{PSNR} = 10 * \log_{10} \left[(\text{MAX}^2) / \text{MSE} \right] \quad (8)$$

$$\text{MSE} = \frac{1}{mn} \times \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (9)$$

Correlation Analysis

The correlation coefficient is a number representing the similarity between two images in relation with their respective pixel intensity. The correlation between an original image and an encrypted image must be low, so that it becomes difficult to guess the value of neighbors of a pixel. For every pixel location in both images, the difference between the intensity value at that pixel and the mean intensity of the whole image is computed. Correlation between two images is calculated by equation below.

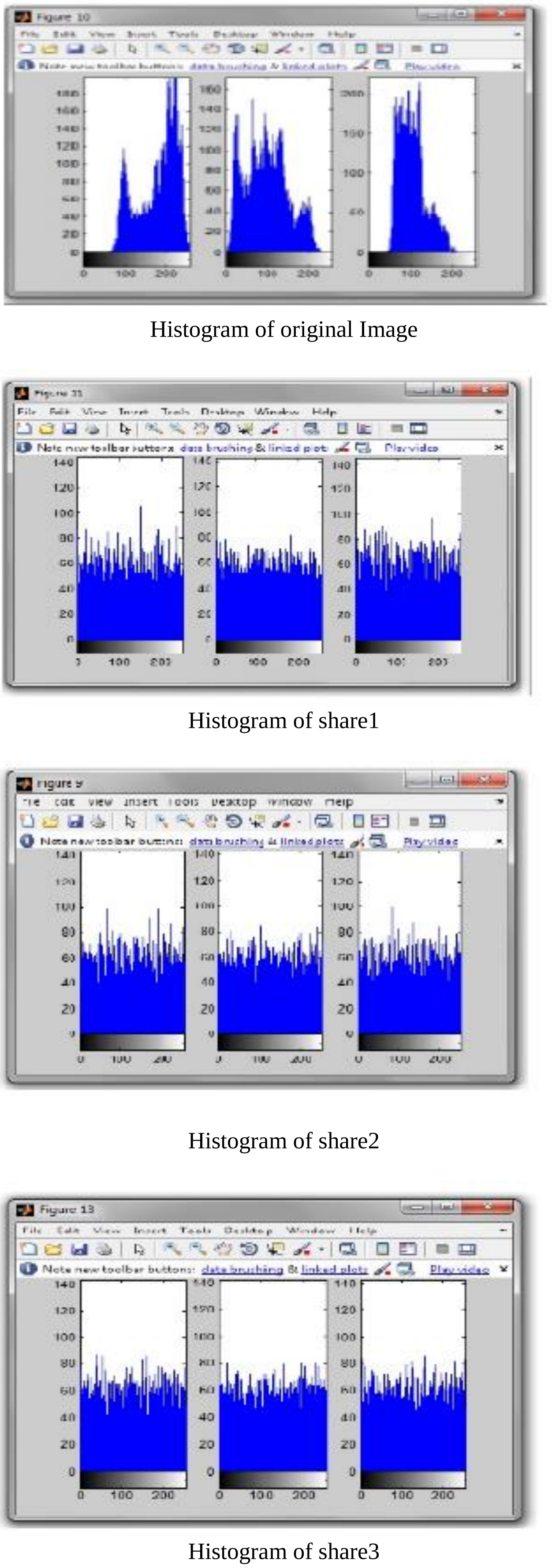
$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}}$$

Here A and B are the images you are comparing, whereas the subscript indices m and n refer to the pixel location in the image .A' and B' indicates the mean intensity of corresponding images.

V CONCLUSION

In today's corporate world, images travel widely and rapidly, in multiple manifestations, through email and across the Internet. Controlling and protecting sensitive images has become very difficult. Proposed method provides a very efficient method to transmit a secret image. It is done based on the technology - Visual cryptography. The system itself generates a cover image based on a key. This cover image is not directly used for encryption. We are extracting a feature image from the cover image. We are applying (k,n) secret sharing scheme to the color secret image. i.e before encryption the secret image is converted to n shares.Each of the share is encrypted with the feature image created to get the encrypted share. They are then hidden inside Quick Response code. QR code is a type of matrix bar code. It stores information in both dimensions. QR code is then send to the receiver side. If k number shares are stacked together, then the secret can be retrieved correctly. Use of (k,n) secret sharing scheme increases the security and applicability of the entire system.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)



Histogram of original Image

Histogram of share1

Histogram of share2

Histogram of share3

Fig.4. Histograms for original image and the shares generated.

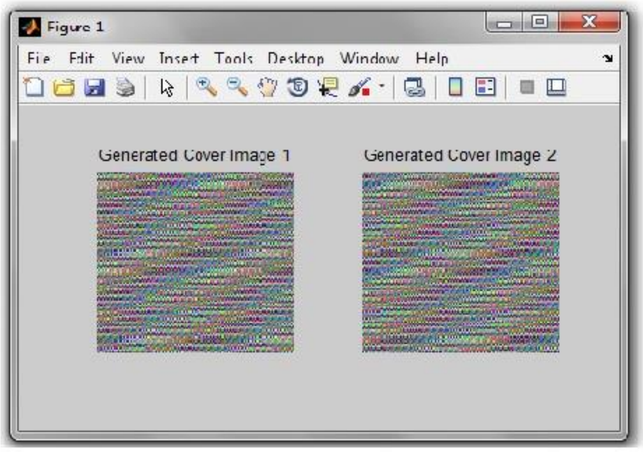


Fig5. Cover images used to send Lena

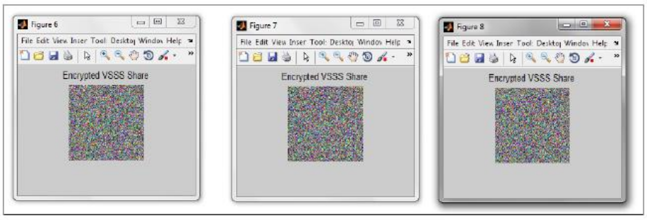


Fig6. Encrypted Shares

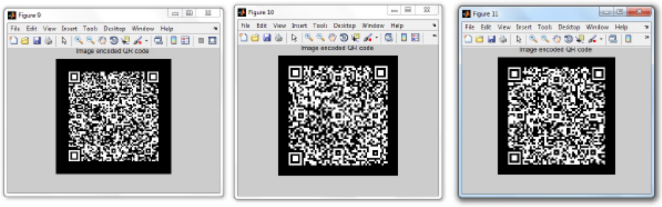


Fig7. QR codes generated for each encrypted shares.

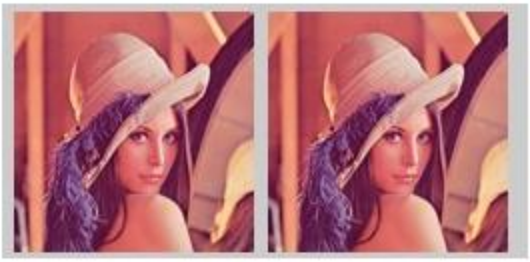


Fig6. Lena on the left is the image send and Lena on right is the retrieved image.

VI. FUTURE WORK

The reliability of the system is improved for high secure communication. In the current method the system only transmits a single secret image. Hence it is required to find a solution. So this needs to be extended to multiple images. Transmission of audio is also an area that can be explored.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

VII. REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu, `Digital Image Sharing by Diverse Image Media", in IEEE, January 2014..

[2] Moni Naor and Adi shamir, ``Visual Cryptography," Springer, 1995.

[3] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, ``Halftone Visual Cryptography," in IEEE, 2006.

[4] Ran-Zan Wang "Region Incrementing Visual Cryptography" in IEEE Signal Processing Letters, Vol. 16, No. 8, August 2009.

[5] Thomas Monoth and Babu Anto "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion " in IEEE , International Conference on Information Technology 2007.

[6] Young-Chang Hou, ``Visual cryptography for color images," in Pattern Recognition,in 2003,pp. 1619 – 1629.

[7] Zhongmin Wang and Gonzalo R. Arce “Halftone Visual Cryptography Through Error Diffusion” IEEE 2006

[8] Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography with Unexpanded Shares", IEEE Transactions On Circuits And Systems For Video Technology, VOL. 21, NO. 11, NOV 2011.

[9] Rezvan Dastanian and Hadi Shahriar Shahhoseini " Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares" IPCSIT vol.6 2011

[10] Debasish Jena and Sanjay Kumar Jena "A Novel Visual Cryptography Scheme " IEEE International Conference on Advanced Computer Control 2008.

[11] John Justin M, Manimurugan S and Alagendran B "Secure Color Visual Secret Sharing Scheme Using Shifting Coefficient with No Pixel Expansion" International Journal of Computer Science and Information Technologies, Vol. 3 2012

(This work is licensed under a Creative Commons Attribution 4.0 International License.)