ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Digital Visual Cryptographical Image Sharing Using DIM

Bhagyashri Machale[1], Prajakta Baravakar[1], Padmashri Thorat[1], Tejshri Bavale[1], Prof.Pankaj Agarkar[2]

U.G. Student, Department of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[1]

Professor, Department of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[2]

ABSTRACT: In this paper, we search technique on how to ameliorate the safety for an original data by hiding important data behind cover image (which may be digital or printed image) by using data hiding, cryptography and NVSS algorithm. The proposed system hides the secret data which is first encrypted and then is hidden behind a one of the patch of a cover image. The total effort of the proposed method is the achievement of hiding and extracting secret images and secret data. In proposed method, we have tried to improve the capacity of the original scheme by improving the capacity of hiding data and increasing security to send image through different media. Our method increase security, efficiency and reliability of the any persons, systems,or organisations important data which is autherised by using data hiding, cryptography method and NVSS algorithm. The natural shares which are unchanged are distinct and inofensive, hence it mainly decreases the risk of traject over communication media. The proposed approach is best for solving the problem of transmission risk for the VSS schemes is shown by experimental results..

KEYWORDS: Digitalimage sharing, Secret image, VSS cryptography, Visual secret sharing.

I. INTRODUCTION

In day to day life sharing information with other person is getting more important. Through network and communication media, we can share the important information like images, text, pictures which are secrete easily. Unauthorized data/personal dataca be access by the Black hackaers. We use certain techniques to solve such problems. Now a days, the environment is computer aided, in such environment sharing secret data like text and images is an important issue . Secret images can be of various types such as handwritten documents, photographs which are shortly called as digital images or printed images. A technique that creates n shares of secrete image by encrypting it ,such as one or more shares are hold by each participant is called as visual cryptography. This technique is used for provide security to important data by using NVSS algorithm, by using feature extraction of digital and printed image. After that it uses the visual cryptography. In that encryption of image, data hiding and decryption are done simultaneously. The major contribution is to decrease the problem of traject dataand provides the user friendliness of biggest range. Major contributions are this is the first attempt to send secret image and data through various carrier media. In enhanced system we can create the segments of the secret image and then will perform the encryption process for all segmented regions, the same process will inversely perform in decryption, in order to achieve the efficient transformation of secret images. A technique that creates n shares of secrete image by encrypting it ,such as one or more shares are hold by each participant is called as visual cryptography. The person or system which holds lesser than *n* shares cannot uncover any type of information about the secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human visual system. The main inspiration of VC is to share secret images more securely in non-computer-aided environments. But Now a days, the environment is computer aided, in such environment sharing secret data like text and images is an important issue hence NVSS is proposed. A unity carrier (e.g., either transparencies or digital images) is used for sharing images by VSS schemes and it creates limits over the practicality of this scheme. Proposed system explores the possibility of using diverse media for sharing digital images and data. The carrier media in the scheme contains digital images, printed images, hand-painted pictures, text and so on. For sharing the secret image using a diversity of media higher the degree of difficulty of intercepting the shares. The NVSS scheme can share a digital secret image over *n* - 1 arbitrary natural images (here after called natural shares) and one share. Instead of altering the contents of the natural images, hiding the secret image behind one of the patch of cover image and for the secret text we create QR image and then hide it behind one of the patch of cover image.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

II. LITURATURE SURVEY

Kai-Hui Lee and Pei-Ling Chiu proposed that Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; But during transmission of the shares there may be interception risk arise. To solve this problem, they proposed a natural-image-based VSS scheme (NVSS scheme). To protect the secret images and participants during transmission NVSS shares secret images through different carrier media. The proposed (*n*, *n*) - NVSS scheme can share one digital secret image over *n* -1 arbitrary selected natural images (called natural shares) and one noise-like share [1].Sunil G. Jare proposed the technique called Visual Cryptography (VC). This technique encrypts a secret image into *n* shares, and every participant involved in this holding one or more shares. The participants who has less number of shares than *n shares* cannot uncover any information about the secret image. This technique is mainly used to avoid transmission risk and to increase security to share data across various carrier media [2].Priyanka R. Pawar, Manjusha S. Borse, proposed Visual Secret Sharing scheme (VSS). To avoid the problem generated by this scheme NVSS is proposed. In this technique they used the concept of OR code. QR code technique is used to encrypt the data by generating QR code of that data [3].MayuriSonkusare, Prof. NitinJanwe proposed A natural-image-based VSS scheme (NVSS scheme) which is use to share secret images during transmission. In this technique feature extraction is performed on natural shares. In this scheme Share-Hiding algorithm is also used in which shares are hide by generating OR code. At the receiver side original image is recovered by using share extraction algorithm and decryption [4]. Miss A ANaphade, Dr. R N Khobaragade, Dr. V M Thakareproposedvisual cryptography (VC). This paper focused on five visual cryptographies i.e. multiple image visual cryptography (MIVC), optimal gray scale reserving visual cryptography (GRVCS), Embedded extended visual cryptography scheme (Embedded EVCS), simulated-annealing-based algorithm.This VC technique is based on black-and-white or binary images. But it will increase interception risk during transmission of the images [5].Mr. Thanguganesh.M and Prof.Sarnaya R proposed system which is used to protect important data from hackers and unauthorized users. In this technique they made use of different types of images like digital image, gray image and natural image [6].

III.MODULE DISCRIPTION

1. IMAGE PROCESSING

Image processing is the method in which input image is crop. Cropping is performed by manually and stored for further processing. The cropped image is resized with predicted size.

2. FEATURE EXTRACTION

Binarization is used to carried out feature extraction of the natural share. It is performed by calculating the median value of the natural share. The stabilization process uses the result of binarization method. The process which is used to balance the number of black and white pixels of an extracted feature image in each block is called stabilization process. The process ensures that the number of black and white pixels in each block is equal. These clustered pixels have the same feature value. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share. The original feature matrix will be disordered by adding noise in the matrix.

There are some existing methods that are used to extract features from images, such as the wavelet transform. However, the appearance of the extracted feature may remain some texture of the original image. It will result in decreasing the randomness of the generated share and eventually reduces security of the scheme. To ensure security of the proposed scheme, we develop a feature extraction method to yield noise like feature images from natural images such that the generated share is also a noise-like image. The feature extraction module consists of three processes —Binarization, stabilization, and chaos processes as shown in Fig. First, a binary feature matrix is extracted from natural image N via the Binarization process. Then, the stabilization balances the occurrence frequency of values 1 and 0 in the matrix. Finally, the chaos process scatters the clustered feature values in the matrix.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Fig 1. The block diagram of the feature extraction

In binarization process, a set threshold is determined by a simple threshold function F to determine a binary feature value. Median M is calculated to obtain approximate appearance for binary values 0 and1.Median M is the threshold value.

In the Binarization process, the binary feature value of a pixel can be determined by a simple threshold function *F* with a set threshold. To obtain an approximate appearance probability for binary values 0 and 1, the median value M of pixels in the same block is an obvious selection as the threshold. Hence, for each block,
We define the notations as follows:
b represents the block size, b .even.
N denotes a natural share.
x, y.denotes the coordinates of pixels in the natural shares and the secret image, 1 .x .w, 1 .y .h.
x1, y1.represents the coordinates of the left-top pixel in each block.
px,y ϕ denotes the value of color ϕ, ϕ._R,G,B.for pixel .x, y.in natural share N, 0 .px,y ϕ .255.
Pixel value Hx,y is the sum of RGB color values of pixel .x, y.in natural share N and Hx,y_px,yR.px,y G .px,y B . (1)
M represents the median of all pixel values (Hx1,y1, . . . ,Hxb,yb) in a block of N.
F is the feature matrix of N, the element fx,y .F denotes the feature value of pixel .x, y_. If the feature value fx,y is 0, the feature of pixel .x, y.in N is defined as black. the extraction function of pixel *x, y_* of N is defined as follows:

$$f^{x,y} = \mathcal{F}(H^{x,y}) = \begin{cases} 1, & H^{x,y} \geq M, \\ 0, & \text{otherwise.} \end{cases}$$

In the stabilization process the number of black and white pixels are balanced in each block the number of unbalanced pixels Qs is calculated by using the formula

$$Q_s = \left(\sum_{\substack{\forall x_1 \leq x \leq x_b \\ \forall y_1 \leq y \leq y_b}} f^{x,y} \right) - \frac{b^2}{2}.$$

In the process, there are Qs pixels in which f x,y = 1 is randomly selected and then the value of these pixels is setto 0. The process ensures that the number of black and white pixels in each block is equal. In a natural image, pixels with the same or approximately the same values may cluster together in a continuous region. These clustered pixels have the same feature value; hence it will lead to the feature image and to the generated share revealing some textures of the natural image in the subsequent encryption process. The chaos process is used to eliminate the texture that may appear on the extracted feature images and thegenerated share. In the process, the original feature matrix will be disordered by adding noise in the matrix. First, randomlyselect Qc black feature pixels (fx,y = 0) and Qc white feature pixels (f x,y = 1) from each block, then alter the value of thesepixels. That is, the feature value of a pixel at coordinates (x,y)will be changed to 0 when f x,y = 1, and vice versa. AssumePnoise be the probability to add noise in the matrix, the value of Qc is as follows:

$$Q_c = b^2/2 \times P_{noise}.$$

Pnoise is the salt and paper noise whose value ranges from 0 to1 here P noise =0.5

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

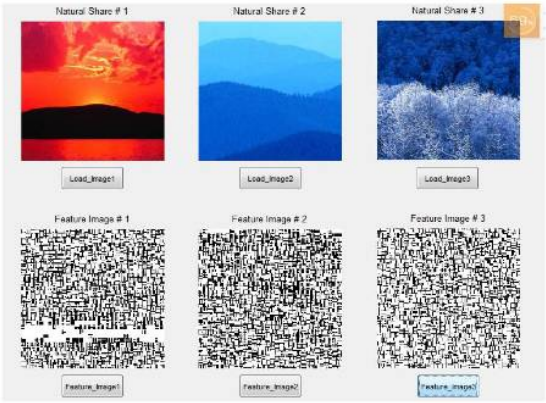


Fig2. Graphical user interface of Feature extraction taking three natural shares at the sender side

Encryption/Decryption:

The (n ,n)-NVSS schemes encrypts a true color secret image by n-1 natural shares and one noise share. Algorithm for encryption/ Decryption as follows.

Input S, N1…..,Nnp+np,np,nd,b,Pnoise ,p,t
Output: S
1. Initialize the random number generator G by the seed p
2. nnP + nd+1
3. 1<= α < n, φ Є (R, G, B), Fl α,φ 0
4. 1<= α < n, φ Є (R, G, B), 0 <= *i*<=*7* repeat steps 5 to 6
5. Call procedure FE(Na,B,Pnoise,F)
6. (X,Y),x Є[1,h],px,y α,φ px,yα,φ+*f* x,y *2i
7.Ifnp=0 then goto step 12
8. 1<= α <np repeat step 9-11 times
9. Randomly select (x1,y1),x1 Є[1,*w*],y1 Є[1,h]
10. Randomly select (x2,y2),x1 Є[1,*w*],y2 Є[1,h]
11. φ Є(R,G,B),exchange value of px1,y1 α,φ and px2,y2 α,φ
12. φ Є(R,G,B), SφSφ F11,φ F1n-1, φ
13.Output S

Algorithm: Feature Extraction Algorithm (FE)

Algorithm (FE)
Input: N,b,Pnoise
Output: F

1. Divide N into blocks with b*b
2. For each block repeat steps 3-11
3. ∀x1≤x≤xb, y1≤y≤yb, calculate Hx,y by eq.(1)
4. calculateM
5. ∀x1≤x≤xb, y1≤y≤yb, determine fx,y by eq(2)
6. calculateQsbyeq(3)
7. randomlyselect Qs pixels where fx,y and Hx,y = M, let fx,y←0
8. calculateQcbyeq(4)
9. randomlyselectcandidatepixelswherefx, y = 1

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

10. randomlyselectcandidatepixelswherefx, y = 0
11. Alter all values of fx,y that were selected in steps 9 and 10
12. Output F

250	200	200	200
185	200	200	160
185	60	90	185
110	80	120	190

(a)

1	1	1	1
0	1	1	0
1	0	0	0
0	0	0	1

(b)

0	1	1	0
0	0	0	1
1	1	1	0
1	0	0	1

(c)

Fig.3.a Encryption process

Fig.3.b.Decryption process

3. ENCRYPTION

In encryption process secret image is encrypted by using cover image concept and for the text QR code is generated .For the secret image ,it is hide behind the one of the patch of the cover image so that attacker can not reveal there is any another image which is hide in that cover image. Text data is encrypted by introducing the concept of OR code. In this OR code of that text is created so that it is difficult uncover original text.

4. DATA HIDING

To hide noise-like shares and to reduce the interception risk during transmission phase Quick-Response Code (QR code) technique is introduced. This code is decoded by smart phones and barcode readers. For the secret communication QR code is used. By using QR code generators the text called secret data is encoded to the QR code, this is called encryption process in which data is encrypted using QR code technique, now the noise share is hidden and a new generated share is obtained by using the Share hiding algorithm. The shares are compressed which is the main theme of this paper called ETC scheme i.e. encryption of the image and then compression of that image. Decryption process is performed at the receiver side which is exact reverse of encryption process. To obtain the original image from compressed image it is decompressed. And then information is extracted from the shares which is hidden. To extract the information share extraction algorithm is used and then original image is obtained.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Fig.4.Compression/hiding process

5. DECRYPTION

By repeating the reversal process of encryption process to predict the secret image. Again feature extraction and pixel swapping performed to predict the secret image.

IV.EXISTING SYSTEM

A. Background

In cryptography, the one-time pad (OTP), which was proven to be impossible to break if used correctly, was developed by Gilbert Vernam in 1917. Each bit or character from the plaintext is encrypted by a modular addition (or a logical XOR operation) with a bit or character from a secret random key of the same length as the plaintext resulting in a cipher text. The cipher text was sent to a receiver; then, the original plaintext can be decrypted in the receiver side by applying the same operation and the same secret key as the sender used for encrypting the cipher text.

B. Assumptions

The proposed (*n*, *n*)-NVSS scheme adopts arbitrary natural shares and one generated share as media to share one digital true color secret image that has 24-bit/pixel color depth. The objective of this study is to reduce the transmission risk of shares by using diverse and innocuous media. We make the following assumptions:

1. When the number of delivered shares increases, thetransmission risk also increases.
2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.
3. The transmission risk decreases as the quality of themeaningful shares increases.
4. The natural images without artificially altered or modified contents have the lowest transmission risk, lower than that of noise-like and meaningful shares.

In the NVSS scheme, the natural shares can be gray
orcolor photographs of scenery, family activities, or evenflysheets, bookmarks, hand-painted pictures, web images, or photographs. The natural shares can be in digital or printed form. The encryption process only extracts features from the natural shares; it does not alter the natural shares. The innocuous natural shares can be delivered by participants who are involved in the NVSS scheme, by the owners of the photographs, or via public Internet. In the existing VSS schemes, the types of shares include noise-like shares, shares with binary cover images, and shares with halftone cover images; the latter has the best display quality among the above-mentioned types of shares. Furthermore, the display quality of the proposed true-color natural shares is superior to that of shares with halftone cover images. Based on Assumptions 2 and 3, the transmission risk of the true-color natural shares is the lowest among the existing approaches. Based on Assumptions 4 and 5, the proposed (*n*, *n*)-NVSS scheme delivers *n* □ 1 unaltered natural shares that have a very low transmission risk, this property greatly reduces the transmission cost of delivering *n* □1 natural shares of the scheme.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

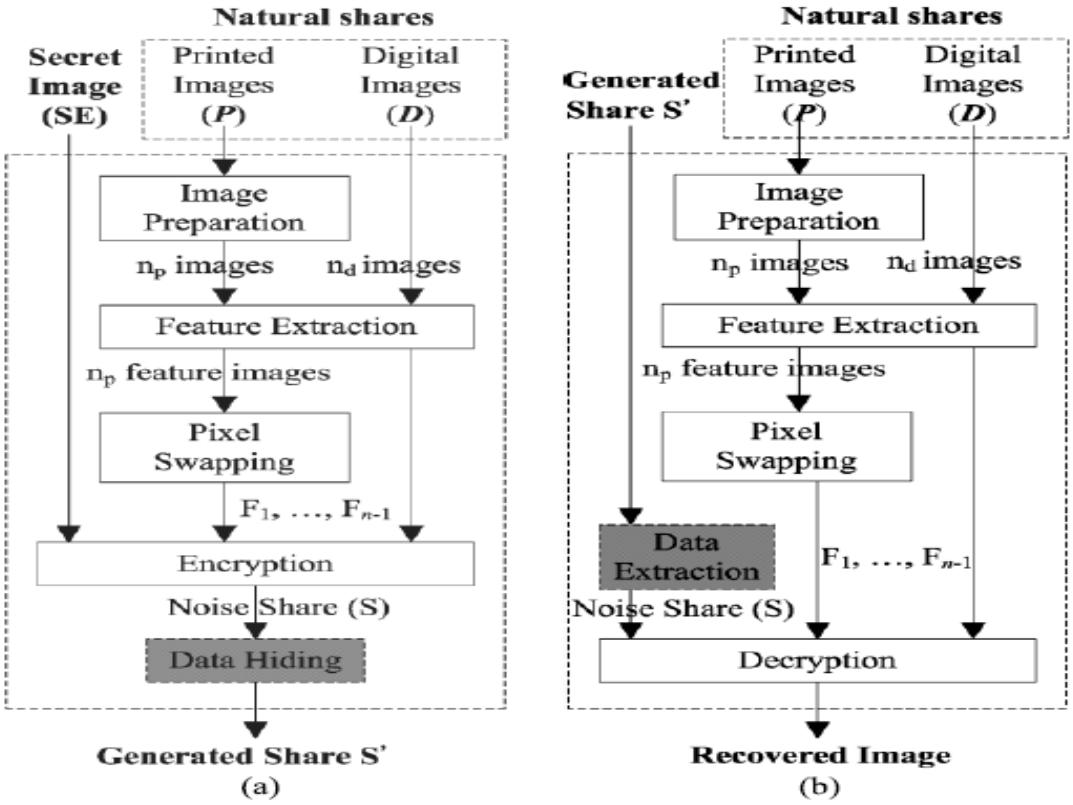


FIG 5. EXISTING SYSTEM

V.PROPOSED SYSTEM

This system proposed (n, n)-NVSS scheme, n is greater than 2, includes two main phases: QR code generation and encryption/Data hiding. QR code generation consist generating one QR image of the secrete data. This QR code is decoded or read by barcode reader or smart phones. In the encryption phase, the n shares of the natural image were created. Then the QR code image of the secrete data or text is hidden behind any one of the share of this created shares. The secrete image which we want to send secretly is resized using feature extraction process. And after resizing this image is hidden behind the natural image shares.The n- 1 innocuous natural shares and the generated share are n shares in the (n, n)-NVSS scheme. When all n shares are received, the decryption end extracts n-1 feature images from all natural shares and then executes the XOR operation with share S_ to obtain the recovered image, as shown in Fig. (b). Each module in Fig. is described inthe following sections.The (n, n)-NVSS scheme takes arbitrary n - 1 natural shares and one generated share as carrier media toshare one digital true colour secret image that has 24-bit/pixel color depth. The objective is to reduce thetransmission risk of shares by using diverse and innocuous media.

1. As the number of delivered shares increases, the transmission risks increases.
2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.
3. The transmission risk decreases as the quality of the meaningful shares increases.
4. The natural images without artificially altered or modified contents have the lowest transmission risk.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

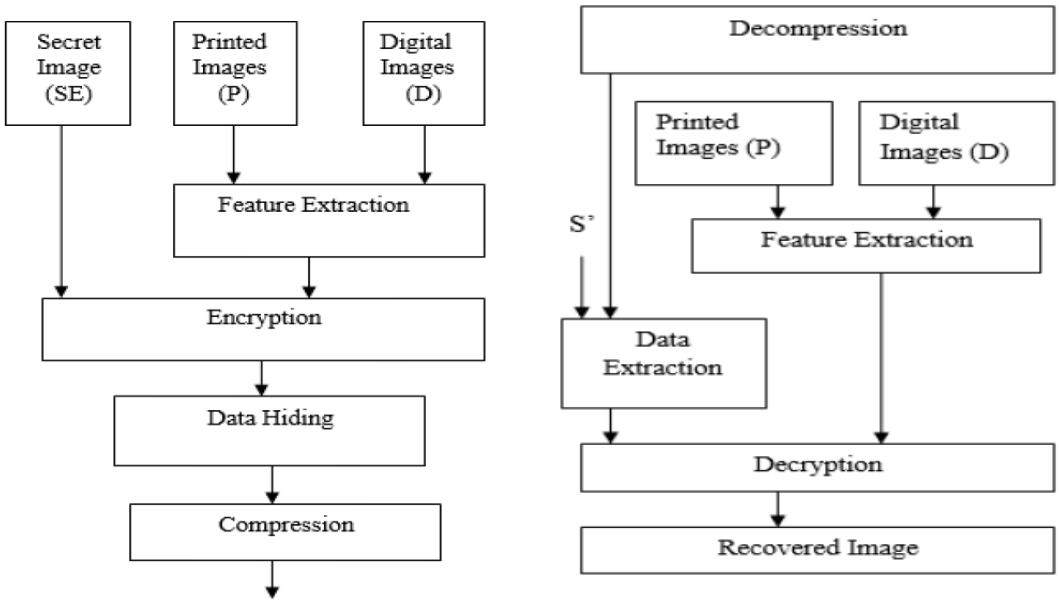
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

VI.SYSTEM ARCHITECTURE



6(a) 6(b)

Fig 6(a): Extraction process 6(b):Decryption process

VII. EXPERIMENTAL RESULTS

In this section, we perform three experiments to evaluate the performance of the proposed NVSS scheme.

A. Experiment I

Fig. is the graphic representation showing the statisticalresults on the distribution of pixel values in share S and secret image (SE1, Lena). The distributions in SE1 in the red, green, and blue color planes are denoted as Secret (R), Secret (G), and Secret (B), respectively. Fig.shows that thedistribution in S (denoted as Share in Fig, in each color plane is random;

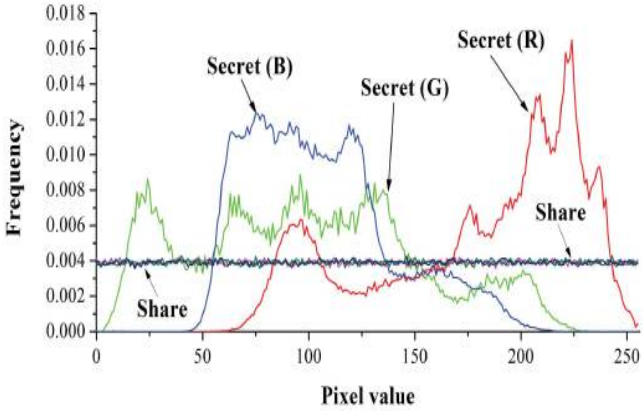


Fig 8. The Distribution Of Pixel Value In Share S And Secret Image Se1.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

it is totally different from the distribution in SE1. Hence, it is difficult to obtain any information related to SE1 from share S. The distribution in share S also agrees with Property 5.

B. Experiment II

This experiment evaluates the performance of the proposed NVSS scheme for sharing color and binary secret images by diverse shares. The shares used in the NVSS scheme include three digital images and one hand-painted picture. The digital images and the color secret image are the same as those used in Experiment I. The hand-painted picture is drawn on A4 paper, as shown in Fig. The picture is processed by the image preparation process to obtain two digitized shares, one for the encryption process and one for the decryption process.

C. Experiment III

This subsection demonstrates the performance of theNVSS scheme by using the QR code to hide the noise share. The natural shares are as shown in Fig10. (a) to Fig. (c).

(a) (b) (c)

The secret images are binary and have the same cipher text— “NO SECRET Here”. Parameters b and P*noise*are set to 8 and 0.5, respectively

VIII. CONCLUSION

The paper proposes a VSS scheme, (n, n)-NVSS scheme, that are used to avoid interception risk which may arise during transmission of secret data. In this scheme secret data is encrypted by generating QR code of that data and then it is hidden behind one of the patch of the natural image. For the image it is hide behind one of the natural image and at the receiver side exact reverse process is performed to recover original data. Thisscheme is more efficient to transfer data trough carrier media; it is friendly as well as original data cannot get recover easily by attackers.

REFERENCES

[1] . Kai-Hui Lee and Pei-Ling Chiu,”Digital Image Sharing by Diverse Image Media”, IEEE transactions on information forensics and security, vol. 9, no. 1, January 2014.
[2]. Sunil G. Jare, ”Digital Image Sharing Using Visual Cryptography Techniques”, Sunil G. Jare*et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 717-721.
[3] .Priyanka R. Pawar, Manjusha S. Borse, “transmission risk reduction in image sharing scheme with diverse image media”
[4]. MayuriSonkusare, Prof. NitinJanwe,“Analysis of Digital Image Sharing By Diverse Image Media” ,MayuriSonkusare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3784-3786.
[5] Miss A ANaphade, Dr.R N Khobaragade,Dr.V M Thakare,”Improved NVSS Scheme for Diverse image media”
[6]Mr.Thanguganesh.M and Prof.SarnayaR.,’’Assorted Image Based Obscure Techniques in Visual Cryptography”.