DIGITAL IMAGE SHARING BY DIVERSE IMAGE MEDIA USING NVSS TECHNIQUE

R.H. ADEKAR[1], N.M. JADHAV[2], N.D. PERGAD[3]

[1] *Head of Department, CSE Department, S.T.B.C.E. Tuljapur, Maharashtra, India*
[2] *Master of Engineering E&TC Student, S.T.B.C.E. Tuljapur, Maharashtra, India*
[3] *Associate Professor, E & TC Department, S.T.B.C.E. Tuljapur, Maharashtra, India*

ABSTRACT

Visual Secret Sharing Schemes hide a Secret image in shares that appear noise like picture or noiseless picture.VSS schemes suffer from a transmission risk problem while sharing shares contains Secret Images. To address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. This Process involved sharing a secret image over arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares. We successfully introduce hand-printed images for images-haring schemes. The proposed Algorithms are applicable to digital and printed media. This study proposes a useful concept and method for using unaltered images as shares in a VSS scheme. We develop a method to store the noise share as the QR code. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

Keywords: - *Visual secret sharing(VSS) scheme, extended visual secret sharing(EVSS) scheme, natural-image based visual secret sharing (NVSS), transmission risk.*

1. INTRODUCTION

Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. A block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. As a result, different security techniques have been used to provide the required protection. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

1.1 Visual Cryptography

The internet is a general term which provides many services to user. Users can transmit their messages or information to distance friends or go shopping in virtual shops by using the Internet, so it helps us to reduce our precious time. Many types of protection methods are used for preventing the sensitive message to be stolen such as cryptography, visual sharing, and data hiding. The technique that divides a secret image into *n* shares, with each participant holding one or more shares is known as visual cryptography (VC).Anyone holding the all n shares when provides those n shares after stacking those n shares will get the relived secret damage which can be recognized by human eyes directly. The secret images can be of various types such as hand written document, printed images, photographs, digital images, others. This technique of sharing & retrieving the images is also known as visual secret sharing scheme (VCC).

In (2, 2) VSS scheme the image is divided into two component images. Every pixel of an image component is divided into parts. If the pixel is divided into two parts then it has one white and one black block. Every pixel is in proximity to each other.

Fig - 1: Basic concept of Visual Cryptography

In the Fig - 1 we see that the original image was broken up into two shares, neither of the two shares shows any information about the image but when share 1 is overlaid onto share 2 and Ex-OR operation is performed on them the original image appears back.

The VSS scheme has a major drawback that is it suffers from high transmission risk because the shares are like noise. As the shares are like noise that causes the attackers attention. Also the meaningless shares are not user friendly &the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares. Then there is new method developed called as "extended visual secret sharing(EVSS)" which uses steganography.

1.2 Extended Visual Secret Sharing(EVSS)

Using steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images. This EVSS system is more users friendly. But this system to have a drawback that by stego-images still can be detected by steganalysis methods.

To overcome the drawback of VSS & EVSS scheme the Natural- image based visual secret sharing (NVSS) is developed.

1.3 Natural- Image Based Visual Secret Sharing (NVSS)

The natural visual secret sharing (NVSS) scheme is defined as how a user sends a secret image securely in a network. This scheme combines one or more images to the secret image, the images that are combined with the secret image are known as natural shares. Considering the aspects of high transmission risk, corruption by

unauthorized users this scheme serves at its best. The natural visual secret sharing scheme uses multiple forms of images namely the natural shares these shares could be of any digital image. Printed images include hand-painted pictures, flysheets. Digital images include any image captured via digital camera or smart phones. The secret image combined a long with the natural shares is subjected to various techniques namely Image preparation, feature extraction, steganography for hiding purpose and QR code formation.

2. THE PROPOSED SCHEME

2.1 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 ciphertext. The ciphertext 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 ciphertext. As pointed out by Naor and Shamir, the visual secret sharing scheme is similar to the OTP encryption system. In a (2, 2)-VSS scheme, the secret random key and the ciphertext that can be treated as two shares in the scheme were distributed to two participants who involve in the scheme. Instead of generating a secret random key, we extract the secret key from an arbitrarily picked natural image in the (2, 2)-NVSS scheme. The natural image and the generated share (i.e., ciphertext) were distributed to two participants. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the original secret image.

2.2 Assumptions

The proposed (*n*, *n*)-NVSS scheme adopts arbitrary *n*-1 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, the transmission 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 the meaningful 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.

5. The display quality of distortion-free true-color images is superior to that of halftone images.

In the NVSS scheme, the natural shares can be gray or color photographs of scenery, family activities, or even flysheets, 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 Compared with traditional (*n*, *n*)-VSS schemes, which must carefully deliver *n* noise-like shares, the proposed (*n*, *n*)-NVSS scheme must deliver only one generated share in a high-security manner. When the transmission cost is limited, the proposed scheme using unaltered natural shares can greatly reduce transmission risk.

2.3 Implementation Modules

- Input Image
- Embedding Procedure
- Extraction Procedure

MODULES DESCRIPTION:

- **Input Image (or) Video**

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person. Image is a two-dimensional, such as a photograph, screen display. They may be captured by optical devices—such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces.

➢ **Embedding Procedure**

Input: Cover image of size, secret Image bit stream.
Output: Stego image.
1. Find the minimum satisfying, and convert into a list of digits with a binary notational system.
2. Solve the discrete optimization problem to find and.
3. In the region defined by, record the coordinate such that,
4. Construct a no repeat random embedding sequence.
5. To embed a secret Image bit stream, two pixels in the cover image are selected according to the embedding sequence, and calculate the modulus distance between and, then replace with.
6. Repeat Step 5 until all the secret Image bit streams are embedded.

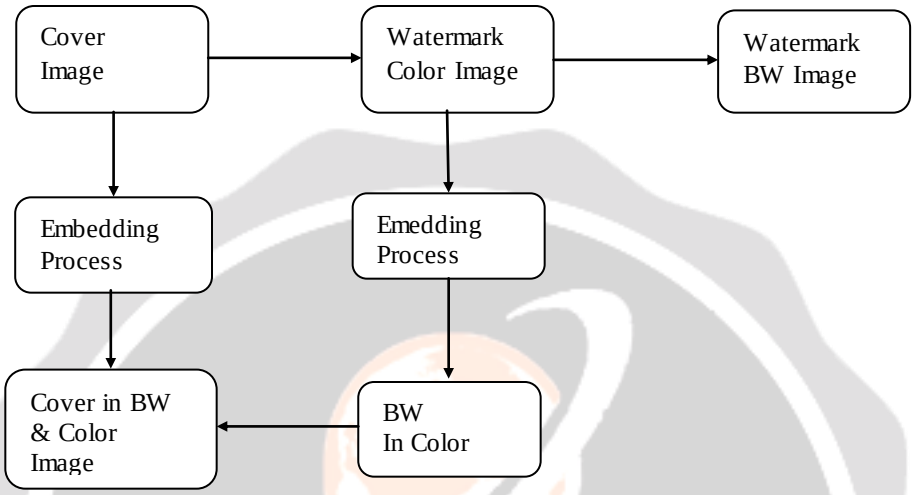


Fig - 2: Block Diagram of Embedding process

➢ **Extraction Procedure**

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded secret Image bit streams are the values of extraction function of the scanned pixel pairs.
Input: Stego image.
Output: secret Image bit stream.
1. Construct the embedding sequence.
2. Select two pixels according to the embedding sequence.
3. Calculate, the result is the embedded digit.
4. Repeat Steps 2 and 3 until all the secret Image bit streams are extracted.
5. Finally, the secret Image bits can be obtained by converting the extracted secret Image bit stream.

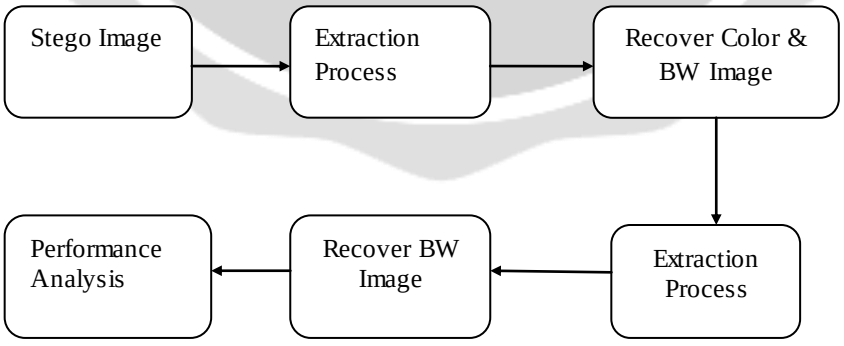


Fig - 3: Block Diagram of Extraction Process

3. NATURAL IMAGE BASED VSS SCHEME

Natural Image Based Visual Secret Sharing Scheme (NVSS) is a method that is introduced to reduce the transmission risk that occurs in the VSS Scheme. The NVSS makes use of natural image such as photographs, paintings, landscapes etc as digital shares, making use of natural shares rather than noise like image can reduce the transmission risk to certain extent. The NVSS scheme also makes use of different media to transmit the

share this will make the catch of data difficult. The NVSS scheme uses the one time pad (OTP) technique .OTP is a java program that encrypts the image, after encryption the image contains only black and white pixels and it is very difficult to extract the information making it un intercept able .In (2, 2) VSS Scheme we make use of random generated key and the cipher text as the two shares, these two shares are distributed to the participants. In NVSS scheme the secret key is extracted from the randomly selected natural image. In the process of encryption the natural image and the generated secret key is sent to the participants. During the decryption secret image In the process of encryption the natural image and the generated secret key is sent to the participants. During the decryption secret image and the generated image reveal the original image. The NVSS can also be extended to (n, n) NVSS scheme as shown in Fig - 4.

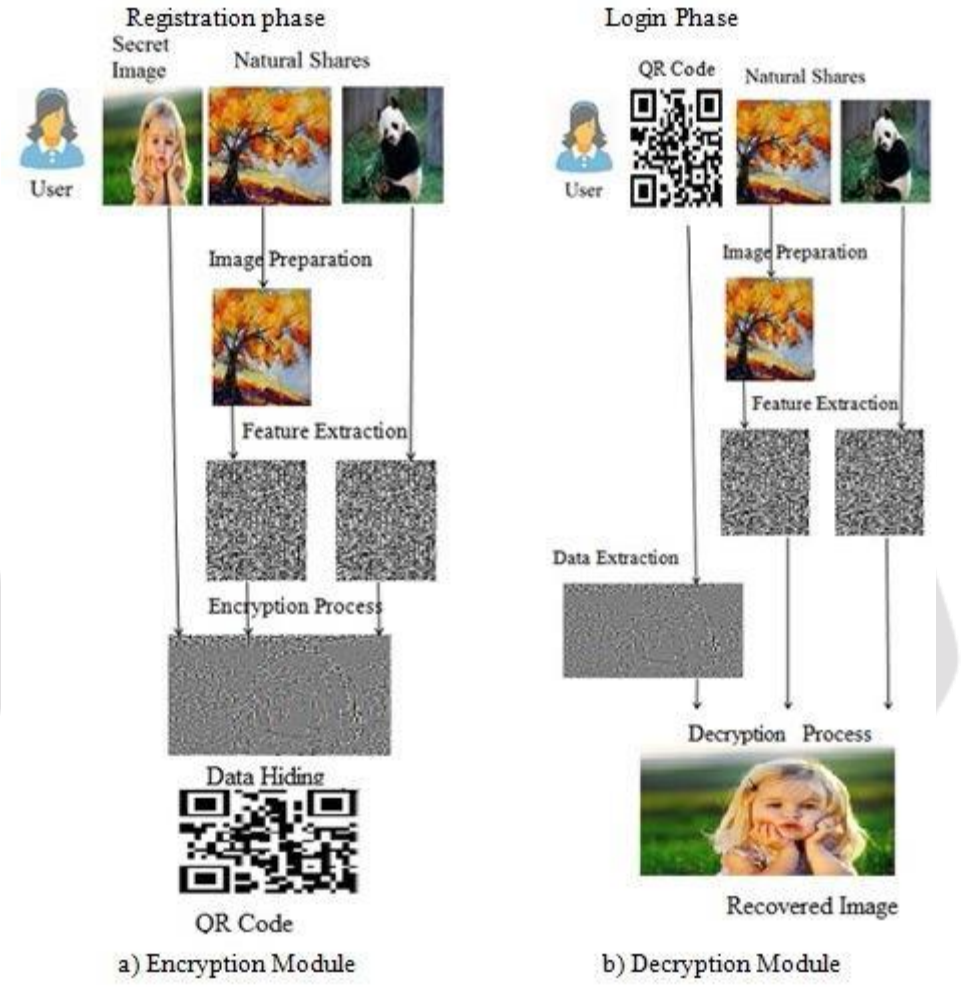


Fig - 4: The encryption/decryption process of the (*n*, *n*)-NVSS scheme: (a)encryption process, (b) decryption process.

3.1 Encryption Process in NVSS (n, n) scheme

The encryption process in NVSS consists of two phases the feature extraction phase and the encryption phase.

3.1.1 Feature Extraction Process

In feature extraction process some features are extracted from the natural shares i.e. both the printed image and the natural image simultaneously using wave transform method. Wavelet transform method is a mathematical method for compressing the image and for processing the digital signals. The extracted feature is an image that looks somewhat like the original image this extraction reduces the randomness and hence the security of the share. The feature extraction has three processes 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 to it. A simple threshold function F is used to determine the binary feature value of a pixel this process is called

binarization. The extracted feature of each block in binarization process is balanced using the stabilization process i.e. the black and white pixels of each block are balanced . After stabilization the chaos process is applied this process which adds noise in the matrix which can disorder the original matrix that will not reveal the texture of the image from the original share.

3.1.2 Image Preprocessing

In this process the printed image that is captured or acquired by digital cameras or smart phones are cropped so that the extra image is removed and then the acquired image is resized so that its dimensions matches the natural shares . Printed images are needed to transmit the secret image.

3.1.3. Pixel Swapping Post processing

Pixel swapping is done in order to add randomness to the image. Two pixels are picked from random column and swapped if upper pixel has higher hue. The pixels of the random row are selected and swapped so the left pixel will have higher brightness than the right. This process is repeated on the complete image.

3.2 Encryption / Decryption Process

The input of Encryption process is a secret image and the n-1 natural shares and the output of the Encryption process is a noise like image. The binary feature of the natural share is extracted and the XOR operation of secret pixel and binary feature value is performed. This process randomly distributes the pixel values in the feature image. The generated share after the encryption process is secure as this encryption process has the following properties and hence it is impossible to crack it.

Property 1:- The amount of information required for the generated share is the same as for the secret image.

Property 2:- Pixel values in a feature image are distributed uniformly over [0, 255].

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

Property 4:- *The* generated share is secure.

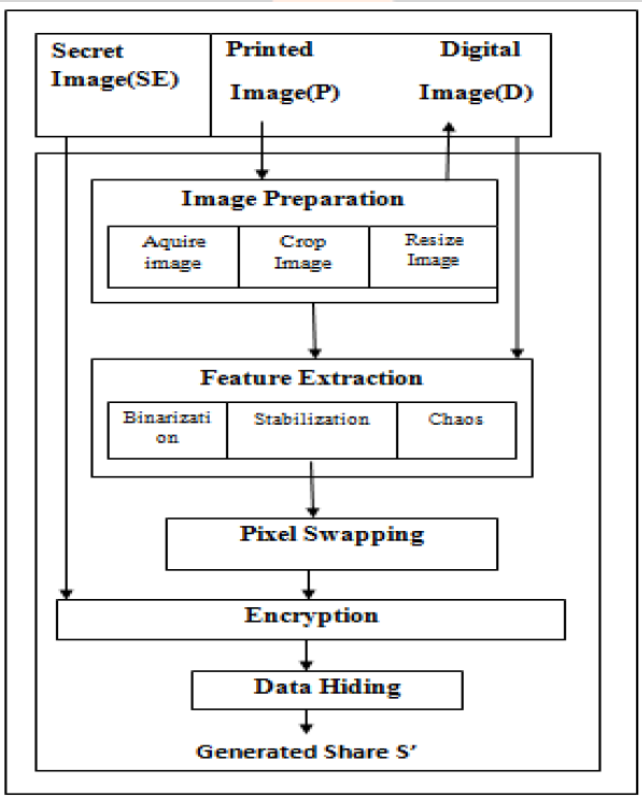


Fig-5: Encryption Process

3.3 Data Hiding

To further reduce the transmission risk the data hiding techniques such as Steganography and Quick Response Code (QR code) is used to hide the noise like share during the transmission. Steganography is a technique to hide information inside information which will secure the secrecy of transmission. A QR ("quick response") code is a two dimensional barcode Invented by the Japanese corporation Denso Wave. Information is encoded in both the vertical and horizontal direction, thus holding up to several hundred times more data than a traditional bar code. QR code is used as a carrier for secret communication.

3.4 Decryption Process

In the decryption process from the stego-share the share is extracted. The feature matrix F is extracted from the numeric string SQR then decoded which is in the QR code format. In this process the feature extracted images of natural shares is combined with noise like share. The step wise logic of decryption process is explained below.

- The input for this process is generated share, combination of generated feature extracted images of natural shares, random generator G which is initialized by a seed. All the input images will be equal to 24bit.
- So natural shares are also extended to 24 bit plane. Each bit plane in a feature image will correspond to the same bit plane in secret image. Before encryption process will start need to extract n-1 feature matrices from natural share.
- After extracting these n-1 feature matrices theses matrices executes XOR operation with each bit plane of noise like share(s). This XOR operation should be performed on every bit plane which will result to generate Secret image. Thus the process of decryption will be completed.

After successful decryption process user will be able to see his recovered original secret image, which will confirm that this is original site and not the fake. Thus user will have extra protection for his password. This system will be very helpful for preventing phishing attack.
In the decryption phase, on receipt of the stego-share, the hidden information must be extracted from the stego share. Algorithm 4 lists the share extraction algorithm that extracts a feature matrix F from numeric string S_{QR}. The string S_{QR} is decoded from the stego-share, which is in QR code format. Step 1 retrieves the related parameters from SQR.

4. RESULT AND DISCUSSION

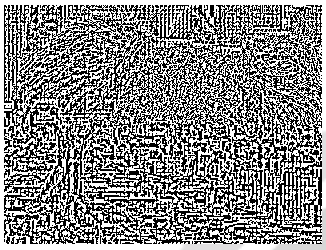
In our proposed system (n, n) - NVSS scheme has been implemented. Here both printed image and digital image have been taken into account to create the noise-like share. This natural image needed to be extracted feature for further process. With the featured image and secret image can perform encryption process.By applying (n, n) NVSS scheme developed encrypted image or (n-1) natural share. Feature extraction has been performed for two natural shares, so as the natural share's pixels are more efficiently compressed. This extracted features are encrypted with Secret Image. This process is performed by (n, n) – NVSS scheme. Then the encrypted image will be hided using share hiding algorithm. This process performed with the QR code technology. QR code is a two-dimensional code. The QR Code system has become popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. The transmission risk of the conventional VSS schemes increases rapidly. On the contrary, regardless of the increasing number of shares, the proposed NVSS scheme always requires only one generated share. In decryption process Share extraction algorithm performed and decryption algorithm applied to recover the Secret image.

The performance of the proposed scheme is shown in figure. Figure shows two natural shares and one secret image in the experiments. Figure a and b shows the natural shares and Figure c is the secret image. Figure d and e shows feature image for NS1 and NS2 respectively and Figure f shows the combination of d and e. Generated share is represented in figure g with corresponding QR code in Figure h. After decryption process system gives recovered secret image which is shown in Figure i.

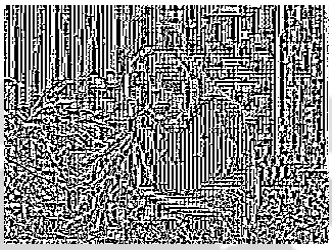
a) Natural Share 1 (NS1)

b) Natural Share 2 (NS2)

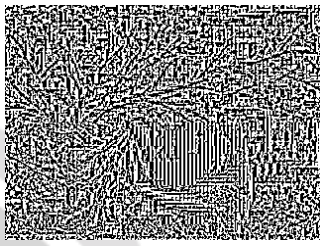
c) Secret Image(S)



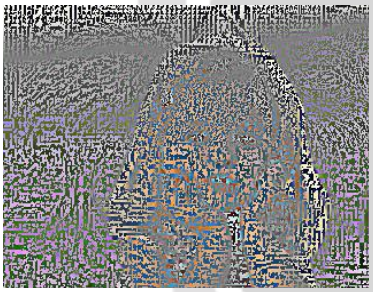
d) FI1 of NS1



e) FI2 of (NS2)



f) Combination of FI1& FI2



g) Share (S')

h) QR code for S'

i) Recovered Secret Image

5. ADVANTAGES OF PROPOSED SYSTEM

- To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.
- Transmission is highly secure due to QR code
- Cost for transmission is reduced.
- Recovered image is almost the same as that of the input image.

6. APPLICATIONS

Secure Web browsing using Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols, the use of encryption may be transparent to users.

- Encrypting entity needs to share the key with a separate decrypting entity, the key must be transported to the decrypting entity in a secure manner.
- It also applied in the field of ecology, biometrics and medical applications.

7. CONCLUSION & FUTURE SCOPE

7.1 Conclusion

The paper proposes a VSS scheme, (*n*, *n*)-NVSS scheme, that can share a digital image using diverse image media. The media that include *n*-1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants. This study provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for images-haring schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme. Fourth, we develop a method to store the noise share as the QR code.

7.2 Future Scope

The Natural image based visual secret sharing scheme is effectively reduce the transmission risk of shares. These natural shares are totally secure and innocuous.. Therefore visual secret sharing scheme reduce the transmission risk problem and provide security for secret image. NVSS scheme also reduces the pixel expansion problem. The major contribution of our work is, to reduce the transmission risk problem and provides the highest level of user friendliness. Major contributions are this is the first attempt to send secret image through various carrier media and for image. In enhanced system can segment the secret image and 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.

8. 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] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[3] 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.

[4] 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.

[5] 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.

[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] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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. 2011.

[12] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.