ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Improved NVSS Based Anti-phishing Framework Using Diverse Image Media

Pratidnya Deshmukh, Navnath Kale

Student, Department of computer Engineering, PVPIT, Pune, India

H.O.D., Department of computer Engineering, PVPIT, Pune, India

ABSTRACT: For sharing sensitive information over a network conventional visual secret sharing technique is used. 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. To overcome the drawback of VSS scheme the Natural-image based visual secret sharing (NVSS) is developed. The NVSS scheme uses the natural images such as paintings, photographs etc. as digital shares. As the scheme using the natural shares instead of noise like shares which reduces the transmission risk to certain limit. This scheme also uses the different media to transmit the shares. Phishing has become one of the major issues in the recent times. Hackers attempt to steal user personal information such as usernames, passwords, credit card details etc. This problem can be solved by using biometric image sharing. This is a new alternative for outsourcing data in a secure way. NVSS scheme firstly hides secret image with other natural shares. After performing Image preparation & feature extraction on natural shares the secret image is encrypted with those natural shares or images. This will provide encrypted share. Then this encrypted share will be converted to QR code. User can download the share or can get it through mail. QR code provides extra security for password. After providing QR code user will get his secret image thus user will identify it's a fake site or original site. On the basis of QR code and generated secret image user will not proceed further and will not give his sensitive information on fake site.

KEYWORDS: Natural visual secret sharing scheme, Image preparation, feature extraction, QR code, decryption code

I. INTRODUCTION

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 image 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.

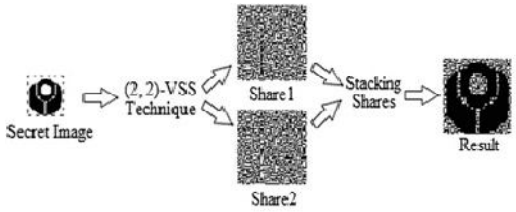


Figure 1: VSS Scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

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. 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.

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 along with the natural shares is subjected to various techniques namely Image preparation, feature extraction, steganography for hiding purpose and QR code formation.

The following are the contributions made in the **proposed work**:

1. Developed a web based system for online banking which will be useful for prevention from phishing attack. In this system user have to provide secret image at the time of registration. After completion of registration user will Get QR code.
2. When any user goes to online banking site he provides his username & password. The developed system helps us from fake site. Before providing password and other details user will be asked for QR code. If it's an original site then user will see his secret image before proceeding for password & if it's fake site user will not get his secret image. Thus user will be able to protect his password from fake site & fulfilling our main aim of anti-phishing attack. Reduce the transmission risk it's the main motive for (n,n) NVSS technique. For which we are using different forms of media generally termed here as natural shares, the shares include digital or printed images, these natural shares have low transmission risk than noise-like or meaningful shares.
3. The display quality of true-color natural images is greater than that of halftone cover images or previously used techniques.
4. The generated QR code helps us to hide the generated share. We can print this QR code or can save it in laptop/mobile or may be in printed form. The code carries meaningful information and can be read by devices such as smart phones and barcode readers. Thus QR code helps us to hide generated share. Developed banking application can provide these QR code though mail also.

II. RELATED WORK

K. H. Lee et al. [1] provides (n, n) - NVSS (natural image based VSS) scheme to reduce the transmission risk that occurs in the VSS Scheme by using natural images and diverse media as carrier. This scheme uses the feature extraction process and encryption/decryption algorithms. Secret key is extracted from the randomly selected natural image using feature extraction. 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. Quick Response Code (QR code) is used to hide the noise like share during the transmission.

P. L. Chiu et al. [3] have studied about simulated annealing based algorithm which is used to solve the threshold VCS problem. This scheme reduces the pixel expansion problem and improves the visual quality.

H. Lee et al. [4] proposed a two-phased encryption algorithm for the EVCS (Extended Visual cryptography scheme) for general access structure. The first phase uses the optimization techniques for a given access structure, construct a noise-like shares. The second phase directly adds a cover image on each share via stamping algorithm. This algorithm is applicable to binary secret/cover images. No computational devices are needed during the decryption phase. This scheme reduces the management problem but not pixel expansion problem.

F. Liu et al [5] describes the Embedded EVCS (Embedded extended visual cryptography schemes) which is constructed by adding random shares of secret image into meaningful covering images. It will improve the contrast of the recovered secret image and produce clear image. Embedded EVCS has many advantages, such as it can deal with

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

gray-scale input images, has smaller pixel expansion, is always unconditionally secure, one participant only needs to carry one share, and can be applied for general access structure.

I. Kang et al [6] introduces the concept of visual information pixel (VIP) and error diffusion to gain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. VIPs are used to synchronize the positions of pixels that carries the information of original images across the color channels so as to retain the original pixel values the same before and after encryption. Error diffusion is a type of halftoning in which the quantization residual is distributed to neighboring pixels that have not yet been processed. Its main use is to convert a multi-level image into a binary image.

T. H. Chen et al [7] tells about friendly random-grid algorithm (FRGVSS) which solves the problem of pixel expansion and converts meaningless shares into meaningful shares images. This is very user friendly and gives wide image format.

Z. Zhou et al [8] have proposed halftone visual cryptography in which the secret binary image is encoded into halftone images or halftone shares. This method uses the rich theory of blue noise halftoning to generate the halftone shares and which applies to the construction mechanism used in conventional VC. The obtained visual quality is better than extended VC.

Z. Wang et al [9] have studied about HVC (Halftone visual cryptography) construction method based on error diffusion. Meaningless shares are encoded into halftone shares taking meaningful information which reduces the suspicion of intruders. The pixel which carries the secret image information is predetermined before a halftone share is generated. Error diffusion improves the image quality of halftone shares and completely remove the error interference of reconstructed secure image.

C. Guo et al [10] describes a multi-threshold secret image sharing scheme based on MSP (monotone span programs). In this scheme we can define different types of pre-define access structure on shadow images. The aim is to construct a multi- threshold access structure in secret image sharing. This scheme also provides the authentication to verify the shadow images.

III. SYSTEM MODEL

The system Architecture explains the entire flow of the application. The main advantages of (n, n) NVSS scheme which is the logic behind this web based application under various circumstances are as follows

- Transmission is highly secure due to QR code.
- Cost for transmission is reduced.
- Images that are used are of high display quality since they are subjected to various constrains.
- Recovered image is almost the same as that of the input image.

There are two main phases for this web based application. First is Registration & second is of Login.

I) First phase: During registration user have to give three input images including one secret image, one printed image & one digital image. User also has to fill all the mandatory details. After successful registration user will receive QR code. User can download it. If user not downloads the share then he can get that on his mail through request QR options.

II) Second phase: During this phase user have to provide QR code with username for login purpose. If site is original then he will see the secret image before providing password.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

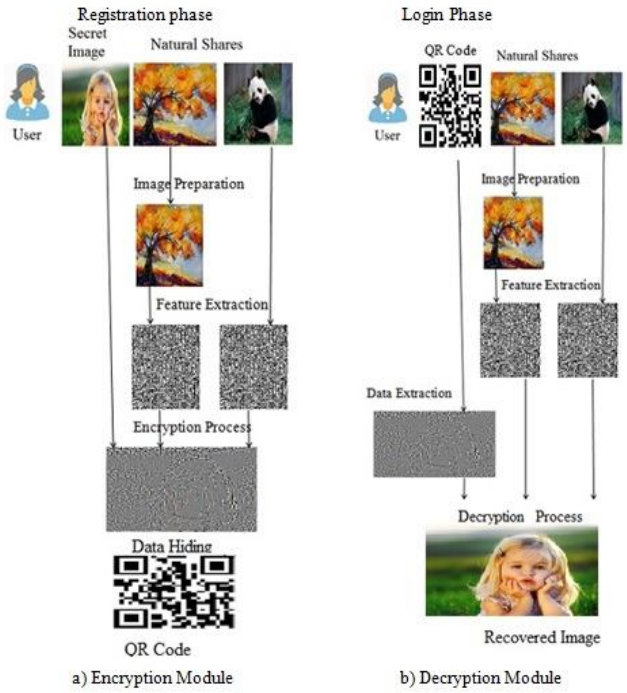


Figure 2: System Architecture

A. *Registration Phase:*

There will be various background processes behind these phases. Image preparation, feature extraction, pixel swapping will be same for both the processes.

i) *Image preparation:* The process is done both at the Registration and the Login side, it is carried out as user gives natural shares that are digital images to be used for processing, and these images are subjected to operations such as cropping and resizing to its desired dimensions. The following diagram will describe this process.

Figure 3: Image Preparation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Figure 4: example of image preparation

ii) Feature extraction:

In this phase the image acquired from the image preparation module will be used as a input. In this module algorithm is used to extract the feature. There are some existing modules which can extract the feature such as wavelet transform. But the output given by these methods will have some textures of the original image. So for security reasons we must remove these textures. For this purpose we will use different technique and output image will be in the form of noise like shares. Below diagram will provide the short description of the Feature extraction module and then there will be description for the same in detail.

Figure 5: Feature Extraction Process

- Let the input image given by user in dimension length (L) X Height (H).
- Then this image is divided into b x b pixel blocks. Where b belongs to even number so b describes the block size.
- **N** represents the **natural share**.
- $K^{xy}$is the sum of RGB color values of (x, y) pixel in natural share N.
- M is represents the median of all pixel values.
- When we get a block of $K^{xy}$with values for any pixel. Then for feature extraction process we compare each value with median M of that block. If the value is greater than M we assign it 1 value and if value is less than M we assign it 0.This is nothing but the **binarization** process.
- But there are chances that the number of black & white pixels will not be the same. May be white or may black pixels will be greater. So need to balance the no. of black & white pixel. By using a formula pixels can be balanced. The formula used will randomly select the pixels which will be greater and then will convert it into opposite pixel. So we will have a matrix with same number of black & white pixel. This process is **stabilization**.
- After getting the image there will be some texture or sharp edges which will remain in the coming output of image. So to remove this texture we will use another formula. This will randomly change the some black pixels into white and white pixels into black. Still there will be equal no. of black & white pixels. But there position will be changed due to applied formula. This is **chaos process**. The output of this process will be **feature matrix (F)**.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Example: Suppose the pixel value K^{xy} for 4 x 4 block is as shown.

Pixel value for single block Of 4X4 in natural share			
185	195	225	80
250	210	90	170
110	60	200	160
185	200	120	180

⇒

Binarization for above block with mean of 164			
1	1	1	0
1	1	0	1
0	0	1	0
1	1	0	1

Stabilization with changing two white pixels into black			
0	1	1	0
1	1	0	**0**
0	0	1	0
1	1	0	1

⇒

Feature Matrix (F) After chaos Process			
0	1	**0**	**1**
0	1	**1**	0
0	**1**	**0**	0
0	1	**1**	1

iii) Encryption process:

In this process the feature extracted images of natural shares is combined with secret image.

The step wise logic of encryption process is explained below.

- The input for this process is secret image, 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 secret image. This XOR operation should be performed on every bit plane which will result to generate **noise like share (s).** Thus the process of encryption will be completed.

iv) Data Hiding:

1) Generation of hash code from noise like share:

The output of the encryption is noise like share which have color pixels. So we will not able to generate QR (Quick Respond) code directly. So need to use a MD5 algorithm. This will generate 16no. Hash code. By using this hash code; QR code can be generated easily.

The structure for MD5 algorithm is given below:

Steps:

1. Append Padding bits to the input image that is noise like share.
2. Append length to the input image that is noise like share.
3. The resulting message (after padding with bits and with length) has a length that is an exact multiple of 512 bits. The input message will have a length that is an exact multiple of 16 (32-bit) words.
4. After performing various operations will get the hash code of 16 characters.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

2) Generation of QR code from hash code:
The generated 16 character unique code is then converted in to QR code.
By using QR code generation technique will develop the QR code. User can download this QR code or can request it any time on his registered mail id.

B. *Login Phase:*In this phase user will give his username and his corresponding QR code.

i) Data extraction/QR code reading:
The system will read the QR code. If it's a correct QR code, username and original site, then the 16 character number generated by reading the QR code will be matched with the database username and hash code generated at the time of registration. If this code matches then system will provide the noise like share(s) same as that of generated at the time of registration.

ii) Decryption process:
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.

IV. EXPERIMENTAL RESULTS

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 c is the secret image. Figure d and e shows feature image for NS_1 and NS_2 respectively and f shows the combination of d and e. Generated share is represented in figure g with corresponding QR code in fig. h. After decryption process system gives recovered secret image which is shown in fig. i.

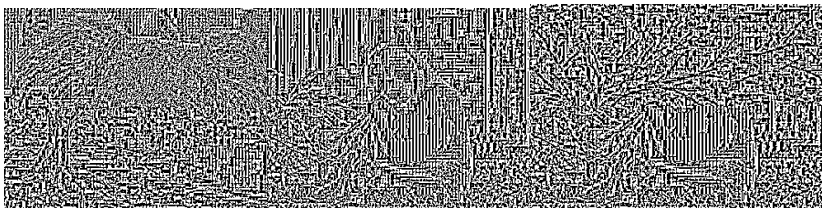
a) Natural Share 1 (NS_1) b) Natural Share 2 (NS_2) c) Secret Image(S)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015



d) FI_1 of NS1 e) FI_2 of (NS2) f) Combination of FI_1& FI_2

g) Share ($S^{'}$) h) QR code for $S^{'}$ i) Recovered Secret Image

Figure: Experimental results

V. CONCLUSION

The NVSS scheme reduces the transmission risk problem by using the natural images as shares. This scheme shares the images using heterogeneous carriers. The NVSS scheme also uses data hiding techniques such as stenography and QR code. This is a user friendly scheme for both participants and shares.

This study provides Four major contributions. First is prevention from phishing attack. Second, display quality of true-color natural images is greater than that of halftone cover images or previously used techniques. Third, reduces transmission risk. Forth, the QR code helps us to hide the generated share which provides high level of security.

VI. ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. N. D. Kale (H.O.D. of computer department) for his valuable suggestions and guidance throughout my course of study and precious help given to me in completion of my paper.

I am thankful to the entire staff of the Computer Engineer Department for their kind cooperation and help. I also take this opportunity to thanks my colleague, who backed our interest by giving useful suggestions and all possible help.

REFERENCES

[1] Kai-Hui Lee , Pei-Ling Chiu, "Digital Image Sharing by Diverse Image media", IEEE Transactions on Information Forensics and Security, vol 9, No. 1,pp.88-98,January 2014.

[2] Pratidnya S. Deshmukh , N. D. Kale " Survey on Biometric Image Sharing using cryptography and diverse image media" International Journal on Recent and Innovation Trends in Computing and Communication, volume 2, issue 11, dec 2014

[3] 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.

[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] 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.

[7] 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, pp. 1693–1703, Nov. 2011.

[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.