Enhancing Security by Using Multiple Images and QR Code

Upendra Joshi
Research Scholar, Department of CSE,
Government College of Engineering, Aurangabad, India. 431005

Abstract - **Within the previous visual secret sharing schemes which can hide secret image in image shares and also the used image additionally written on transparencies or encoded and also stored in a very digital kind. The shares of the image will seem like noise pixels or as meaty images; however it'll suspicion and increase interception risk throughout transmission of the shares. Hence, VSSS schemes suffers from disadvantage that it suffers from a transmission risk drawback for the key itself and for the participants concerned within the VSSS scheme. To avoid the drawback i.e. transmission risk, a natural picture primarily based VSS scheme (NVSS scheme) which may shares secret pictures via different carrier media to safeguard the key and also the participants throughout the transmission part. This proposed (n, n) - NVSS scheme will share digital secret image over n-1 arbitrary natural pictures (called natural shares) and one noise-like share. The natural pictures will be photos or hand-painted photos in digital kind or in printed kind. The shares that seem like screeching share may be generated supported these natural shares and also the secret image. The unchanged natural shares square measure varied and inoffensive, thus considerably reducing the transmission risk drawback.**

Index Terms – **Visual secret sharing, image encryption/decryption, transmission risk, QR code, natural images.**

I. INTRODUCTION

In traditional visual cryptography scheme, shares are created as random patterns of picture element. These shares appear as if a noise. Noise-like shares arouse the eye of hackers, as hacker might suspect that some knowledge is encrypted in these noise-like pictures. Therefore it becomes vulnerable to security connected issues. It additionally becomes tough to maintain noise-like shares, as all shares look alike. Nakajima, M. and Yamaguchi, Y. developed Extended visual cryptography scheme (EVS). An extended visual cryptography (EVC) offer techniques to create meaningful shares rather than random shares of traditional visual cryptography and facilitate to avoid the possible issues, which can arise by noise-like shares in traditional visual cryptography. Traditional visual cryptography schemes were supported pixels within the input image. The limitation of pixel based mostly visual cryptography scheme is loss in distinction of their constructed image that is directly proportional to pixel expansion. Visual cryptography (VC) could be a technique that encrypts a secret image into n shares, with each member holding one or additional shares. There are differing types of Secret pictures like : pictures, written documents, photographs etc. a vital purpose of the VC is to provide security to the key image or message. In traditional VC's thy suffer from a retardant of a) Share management, b) pixel enlargement, c) Transmission Risk problems, d) Standard of recovered image[1]. Sharing and delivering secret pictures is additionally referred to as a visual secret sharing (VSS) scheme. VSS schemes play important role within the visual cryptography, as a result of it use images and text messages to cover secrets and supply secure communication. Another important issue is that the aspect of the image which may be won't to show the image in numerous formats like noise like image, significant image, stego image and natural image. These various styles of pictures are wont to hide secrete message and build the communication reliable.

II. LITERATURE SURVEY

Visual cryptography idea came into focus to cover the secret text or image behind another image conjointly this idea used by M. Naor and A. Shamir. These are often done by generating the various shares of the image. Then apply the process of cryptography to encipher that image and send to the proper destination. Different aspect that received shares are often merged to induce the first image. However it suffers from the problem of share management, as a result of they generate additional than one share to cover the key image [2]. The problem occurred within the VC scheme that may be overcome by the extended visual cryptography scheme. This visual cryptography schemes work on the Share management drawback. To get the higher answer Kai-Hui Lee and Pei-Ling Chiu uses a substantive cover image idea. This kind of VC scheme uses binary pictures. For the aim of managing shares this method first construct significant share using optimization technique. And within the next step it'll uses cover pictures that may be additional in every share directly by the stamping algorithmic rule. As this VC scheme uses binary image they're ineffective to take care of the standard of recovered image [3]. The purpose of such schemes is to get noise-like random pixels on shares to cover secret pictures which may be done in the traditional visual secret sharing. However it suffers a management drawback, thanks to that dealers cannot visually establish every share. This management drawback is solved by the extended visual cryptography scheme (EVCS), that adds a substantive cover image in every share. However, the previous approaches involving the EVCS for general access structures suffer from a constituent expansion problem[4]. A construction of EVCS which is accomplished by embedding random shares into relevant covering shares, and we decision it the embedded extended visual cryptography scheme (embedded EVCS). A construction of EVCS was noticed by embedding the arbitrary shares into the meaningful covering shares. A method is to spice up the visual standard of the share picture. Embedded EVCS has many specific advantages against different well-known schemes, such as can deal with grey-scale input picture, has tiny pixel enlargement,

always flatly secure, and does not would like complementary share images, one participant only needs to carry one share [5]. Extended VCS is that where hyper graph coloring space unit used in constructing meaningful binary shares. Since hyper graph coloring are created by random dispense pixels, the resultant binary share contains strong white noise leading to inadequate results. An encryption methodology to construct color EVCS with VIP (Visual knowledge pixel) synchronization and error diffusion for visual standard enhancement [6]. Gray level visual cryptography is made-up to provide the better quality standard in the VC scheme. At this point they apply adaptive order dither technique as well as existing visual cryptography scheme for binary image to create the shares. This procedure reduces the size of decrypted picture. The quality of decrypted image are about to be increased than the ECVS scheme. But this technique suffers from the constituent expansion drawback [7]. Pixel growth problem will be supplementary considered within the Halftone VC scheme. This technique uses Halftone error diffusion technique to convert secret picture and the visible image in to the halftone image. Halftone shares are generated, because the secret data is embedded into the halftone shares and it will provide the result as recovered good quality of image. This technique can avoid the conveyance risk problem [8]. Technique used for halftone technique is error diffusion method. In this binary share images, put secret image element in to every share image by applying void and cluster algorithm. The reconstructed image is obtained by superimposing 2 share images. It is a really good technique however still there's a tradeoff between pixel growth and distinction loss of original image. this method size of element is same as original image pixel size. That means alleviated secret image size and original image size is same so it reduces the drawback of pixel growth. In this method random grid R is outlined as a two dimensional array of pixels. Each element is either translucent (white) or non-transparent (black) by a coin flip procedure. The numbers of transparent pixels and opaque pixels are probabilistically same and the ordinary non-transparency of a random grid is 50% [9-11]. Color picture with natural visual cryptography scheme use the natural image to hide the key info and one noise-like share image. For the encryption method it is need to alter the natural image. So that this kind of VC scheme suffers from texture drawback i.e. original texture of the image will be lost [12]. In order to ensure the key image that transmits through the network will not be taken, the secret images must be encrypted. The concept of this method is known as secret image encryption. The random grid algorithm is used to encrypt the secret image. The scheme will change distortion to infinitesimal it additionally improve on the issues of secret writing. The secret image consists of a group of pixels, where to each component is associated a gray level starting from white to black and each component is handled one by one. Any set of qualified members stack their transparencies they can correctly recover the picture shared by the dealer. The reliability of the scheme, since it implies that, even by inspecting all their shares, any set of forbidden members cannot gain any information on the price of the gray level of the shared pixel. [13-15].

III. PROPOSED SCHEME

In the below diagram it gives the transient data about the design of the proposed NVSS scheme and the whole process of secret writing are often displayed in different steps. In this process it only extracts options from the natural shares; but while not altering the natural shares. In the image preparation and pixel swapping processes are used for pre-processing printed pictures and for post processing the feature matrices that are extracted from the printed pictures. Image preparation process contains 3 small operations on printed image such as acquire image, crop image, resize image. The feature extraction process is used to extract feature from the natural image by doing the three operations namely binarization, stabilization, chaos. Binarization process used to extract feature matrix from natural image. Balancing the prevalence frequency of values one and zero in the obtained feature matrix can be done in the method of stabilization. The process named chaos is employed to eliminate the texture of the extracted feature images and also the generated share. In this process, the original feature matrix are going to be disordered by adding noise in the matrix. Image distortion created by the image preparation process can be permitted within the pixel swapping method. The image distortions were found in the image preparation process was spread in a feature matrix, and the noise is also distributed in the recovered image without clustering jointly. Plenty of the image distortions lead to noise that appears in the retrieve images and if there is great amount of noise clusters jointly, then the image is severely disrupted that could cause a bad result on recovered image that it makes impossible task for the naked eye to spot it.

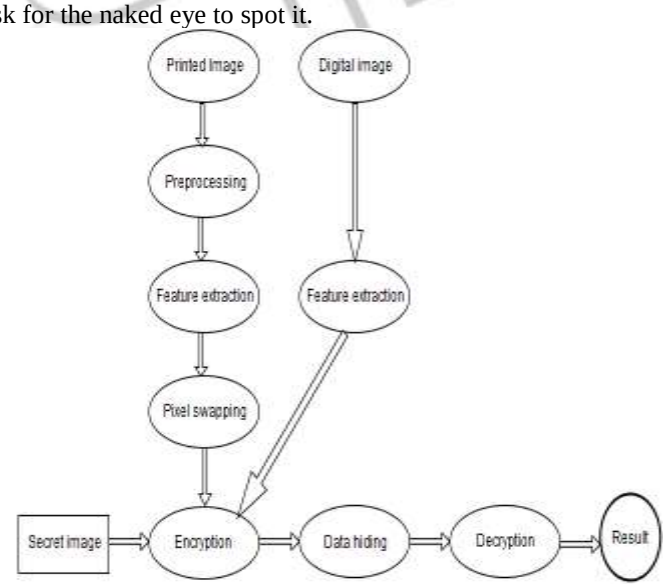

Fig 1 Flowchart of NVS scheme

The pixel swapping process is the answer for this drawback. XOR operation used to do the encryption method. Before applying the XOR function on the input images and feature images FI1,…, FIn--1 can be done after that the XOR function may be apply on in every color plane.

Then the resultant image S is the share image able to send to the destination place. This generated share is reliable because the share image was created by stacking a secret image and n-1 feature images as well because the picture element values in every feature image are distributed every which way and uniformly. These feature images (FI) will be used as n-1 one-time pads(OTP). An necessary OTP system used that is tough to break. The length of each one-time pad is adequate the length of the secret image. The encryption operation uses the logical XOR operator. By using these completely different ways the generated share must be secure. By applying the feature extraction algorithm the generated shares of image have the properties like the new generated share is secure along with the picture element enlargement free.

A Feature extraction from image

In feature extraction procedure features are extracted from the natural shares i.e. both the printed image and the natural image simultaneously using wave transform technique. Wavelet transform technique is a mathematical technique for compressing the image and for process the digital signals. The extracted feature is an image that looks somewhat like the original image this extraction minimizes the randomness and hence the safety of the share. The feature extraction has three procedures binarization, Stabilization and Chaos. From the natural image N the feature matrix is extracted after extracting the feature matrix the other three processes are applied. A simple function F is employed to work out the binary feature worth of a element this method is named binarization. In stabilization method the black and white pixels of each block are well balanced . After stabilization the chaos method is applied this method that adds noise in the matrix that will disorder the original matrix that will not reveal the texture of the image from the first share.

B Image preprocessing

In this process the printed image which is captured by digital cameras or good phones are cropped in order that the additional image is removed so the captured image is resized in order to its dimensions matches the natural shares. Printed pictures are required to transmit the secret image.

C Pixel swapping and post processing

Pixel swapping is applied in order to add randomness to the picture. Two pixels are picked from random column and swapped if upper component has higher hue. The components of the random row are chosen and swapped thus the left pixel can have higher brightness than the right. This procedure is repeated on the complete image.

D Encryption/decryption process

The input of encryption method could be a secret image and also the n-1 natural shares and therefore the output of the Encryption method is a noise like image. The binary feature of the natural share is extracted and the XOR function of secret pixel and binary feature price is performed. This process randomly distributes the element values in the feature image. The generated share after the encryption method is secure as this encryption method has the following properties and therefore it's not possible to crack it.

Property 1 : The amount of data needed for the generated share is that the same as for the key image.

Property 2 : components lues in a feature image are distributed uniformly over [0, 255].

Property 3 : components values in a feature image are distributed randomly.

Property 4 : The generated share is reliable.

E QR code

The Quick-Response Code (QR code) techniques is used to hide the noise-like share and additional minimize intercepted risk for the share throughout the transmission section. In the proposed NVSS scheme, a dealer can hide the generated share by using existing steganography. The amount of data which will be hidden in a cover image is restricted and depends on the concealing methodology. To embed the generated share in a cover image, generally the dimension of the cover image should be larger than that of the key image. If the share will be hidden within the cover image so will be retrieved completely, the secret image will be recovered without distortion. We leave the details of using steganography to cover shares to the reader; our focus is on a way to hide the share in printed media using QR code technology.

IV. PROPOSED ALGORITHMS

A Feature extraction algorithm

1. Extracts one binary feature matrix F from each input natural image N.
2. Determine the feature values of each pixel in a block.
3. The stabilization process is performed and the noise can be added based on a given parameter Pnoise.
4. Finally feature matrix *F* can be generated as an output.

B Encryption/Decryption algorithm

1. Initializes random number generator G and this function G is used for the feature extraction and pixel swapping processes.
2. Initializes all feature images.
3. Extracts a binary feature matrix from a natural share by calling the feature extraction algorithm.
4. Also adds the extracted matrix to corresponding bit and color planes of a feature image.
5. The pixel-swapping process for each feature image extracted from the printed images. For each feature image, the pixel-swapping process randomly selects x and y coordinates of pixels in a feature image.
6. Stacks input image S and feature images FI1….. FIn-1 by applying the XOR operation in each color plane.
7. Finally, the resultant image S is the output.

C Share hiding algorithm

1. Initialize the parameters.
2. Reduce the amount of information in the feature matrix F to fit within the capacity of the hiding media.

3. Decides the value of stego bit sb by majority. Function H(S) represents the Hamming weight of bit string S. Then, the stego-bit is appended to bit string FQR .
4. Convert FQR to the numeric string SQR. And finally the SQR is output share image with QR code.

D Share extraction algotithm

1. Retrieves the related parameters from SQR.
2. Transform 5 numeric characters into binary form, then removes 5 consecutive numeric characters from the front of number string SQR by calling procedure remove().
3. Converts string S to its integer value by procedure str2int ().
4. Transforms the value to a corresponding binary bit string and appends it to bit string FQR.
5. Converts FQR to the resultant feature matrix F.
6. Outputs feature matrix F.

E Hide the noise like share

The Quick-Response Code (QR code) technique is used to cover the secrete image. The QR code is a two dimensional code. A QR code uses four standardized modes i.e. numeric, alphanumeric, byte / binary, and kanji to efficiently store data. A bar code could be a machine legible optical label that contains data regarding the item to that it's connected. This QR code encodes meaningful data. The noise-like share as the numeric sort of the QR code. The encoding method consists of 2 steps: 1) remodel pixels on the share into binary values and represent the values in a decimal format. 2) Encode the decimal values into QR code format. Also the multiple QR will be wont to cipher a lot of information bits. The QR code can be scan by using QR code scanner and sensible phone devices. It is necessary to supply security to the QR code also in order that nobody will simply scan that individual QR code. That's why the concept of applying digital signature to the QR code is necessary to supply security to QR code. Digital signatures employ a sort of uneven cryptography. For messages transmitting through a non secure channel, a properly implemented digital signature offers the receiver reason to believe the message was sent by the claimer sender. In other word we tend to will say that a Digital signature could be a mathematical scheme for demonstrating the reliability of a digital message or document.

V. RESULT ANALYSIS

The result shows that the proposed NVSS system can uses the digital, printed images to hide the secret data in it. In other words it can be say that it uses the natural image so it decreases the rate of transmission risk. This system uses its own Encryption Decryption algorithms to encode the share and also decode the share. The new concept of QR code is used which is more beneficial to provide security to the secret data. The QR code having the minimum size and save large data. The most important thing in implementing the QR code is that it will generate a password which at the time of encoding process and that password is needed at the time of decoding. Without this password the system will not decode the QR code and get back the share which having the secret data. Following histogram analysis shows that there is no data loss after retrieving original image.

An image histogram is a graphical representation of the total number of pixels which are present in an image that can act as a function of the intensity. The term histograms that are made up of bins which can use as a container, every bin will represent a specific value range for intensity. The value of histogram is calculated by examining all the pixels that are present in the image and allocating each to a particular bin based on the intensity of pixel. The number of pixels that can be assigned to a bin is its final value. The total number of bins in which the full intensity range that can be divided which is usually in the sequence of the square root of the total number of pixels. The concepts of Image histograms have an important too for examining the images. This can allow focusing Background as well as the range of grey value. Also the method of clipping and the Noise of Quantization in image values can be marked immediately. These tasks firstly start with the Color Bins.

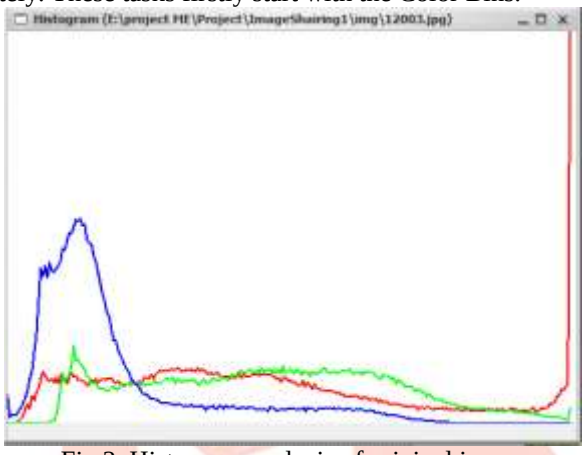

Fig 2. Histogram analysis of original image

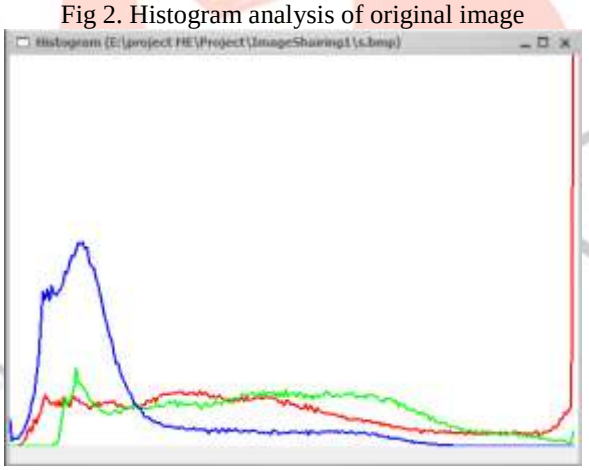

Fig 3. Histogram analysis of retrieved image

Initially the value of all the bins is put as 0. Then start a loop that visits every pixel in a image and extract the RGB value of the pixel. These RGB values are further separated into specific colors RED, GREEN and BLUE and are stored in their respective color bins. Then calculate the MAX color bin value. Then finally plot the graph for each individual Color Bin. In the above graph the first graph will show the histogram for the original secret image, whereas the second graph shows the histogram for the recovered secret image. Red color indicates the red histogram, similarly the green color and blue color indicates the green and blue histogram respectively. The X axis represent the width of the image and Y axis represent the gray level of image.

VI. CONCLUSION AND FUTURE SCOPE

The presented VSS scheme, (n, n) - NVSS scheme, which can share a digital image using various image media. The media that include n-1 arbitrarily chosen images are unchanged in the encoding part. Therefore, they are completely innocuous. Regardless of the quantity of participant's n increases, the NVSS scheme uses solely one noise share for sharing the key image. Compared with existing VSS schemes, the proposed NVSS scheme will effectively cut back transmission risk and give the best level of user friendliness, both for shares and for participants. This is the primary attempt to share images via heterogeneous carriers in a VSS scheme. Successfully introduced hand-printed images for image sharing schemes. This proposes a useful idea and technique for using unchanged images as shares in a VSS scheme. In future work it can be used for the more encryption and decryption algorithms and develop stronger, secure, and easy new algorithm for encryption and decryption for transmission of the secret image using natural shares.

REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media" ," IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 88–98, Jan. 2014.
[2] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*,vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.
[3] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," *Int. J. Pattern Recognit. Artif.Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.
[4] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7,no. 1, pp. 219–229, Feb. 2012.
[5] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun.2011.
[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250,nos. 1–2, pp. 143–161, Jan. 2001.
[7] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1,pp. 132–145, Jan. 201.
[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual Cryptography," *IEEE Trans. Image Process.* vol. 15, no. 8, pp. 2441– 2453,Aug. 2006.
[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4,no. 3, pp. 383–396, Sep. 2009.
[10] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," *Opt. Commun.*,vol. 283, no. 21, pp. 4242–4249, Nov. 2010.
[11] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.
[12] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEE Trans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.
[13] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual
secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21,no. 11
[14] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for gray scale images," *Digit. Signal Process.*, vol. 21, no. 6, pp. 734–745, Dec. 2011.
[15] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-color images with size constraint," *Inf. Sci.*, vol. 179, no. 19, pp. 3247–3254, Sep. 2009.