Secret Sharing in Visual Cryptography using NVSS and Data Hiding techniques.

Ms.Misha Ann Alexander
Student, Computer Engineering Department
Sinhgad Institute of Technology
Lonavala, India
annalexander33@gmail.com

Mr. Sanjay B. Waykar
Asst Prof, Computer Engineering Department
Sinhgad Institute of Technology
Lonavala, India
sbwaykar@gmail.com

***Abstract*— Visual Cryptography is a special unbreakable encryption technique that transforms the secret image into random noisy pixels. These shares are transmitted over the network and because of its noisy texture it attracts the hackers. To address this issue a Natural Visual Secret Sharing Scheme (NVSS) was introduced that uses natural shares either in digital or printed form to generate the noisy secret share. This scheme greatly reduces the transmission risk but causes distortion in the retrieved secret image through variation in settings and properties of digital devices used to capture the natural image during encryption / decryption phase. This paper proposes a new NVSS scheme that extracts the secret key from randomly selected unaltered multiple natural images. To further improve the security of the shares data hiding techniques such as Steganography and Alpha channel watermarking are proposed.**

***Index Terms*—Natural Visual Secret sharing, natural images, noisy share, pixel swapping, encryption, decryption.**

I. Introduction

We are in a digital world where digitization has touched industries, governments, education, research, trade etc. This has basically caused a large amount of high-risk data to be transacted over the Internet which is an insecure medium of data exchange. Cryptography is an encryption technique widely used in electronic communication to provide security in transmission. This technique converts plain text to cipher text so that only the intended people can read the content. Visual Cryptography is a new simple, easy to implement encryption technique developed by Moni Naor and Adi Shamir that encrypts the visual information such as text, pictures or written data and uses human visual system for decryption [2].The transmission of the visual shares in Visual Cryptography is called as visual secret sharing (VSS) Scheme [1]. In conventional cryptography, the secret is scattered into multiple shares and transmitted through multiple modes to a set of quantified users. When these shares are stacked together it reveals the secret content. The noisy textured share fulfills the security constraint but at the same time it causes the attackers attention. The increasing number of noisy shares makes the VSS scheme less user-friendly and difficult to manage. Natural Visual Secret Sharing (NVSS) provides an effective solution to these problems of VSS by reducing the number of transmitted shares and enhancing the user friendliness of the shares by using the QR code technique to hide the secret share. NVSS scheme extracts the features from natural images either printed or digital in nature captured with the help of digital devices having different settings, make and configurations. These extracted features are applied to the secret image which transforms it to an unidentifiable share. Theses natural shares are innocuous in nature and hence there is very less probability of the secret being intercepted during transmission [1]. To make the scheme more secure NVSS makes use of diverse carrier media to transmit the shares, but it suffers due to the reason that the secret image is distorted at the receiver end during decryption. The regeneration of similar natural images with same dimensions and settings during the encryption and decryption is truly a difficult task due to the use of dissimilar electronic devices. To reduce the distortion of the retrieved secret, a new NVSS scheme is proposed in which the secret key is extracted by processing the randomly selected natural meaningful images either selected from the database or some websites. The key generated along with chaotic equations are used to map the original pixels of a secret image onto new locations. To further enhance the security of the noisy shares during transmission it is hidden behind meaningful cover images.

This paper proposes algorithms for Key Extraction and Encryption /Decryption of Secret images. The remainder of the paper is as follows Section II contains the related work Section III presents the Proposed Scheme Section IV and V contains the evaluation and results of proposed work finally Section VI concludes the work.

II. RELATED WORK

The current research in visual cryptography basically focus on the VSS where the shares transmitted are noisy in nature [1][2].The noisy shares are not user friendly and hence the researchers tried to improve the user friendliness of the shares and hence the quality of the shares by adding a cover image to the noisy meaningless shares[4].Even though the quality of the shares improved but the recovered image had a problem of pixel expansion. To further improve the quality, user friendliness and security of the secret image researchers adopted the technique of steganography along with the VSS [9]. The Steganography is a technique where the secret is embedded in the cover image the embedded image is the Stego share. The stego share are also identified by the steganalysis technique [6].Thereafter the researchers tried to use natural images to share the secret content but, however, the system failed due to the textures of the natural images were visible on the secret share [15].In [1] authors attempted to extract the features from some natural images and encrypted the secret image based on the features of the natural image selected. The natural images consist of both the digital image and the printed image. The printed image can be some handwritten data or some pictures and equipment like the cameras were used to capture the images. Even though natural images had a very high level of security due to the use of different equipment with variety of settings and features the image captured during the encryption and the decryption would vary in its size, resolution and other important parameters and hence this can cause the retrieved image to be distorted.

This paper extends the previous work of the authors by proposing a new NVSS technique which will eliminate the natural image preprocessing phase as well the security, user friendliness and manageability of the shares are increased by using one noisy share with a cover image and data hiding techniques like digital watermarking and Steganography to further improve the security of the system.

III. PROPOSED SCHEME

A. Background

Cryptography is a network security tool that provides confidentiality, integrity, and security. It makes use of encryption to enable confidentiality. One Time Password (OTP) was developed by Gilbert Vernam in 1917 and it is a very secure unbreakable technique which makes use of dynamic or random passwords each time [2]. Visual Secret Sharing (VSS) scheme is a technique which delivers the secret shares to the quantified users. These shares when stacked together it reveals the secret. These shares cause the attention of hackers due to its noisy nature. These shares are meaningless, unmanageable and not user-friendly in nature due to its noisy texture. The Visual Cryptography supports various secret sharing schemes like 2 out of 2 scheme, k out of n and n out of n scheme. In the 2 out of 2 scheme, two shares are generated one the cipher text and the other is the key. Every pixel in the original secret image is divided into sub pixels depending on whether it is a black or a white pixel. Decryption takes place by overlapping the two shares and revealing the secret image.

Natural Visual Secret Sharing (NVSS) Scheme is an improvement over the VSS scheme where the key is extracted from the randomly selected printed and digital images. These images can be photographs which can be captured by the digital equipment and hence the same settings are required during both the encryption and decryption phase.It is not easy to acquire the same image and settings during both encryption and decryption which leads to a distorted retrieved secret image.

The proposed new NVSS scheme extracts the key through multiple natural images either from the public internet or any other source, this key is given to the chaotic equation which scatters the original pixel positions. To further improve the security of the shares data hiding techniques are used. Compared to the previous NVSS scheme the new scheme improves the quality, manageability and user friendliness of the retrieved secret image as well as eliminates the natural image preprocessing phase.

B. Proposed New NVSS Scheme

The proposed new NVSS scheme has two major phases the key generation phase and the encryption phase.

- The Key is extracted from ‘n’ natural meaningful images. These natural images can be 24bit /pixel color images which are randomly selected from any websites on public Internet or photographs stored in the system. To extract the key from these images, it has to first undergo some preprocessing.
- The natural image has to be binarized first so that we can process the individual pixel values which can be either a black or white pixel. The 24-bit images are transformed into an 8-bit binary image or grayscale image.

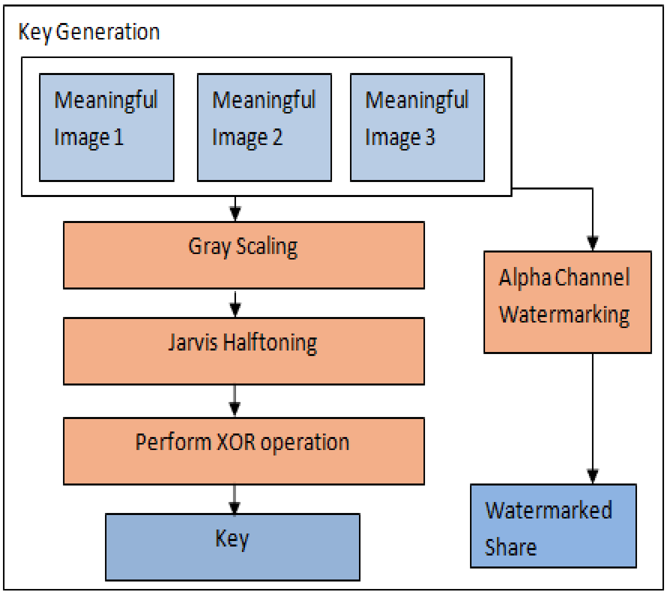

Fig.1. Key Extraction

- In a color image, every pixel is composed of three different color intensities i.e. Red, Green, and Blue. Gray scaling is a method that converts these three intensities into a single value. The conversion can be done by the average method.

$$G_{img} = R(x, y) + G(x, y) + B(x, y) \text{ -------------- } (1)$$

- The result is an 8-bit image. The ‘n’ natural images are converted into grayscale image and then further half toned.

- The grayscale natural images are then half-toned in which the continuous tone images are converted into black and white halftone image. Error diffusion can basically produce halftone images which are of better quality and is pleasing to human eyes rather than that of the other halftone methods.
- Every pixel (x, y) is compared with the threshold value 127 if the pixel value is greater than 127 then a white pixel will be generated or else a black pixel is generated. The resulting images can contain only two colors black and white. This process helps to differentiate between the background and foreground color in the natural images.

$$H(i, j) = \begin{cases} 1 \text{ if } \mathrm{IMG}(i, j) >= \text{Threshold value} \\ 0 \text{ Otherwise} \quad \text{---------------} \ (2) \end{cases}$$

- Either a full black or a full white pixel is generated. An error is diffused by calculating the difference between the halftone and original natural image and then the difference is added to the next pixel.
- This will result into a matrix for each natural image. This matrix contains only 0’s and 1’s. The total number of 0’s and 1’s in each matrix are counted and an XOR operation is performed the result is the key.

Algorithm: - 1 KEY_GENERATION ( )

```
Input: - N1,N2,N3

Output: - KEY

1. Do for each image N1,N2,N3
2. For each pixel  repeat 3-4
3. Calculate Gimg by equation (1).
4. Determine H (i, j) by equation (2).
5. End of Loop
6. KEY<- Calculate number of 0 and 1
   perform XOR  operation.
7. Store the watermark image in each natural
   images alpha channel.
8. Output KEY
9. End
```

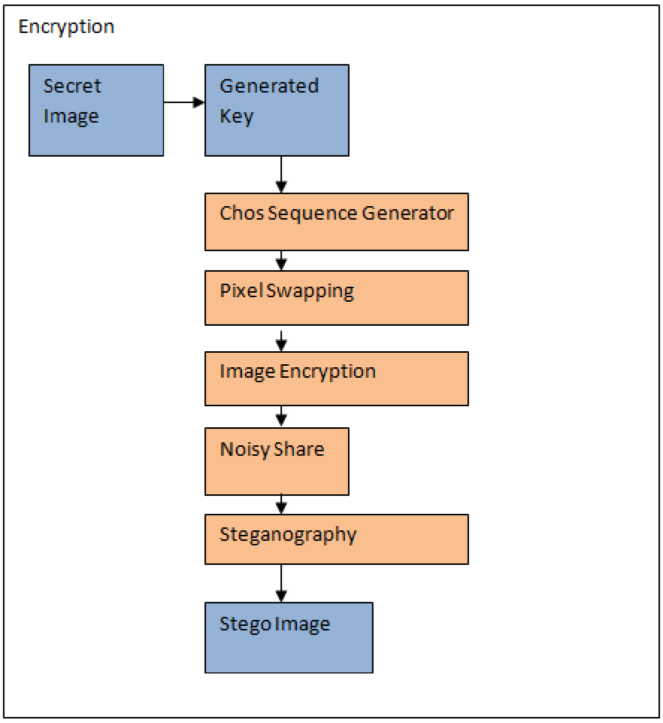

Fig. 2. Encryption Phase

Algorithm: - 2 ENCRYPTION ( )

```
Input: - KEY,SECRET_SHARE

Output: - SSHARE

1. NPIX <- Generate new pixel co-ordinates(x,y)
   using chaotic equations (3)
2. Add Ascii value of Key to the new co-ordinate
   value.
3. SHARE <- Shuffle the co-ordinates(x,y) to
   (x1,y1)
4. Calculate LSB of the cover image
5. SSHARE < - Replace the LSB bits of cover
   image with the bits noisy secret image.
6. Output SSHARE
7. End
```

- The chaotic equations carry a very dynamic behavior every pixel in the secret image is shuffled based on the values generated by the chaotic equations.
- To make it more secure the coordinates (x2, y2) are added with an offset which is the sum of ASCII value of the generated key.

- The pixel (x, y) are placed at a different position (x2, y2) in such a way that the secret image is not visible to the human eyes.

$$X_{n+1} = 1\text{-}ax_n^{2} + y_n$$

$$Y_{n+1} = bx_n \quad \text{---------------} \quad (3)$$

- The share that is generated is noisy in nature and hence attracts the hackers. To safely transmit this noisy share it can be hidden within another cover image.

C. Data Hiding Technique

To improve the security of the share further we can make use of data hiding techniques like steganography. Cryptography and Steganography work very closely with each other to improve the security of the noisy share. A proper container or a cover image has to be selected in which the noisy secret can be embedded completely. There are various sizes of images like 8 bit and 24 bit. The larger the cover images the more bits can be stored in it. The various types of steganography in this system LSB (Least Significant Bit) technique is used and it's a very popular technique. In this technique, the LSB bits of the cover image are replaced with the bits of the noisy share.

If we want to encode A (ACSII value 65 or a binary value 01000001) in the below given carrier file.

01011101 11010000 00011100 10101100

11100111 10000111 01101011 11100011

After Embedding

01011100 11010001 00011100 10101100

11100110 10000110 01101010 11100011

D. Decryption

The stego image is transmitted at the receiver end .The noisy share is then retrieved from the cover image. The meaningful image is either transmitted to the receiver or their address in public Internet is sent to the receiver. The key is regenerated from the same natural meaningful images. This key as offset and the chaotic equation is used to map the pixels back to its original positions.

```
Algorithm: - 3 DECRYPTION ( )
Input: - SSHARE
Output: - SECRET
  1. Stego Image is read
  2. LSB bit is calculated
  3. Noisy share is extracted
  4. The Meaningful image is accessed from the
     appropriate websites
  5. Generate the chaotic equation from the
     Meaningful images
  6. Swap the pixels of the noisy share
  7. End
```

evaluate the performance of the New NVSS scheme. The Secret image is the well-known image of Leena of dimensions 512 x 512 pixels. We also select three natural images from random websites which are 24-bit color images with various dimensions. These three images are passed to the Key Generation algorithm as input. This algorithm returns a unique key 715542 as output. Then the values of every pixel (x, y) is passed to the chaotic equations which exhibit a very dynamic behavior and the new coordinate with then added with the ASCII value of the key which is the new coordinate where the pixel (x, y) is mapped to. The noisy share is then embedded in a cover image and then transmitted. During decryption phase, the key is regenerated from the three same natural images extracted from the same websites. This key is then applied with the chaotic equations to the noisy share to recover the secret image. The time complexity of the algorithm is O(ncd hw) the loop in the algorithm executes for every pixel depending on the height and the width(hXw) of the selected images and the color depth (cd) whether 24bit or 8 bit image.

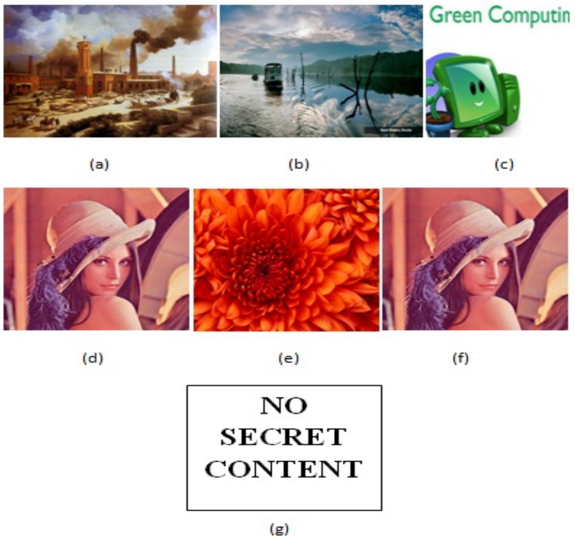

Fig 3. Experimental Results of New NVSS Scheme. a) Natural Image 1. b) Natural Image 2. c) Natural Image 3.d) Secret Image. e) Stego Image f) Recovered Secret Image g) Experimental result when the natural image is noisy or changed

.

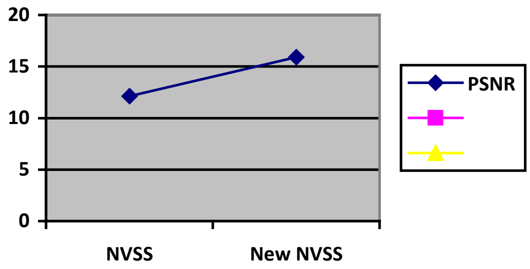

Fig. 4. Graph for PSNR

V. Comparative Study

This section shows the result of the proposed system with the existing NVSS scheme based on the PSNR (Peak Signal to Noise Ratio). The results of new NVSS scheme are more significant than the existing scheme.

Secret Share Dimensions	**NVSS scheme**	**New NVSS scheme**
Leena 256 x 256	---------	17.54db
Leena 512x512	12.12 db	15.92db

Parameter	**NVSS Scheme**	**Secured NVSS Scheme**
Type of Share	Noisy share hidden below QR code or natural image	Noisy share hidden below cover image.
Transmission Risk	Low risk	Very Low risk
No of Shares	One Share	One Share
Data Hiding techniques	QR code and Steganography is used.	Alpha channel watermarking and Steganography will be used.
Quality of Retrieved Share	Distorted Share	No Distortion

VI. Conclusion

This paper proposes a new NVSS scheme that generates a secret key from the natural meaningful images. This scheme uses the unaltered natural shares from random websites or from databases which reduce the distortion in the retrieved secret image. To further improve the security of the noisy shares steganography data hiding technique is used. The natural images can also be transmitted securely in the network using alpha channel watermarking.This study has contributed to the previous work of the authors by effectively reducing the transmission risk and this attempt has reduced the distortion of the retrieved secret share.

ACKNOWLEDGEMENT

I would extend my sincere thanks to my project guide Prof.S.B Waykar ,Assistant Professor Sinhgad Institute Of Technology,Lonavala for his guidance and unending support .I would also like to thank our HOD , ME Coordinator and all other staff members of my college, my parents, friends and all the other individuals for willingly helping me out continuously in the development of my project.

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 ,January 2014 , pp 88-98.

[2] Moni Naor,Adi Shamir “Visual Cryptography”Eurocrypt ,1994,pp1-11.

[3] K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” *IEEE Trans. Inf. Forensics Security*, vol 7 no1, Feb. 2012,pp. 219–229,.

[4] 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.

[5] Inkoo Kang,Gonzalo R.Arce,Heung-Kyu Lee “Color Extended Visual Cryptography using error diffusion” , *IEEE Trans. Image Process.*, vol. 20, no. 1, , Jan. 2011,pp. 132–145.

[6] X. Wu, D. Ou, Q. Liang, and W. Sun, “A user-friendly secret image Sharing scheme with reversible steganography based on cellular automata,”*J. Syst. Softw.*, vol. 85, no. 8 , Aug. 2012 pp 1852–1863.

[7] Sadan Ekdemir,XunXunWo , *Digital Halftoning,Project in mputational Science Report*, January 2011,pp1 34.

[8] Natapon Pantuwong , Nopporn Chotikakamthorn,“Alpha Channel Digital Image Watermarking Method”, IEEE ICSP Proceedings,2008,pp 880-883.

[9] Andrew D. Ker “Steganalysis of LSB Matching in Grayscale Images”, IEEE Signal Proceedings,vol 12,no 6,June 2005,pp 441-444.

[10] M.Natarajan , Gayas Makhdumi,”Safegaurding the digital contents:Digital Watermarking” ,DESIDOC Journal of Library and Information Technology ,vol 29 no 3,May 2009,pp. 29-35.

[11] Pradosh Bandyopadhyay,Soumik Das,Atal Chaudhuri,Monalisa Banerjee,”A new Invisible Color Image Watermarking Framework through Alpha Channel”,March 30 2012,pp. 302-308.

[12] Zhongmin Wang,Gonzalo R.Arce,Giovanni Di Crescenzo, “Halftone Visual Cryptography via error diffusion”, *IEEE Trans. Inf. Forensics Security, vol 4no 3,September 2009,pp.383-396.*

[13] Weiqi Luo , Fangjun Huang , Jiwu Huang , *Edge Adaptive Image Steganography Based on LSB Matching Revisited,IEEE Trans Inf. Forensics Security,* vol 5no 2,June 2010,pp 201 214.

[14] A. Nissar and A. H. Mir, *Classification of steganalysis techniques: A study , Digital. Signal Process”’*, vol. 20, no. 6, Dec. 2010,pp. 1758 1770.

[15] P.L.Chiu K.H.Lee,K.W.Peng and S.Y. Cheng,”A new color image sharing scheme with natural shadows,”in Proc.10th WCICA ,Being,China,Jul .2012,pp 4-15.