Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 9, September - 2015

New Secure Natural Visual Secret Sharing Scheme In Visual Cryptography

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*— Secret Sharing is a technique used to securely distribute the secret content to a set of quantified users. This secret is transformed into multiple noisy shares. Due to the noisy nature of the shares it attracts the hackers. The NVSS scheme was proposed to solve this issue. In this scheme the features from various natural images are extracted and applied to the secret image to shuffle its pixels however this scheme causes distortion in the retrieved secret image during decryption process as the dimensions of the natural images changes during both encryption and decryption as different digital devices are used during both encryption and decryption process. To solve this problem, a new secured NVSS is proposed which extracts the encryption key from randomly selected natural meaningful images from various websites or database. The ASCII value of the key extracted after preprocessing the natural images is combined with the chaotic equations to securely reposition the pixels of the secret image. This share is securely transmitted over the network using steganography and watermarking techniques.**

Keywords—Natural Visual Secret sharing, natural images, noisy share, pixel swapping, encryption, decryption.

I. Introduction

Internet is growing very fast in India as well as in other countries. Maximum business in private and government sectors these days depend on Internet and hence it is need of these days to have a secured network for data exchange. Due to the major progress in technology and digitization of data protecting and safeguarding the data is of major concern. There has been a lot of research in the field of cryptography for safeguarding the content transmitted over the Internet. Cryptography enhances the security of information transmission on the network by writing the secret into cipher text .Visual cryptography is a type of cryptography that allows information in visual format like text, graphics etc to be converted into many shares and transmitted over the Internet.

It is a very easy to carry out cryptographic encryption technique developed by Moni Nahor and Adi Shamir. The decryption in visual cryptography is just a mechanical process which makes use of human visual system [2].In each secret image or message transmitted there are number or pixels both black and white pixels are present. Each pixel is modified into one or more transparency. Numbers of shares are generated based on the Visual Cryptography scheme. These shares are then transmitted over the network to 'n' quantified user's .During decryption theses shares are overlapped to reveal the secret content. The visual secret sharing scheme VSS is a technique used in visual cryptography for transmission of shares. Due to the noisy nature of the transmitted shares it is attacked by the hackers and hence not secure or user friendly neither manageable in nature.

The Natural Visual Secret sharing scheme tackles the drawbacks of the VSS scheme. NVSS makes use of diverse media to transmit each share. The shared secret is encrypted using the features of natural image which are captured using different digital devices with different settings. This scheme has a major drawback when it comes to decryption as the same digital equipments with similar settings has to be used during both encryption and decryption which is not possible most of the time and hence causes distorted secret image. The QR code is used to make the shares more user friendly.

This paper proposes a new improved secured NVSS scheme which extracts a unique key from the randomly selected natural images and the ASCII value of the key is then added and applied to the henon map which will help in repositioning the pixel positions. To further enhance 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 rest of the paper is as follows Section II has the related work Section III presents the Proposed Scheme Section IV and V has the evaluation and results of proposed work finally Section VI concludes the work.

II. Related Work

Early research focused on the generation of noisy shares and various ways to scatter the pixels of the shares. The existing research is on the secret sharing schemes. The traditional VSS scheme has a major drawback concerning the noisy nature of the share as it captures the hackers attention [1][2].

The noisy shares were then embedded into natural cover images which enhance the quality of shares and user friendliness of shares [4]. Later the technique of steganography was used by which the noisy shares were embedded into natural images and shared on the network. But these stego images are identified by steganalysis [6][9].

There after researchers made use of natural images to embed the noisy shares but these embedded shares makes the secret content visible [15].

The researchers in [1] extracted features from natural images captured using digital devices of certain make and settings. The natural images used can be both digital and printed in nature. These natural images are then a preprocessed .Natural image has very high level of security and hence improves the security of shares. This technique however causes distortion in the decrypted secret image.

The proposed system is the extension to the previous work of the authors. A new secured NVSS system is proposed which makes use of randomly selected natural meaningful images from websites or database. These natural images are watermarked and transmitted for decryption process. The natural images are processed and based on the number of black and pixels a unique key is generated this key along with some chaotic equation helps in scattering the pixels of the secret image. To further improve the security and user friendliness of the shares steganography is used.

III. Proposed Work

A. Background

Cryptography is a technique which transforms the original message into unreadable text that can be transmitted over the network. This technique enhances the security, integrity and confidentiality of transmitted data. One Time Password (OTP) 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 Cryptography is a simple encryption technique that encrypts image, text etc in such a way that the decryption is possible by human visual system. This technique proposed by Moni Nahor and Adi Shamir in 1994.

VC has various secret sharing techniques like the 2 out of 2 scheme, n out of n and k out of n secret sharing schemes. Every pixel in the secret image considered separately Based on the pixel a pattern is selected and the secret image is divided into multiple shares[2].Visual Secret sharing scheme transmits the 'n' shares among the quantified users in VC. The drawback of VSS is that the noisy texture of the shares attracts the hackers and hence can cause loss of data.

Natural Visual Secret Sharing (NVSS) Scheme is a technique which makes use of natural images in printed or digital format to extract some features and encrypt the secret image based on these features. The natural images is captured by using different digital devices during both encryption and decryption which leads to capturing images with different dimensions and patterns and hence causes distortion in the retrieved secret image during decryption.

The proposed new secured NVSS scheme extracts a unique key from multiple randomly selected natural images either from the public internet or any other source, the ascii value of the key is given to the henon map chaotic equation which repositions the original pixel positions. To further improve 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 preprocessing phase.

A. Proposed New Secured NVSS Scheme

The proposed new secured NVSS scheme has two major phases the encryption phase and the decryption phase.

- To encrypt the secret image a key has to be generated this key should be unique key. To generate highly secured key natural meaningful images randomly selected from some websites of database are selected. They can be 24 bit color images. In order to generate a key these images has to be first preprocessed using some image processing techniques.
- First these images will be converted into binary format i.e. gray scaling of the images will be performed where the 24 bit image is converted into 8 bit image using the averaging method. It is a very simple method which averages the value of R G and B.

  Gimg = R(x, y) +G(x, y) +B(x, y) (1)

- Further to process every pixel separately Jarvis halftoning will be carried out which helps in differentiating between background and foreground contents. Halftone images of higher quality than other halftone. It quantifies each pixel using a neighborhood operation. The error diffusion scans the image one row at a time and one pixel at a time. The current pixel will be compared to a threshold (127) value. If it is above the value a white pixel will be generated in the resulting image. If the pixel is below the half way value, a black pixel is generated. The generated pixel is either full bright or full black [15].

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

- Every pixel in all three natural images will be counted and an XOR operation will be performed in the total number of black and

white pixels. A value is generated and the ascii value of the generated number will be calculated and added together. This ascii value is applied with the dynamic henon map which exhibits a very dynamic behavior. It will map the pixel co ordinate to a new position.

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

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

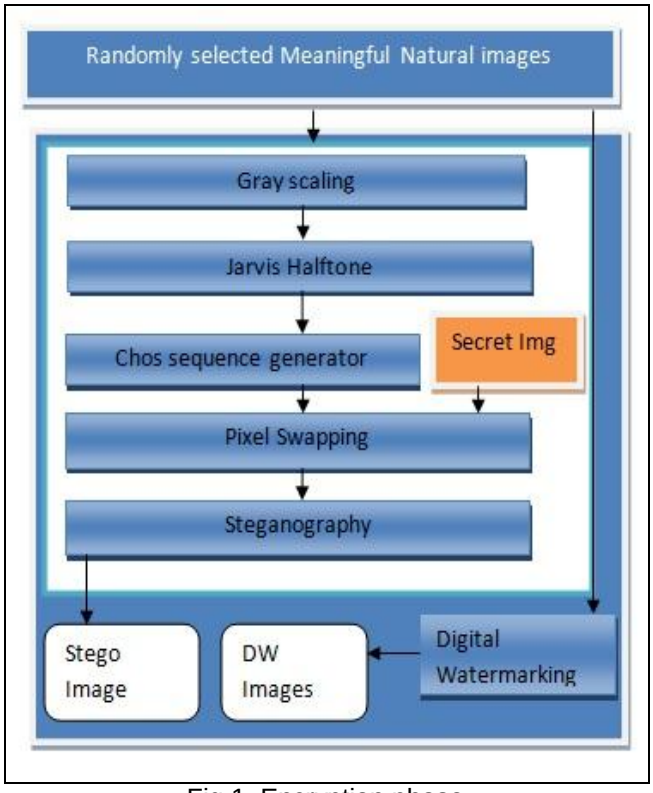

Fig.1. Encryption phase

- To further improve security of the share data hiding techniques like steganography is applied. This data hiding technique covers the secret noisy image under natural image which is large enough to hold the secret noisy share. This process will improve the usability of the share as well as reduces the hacker's attention on the noisy share. Least Significant Bit (LSB) steganography technique is a simple technique which embeds the pixel of secret image into the LSB bit of the cover image.

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 1010110

11100110 10000110 01101010 11100011

- During decryption de steganography will be performed and the embedded noisy secret image is retrieved. The natural images used will be selected from the same website that were used for encryption or through mail. The images are preprocessed and the unique key is regenerated. The sequence is applied to chaotic equation to generate the original coordinate position of every pixel in the secret image

Algorithm: - 1 ENCRYPTION ( )

Input: - NATURAL_IMAGES

Output: - STEGO_SHARE, W_IMG

1. Do for each Natural Image
2. For each pixel repeat 3-4
3. Calculate Grayscale value for each pixel..
4. Determine Threshold value of every pixel
5. Count the number of 0 and 1 in every natural image.
6. End of Loop
7. Perform XOR operation on number of 0's and 1's.
8. Generate the random unique key.
9. Calculate the new coordinate position (x,y) based on chaotic equation.
10. Store the watermark image in each natural images alpha channel.
11. Apply Steganography on the noisy share.
12. Output Stego Image
13. End

Algorithm: - 2 DECRYPTION ( )

Input: - STEGO_SHARE

Output: - SECRET_IMAGE

1. Read the stego share.
2. Calculate the LSB bit of the share.
3. Extract Noisy share.
4. The Meaningful image is accessed from the appropriate websites or database.
5. Generate the unique random sequence.
6. Swap the pixels of the noisy share.
7. End

715542 as the unique number which is used in combination with the chaotic equations to reposition the pixels of secret image.

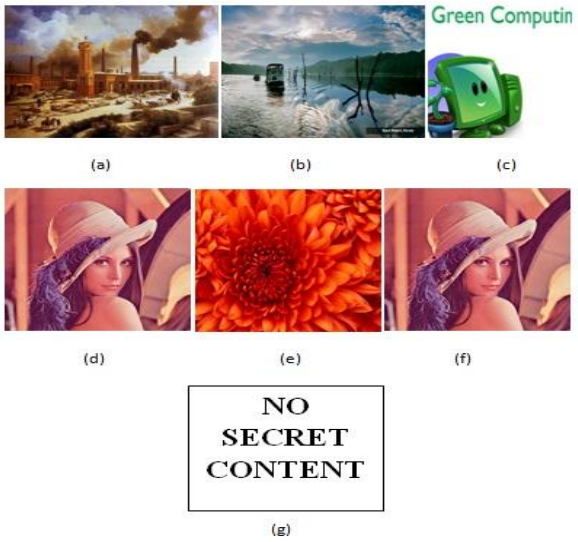

Fig 3. Experimental Results of New NVSS Scheme. a) Natural Image 1. b) Natural Image 2. c) Natural Image 3.d) Secret Image. e) Stego Image f) Recovered Secret Image g) Experimental result when the natural image is noisy or changed

.

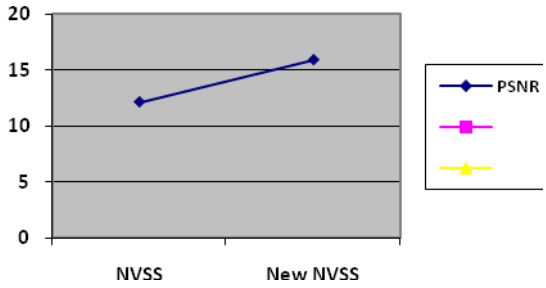

Fig. 4. Graph for PSNR

V. Comparative Study

This section shows the result of the proposed system and existing system.

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

V. Conclusion

This paper proposes a secured NVSS scheme which reduces the transmission risk issue present in the earlier system. The natural images are used without preprocessing it which reduces the distortion rate of the decrypted secret image to further extend the security of the share data hiding techniques like steganography and alpha channel watermarking are used .

The proposed system can be applied to biometric and voting system so that the combination of visual cryptography with these techniques can improve the security of the systems.

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.