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. 4, Issue 8, August 2016

Enhancing Visual Secret Sharing Using Natural Shares

Rekha V. Sarawade[1], Ashish B. Manwatkar [2]

ME Student, Dept. of Computer Engineering, ICEM, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, ICEM, Pune, India[2]

ABSTRACT: Now a days information is very important part of any organization. The Information is shared or transferred from person to person so security of such information is very important. Visual Cryptography is one of the encryption techniques that is used to process the original plaintext into cipher text. In visual cryptography shares are used for the transmission of the secret image. Shares are nothing but the photos or pictures and these shares are noisy shares which transmitted over the network. To transfer the Secret image random noisy pixels are used. Transmission of the secret image using noisy shares creates the transmission risk problem. To address noisy share issue natural visual secret sharing scheme is used for the transmission of the secret image. Natural shares are photos or pictures stored in digital form. Using these natural shares secret image transferred over the network. This NVSS scheme reduces the transmission risk problem using randomly selected unaltered natural shares. In this work key is extracted from randomly selected natural shares also to improve the security level data hiding technique is used.

KEYWORDS: Natural shares; Visual Cryptography; Natural Visual Secret Sharing; Plaintext; Ciphertext.

I. INTRODUCTION

Now a days transmission of the secret image securely from one location to another location is very important. Visual cryptography is a technique which is used for encryption of the secret image. Transmission of secret image without any risk or interruption is very important. Visual cryptography is used for transmission of secret image in non-computer aided environments but now days transmission of secret image in computer-aided environment is big issue for sharing of secret image in computer aided environment there are number of different techniques are avail- able. In these techniques meaningless shares are used for the transmission of secret im- age. But using meaningless shares creates a transmission risk problem also such a noise like shares can be easily detected by attacker that's why personal data get easily revealed also noisy shares are not user responsive [1].

When the number of shares increased management of large number of shares is very difficult. In the proposed system instead of using vss scheme natural visual secret sharing scheme is used to decrease the transmission risk. Using these natural shares secret image is transferred from sender to receiver. In natural visual secret sharing scheme n number of shares used for the transmission of the secret image and such a natural shares are meaningful images. In its place of changing the contents of natural shares the proposed system extracts the features from natural shares that is unaltered natural shares are used to transmission of secret image in order to decrease the transmission risk. Also for more security in this system steganography is used to hide the secret image. The encrypted data is transferred using secret image also in- formation stored in randomness format which is known to only sender and receiver. In this proposed system natural shares are used for transmission of secret image again this secret image concealed into another carrier image to provide more security. So in this proposed system using natural shares secret image is transferred to the receiver and again that secret image is concealed in carrier image so it reduce the transmission risk when we transfer secret image from one location to another location [2].

II. RELATED WORK

In this paper User friendly random grid technique is used [1] which is based on visual secret sharing random grid algorithm. So in this work it provides technique where meaningless shares are used for transmission of the secret

DOI: 10.15680/IJIRCCE.2016. 0408094

image. Meaningless shares is nothing but noisy share are used for transmission of the secret image from sender to receiver also random grid technique is provided to transfer the secret data securely. The main advantage of this system is user friendly and also there is no pixel expansion take place. Thus this proposed system provides RGVSS scheme by using meaningful shares. Embedded extended visual cryptography scheme [2] deliberated about secret sharing scheme using meaningful shares. The main purpose of this system to embedding random shares into meaningful covering shares and it is called as embedded extended visual secret sharing scheme (EVCS). Furthermore better the visual quality of the share images and it deals with gray scale images. In this system smaller pixel expansion takes place for the security purpose. This method provides the covering of secret image into meaningful shares. A novel based secret image sharing scheme [3] with size constraint based on true color secret images. Here size of the image reduced so encryption can be easily applied on such small images. In this system with size constrains and color images used for encryption. This used grouping of neural network and variant visual secret sharing scheme.

It confirms that the difference between the restored true secret image and the original one is not visually visible. It shows the size constraints and difference between cover images and camouflage images. The system required low computational power foe encoding and decoding shares. A high quality gray scale images with small shadow size visual secret sharing scheme [4] based on hybrid strategy. In this system instead of using color images gray scale images are used. Where the different techniques are used to increase the display quality of images. So the proposed system results in high quality images and also generates small grayscale shadows. Image size invariant for general access structure based on visual cryptography [5] to improve the display quality of recovered images. In this method instead of using pixel expansion technique used set of columns vectors to encrypt secret image. So this solution provides a high display quality of recovered images. A multitreshould secret sharing scheme [6] based on monotone span programs (MSP). This system used numerous secret images can be shares between a number of people and each secret image related with access structure.

The main objective of this system to construct multi- threshold access structure in secret image sharing. Extended capabilities for visual cryptography [7] discussed about access structure. In this system pixel expansion technique is used for transmission of secret image. Also in these method hyper graph colorings is used to increase the security level of secret image cryptography [8] to improve the display quality of recovered images. In this method instead of using pixel expansion technique used set of columns vectors to encrypt secret image. So this solution provides a high display quality of recovered images. A multitreshould secret sharing scheme [9] based on monotone span programs (MSP). This system used numerous secret images can be shares between a number of people and each secret image related with access structure. The main objective of this system to construct multi- threshold access structure in secret image sharing. Extended capabilities for visual cryptography [10] discussed about access structure. In this system pixel expansion technique is used for transmission of secret image. Also in these method hyper graph colorings is used to increase the security level of secret image.

III. PROPOSED SYSTEM AND ALGORITHM

A. *System Architecture and Description:*

In visual cryptography different techniques of encryptions used to convert original plaintext into cipher text. Visual secret sharing scheme is used for the transmission of secret image using noisy shares. And again this secret image is concealed in another carrier image for that it used simple and meaningful images but such images easily detected by attacker. So in proposed system natural shares are used for the transmission of the secret image. Natural shares are nothing but photos. Transmission of the secret image using natural visual secret sharing NVSS scheme is more secure as compared to the existing system where the natural shares are used for the transmission of the secret image and again this secret image concealed in another image that is called carrier image. In proposed system instead of generating secret.random key here key is extracted from the natural shares that’s why its very difficult for attacker to get secret data.

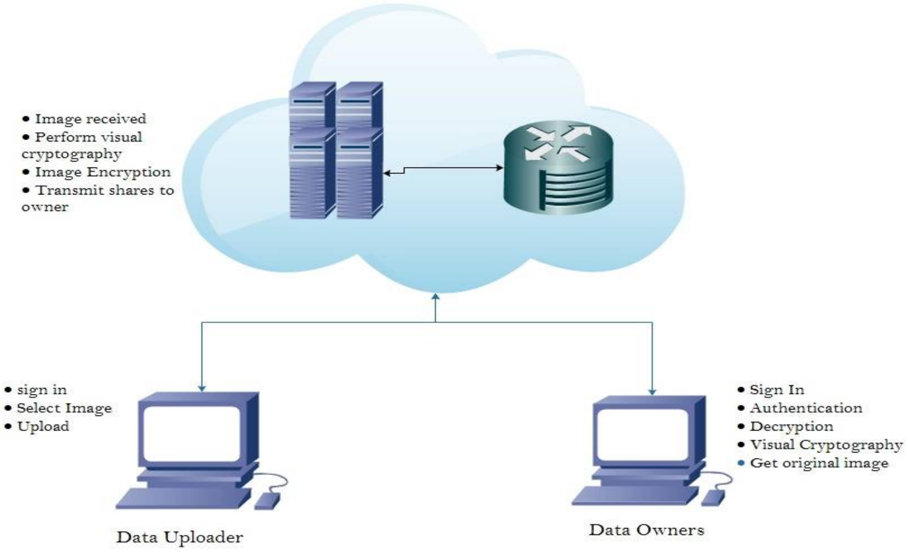


Fig 1: System Architecture

Above figure 1 shows the exact flow of the system and the methods used in the system. In the proposed system meaningful shares are used for the transmission of the secret image and there are different methods used to provide more security and transmission of secret image securely.

DESIGN

Following are the different steps included in the proposed system:

- **GRAYSCALING**

  Grayscaling is used in proposed system for the purpose to remove all the information related to the color. In this proposed system pictures or phots are used as natural shares. These natural shares maybe hand painted pictures or digital pictures so such images contains many information. So all the information related pic- ture is removed by ussinggrayscaling. Gras- caling is very important concepyt to remove all the information realated to image. Using grayscaling we get color image in balck and white format such grascaling images are very important in digital image sharing scheme. So here grascaling is used to remove all the color related information of original image.

- **IMAGE SHUFFLING**

  Shuffling is useful to disturb the correlation among the adjacent pixel. Shuffling of the image depends upon the number of rows and columns. Here, shuffling of pixel is done in two steps.

  Step 1: With each iteration, a quadrant is subdivided into sub quadrants. Image Encryption Using Henon Chaotic Map with Byte Sequence.

  Step 2: For the kth iteration, if it is odd then shuffling of quadrant is in clockwise direction otherwise anti-clockwise direction.

- **MESSAGE EMBEDDED STEGANOGRAPHY**

  Steganography can be classified into image, text, audio and video steganography depending on the cover media used to embed secret data. Text steganography can embedded a message secret key Steganography system is similar to a symmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. Anyone who doesn't know the secret key should not be able to obtain evidence of the encoded information.

- **HANON CHAOTIC MAP**

  Henon map was first introduced by Mivheealhenon. HENON map is a discrete time dynamic system. It is one of the most studied examples of dynamic system that exhibit chaotic behaviour. The map depends on two parameters, a andb other values may be chaotic or may converge to a periodic orbit. Chaos shuffling will be performed using this henon map technique. Now in chaos shuffling the positions of the pixels of an image will be scrambled in a way depending upon the chaotic map equation. And then again can be regenerated to its original positions by following the decryption process.

B. *Description of the Proposed Algorithm:*

Jarvis Halftoning:

For the purpose of performing thresholding to the three meaningful images, we make use the Jarvis halftoning algorithm. In the process of thresholding, the pixel of the greyscale image is considered and each pixel is checked whether it is greater than or less than the threshold value. If the pixel is greater than , its filled with black otherwise filled with white. The result of this basic method of thresholding is an image with blobs of black and white To have a clearer view of the threshold image we use Jarvis thresholding Algorithm. This algorithm makes use of error diffusion method. Error diffusion produces an image of much higher quality than the others. 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 is compared to a threshold value. If it is above the value a white pixel is 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.

Hanon Algorithm:

Chaotic systems are sensitive, non-liner, deterministic and easy to reconstruct after filling in the image. Henon map is one of the chaotic map used for generating Pseudo-random sequence required for encryption. Henon chaotic map is used as a symmetric key stream cipher cryptographic system. symmetric key for chaotic cryptographic system used for encryption at sender's end and decryption at receiver's end .
Thus, sensitivity of key and encryption algorithm together contributes to avoid all kind of cryptanalysis attacks.

Step 1: choose the initial value of (X1,Y1) for Henon map. This value works as an initial secret symmetric key for Henon map.

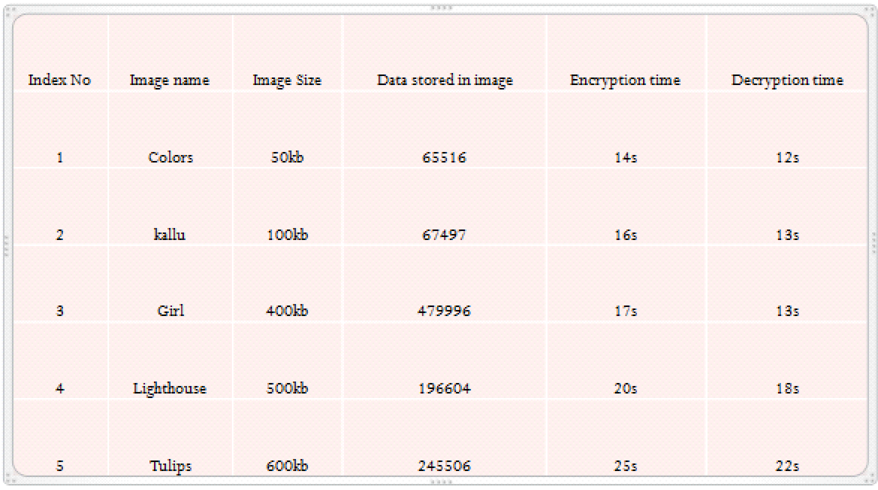
Step 2: Henon map work as a key stream generator for cryptosystem. The size of sequence depends upon the size of image.

Step 3: The decimal values are then converted into binary values depending upon this threshold value as given in equation.

Step 4: Henon sequence is then reduced by combining each consecutive 8 bits into one decimal values.Step 5: Encryption is done by bitwise Exclusive-OR operation between shuffled image and sequence generated in step 4.

IV. SIMULATION RESULTS

In this section, two encryption algorithms are compared. These are Natural visual secret sharing (NVSS) and Henon algorithm. Comparison of these two algorithms shows the encryption time of image. In following figure 2 it shows the different images having different size.shows that the Images with different sizes requires different encryption and decryption time. Image with smaller size required less time for encryption and decryption.



Index No	Image name	Image Size	Data stored in image	Encryption time	Decryption time
1	Colors	50kb	65516	14s	12s
2	kallu	100kb	67497	16s	13s
3	Girl	400kb	479996	17s	13s
4	Lighthouse	500kb	196604	20s	18s
5	Tulips	600kb	245506	25s	22s

Fig.2.Comparison of different images for encryption and decryption

These different images of different size are used for transmission of the secret image. This image shows the encryption time using the existing system and proposed system. In following figure 3 it shows the encryption time difference between RSA and HANON algorithm.

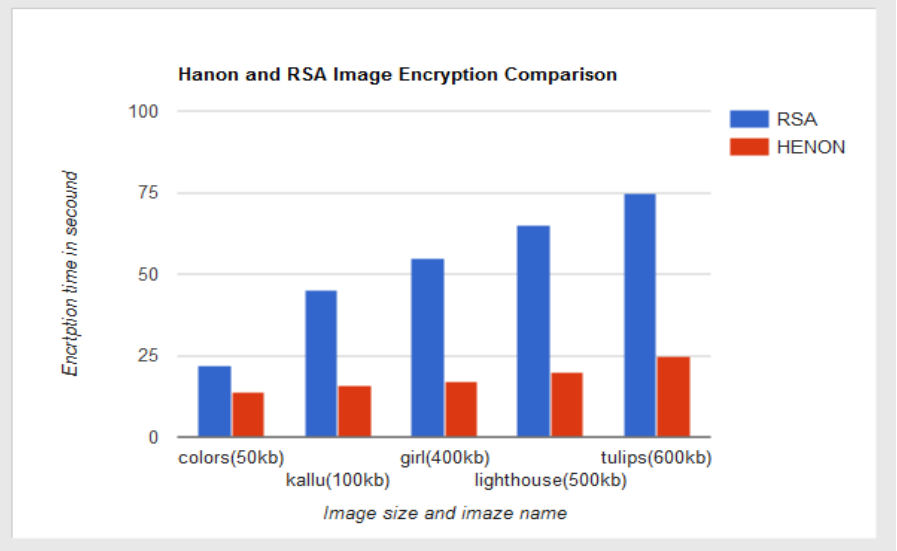


Fig.3.Comparison between RSA and HANON

Here compared the different encryption algorithms with current system. Using these algorithms tried to find the differences between the encryption and decryption time.

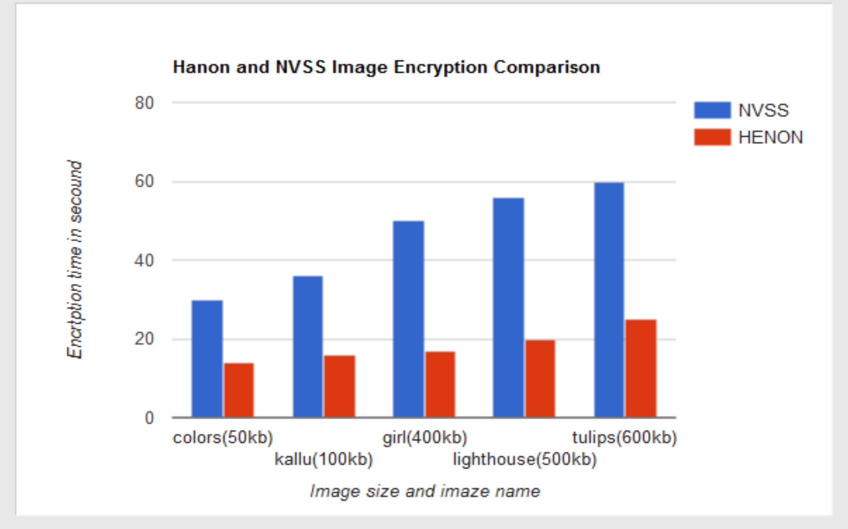


Fig.4.Comparison between NVSS and HANON

In above figure 4 shows the comparison between the existing system and proposed system. Also using graph it shows the differences between encryption and decryption time.

V. Conclusion and Future Work

Transmission of the information securely from one location to another location is very important. In previous work secret image transferred using noisy shares which creates transmission risk problem to overcome these disadvantages in this work a natural visual secret sharing scheme used. These Natural shares are used as meaningful images. Using these natural shares secret image transferred over the network. To further improve the security of the noisy shares steganography data hiding technique is used. Use of data hiding technique improves the security level as compared to the previous work. In future work number of number of natural shares can be increased to provide more security. Also here to hide the secret image message embedding method of steganography is used. In future other steganography method can be tried.

ACKNOWLEDGEMENTS

We would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. I am thankful to my Guide Prof. Ashish Manwatkar, PG Co-ordinator Prof. Manjusha Tatiya and Head of Department Prof. Ram Joshi, Contributed to this paper for their valuable comments and sharing their knowledge and idea.

References

1. T. H. Chen and K. H. Tsao, User-friendly random-grid-based visual secret sharing,Gizem, Aksahya&Ayese, Ozcan (2009) *Coomunications& Networks*, Network Books, ABC Publishers. IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 16931703, Nov. 2011.
2. F. Liu and C. Wu, Embedded extended visual cryptography schemes, IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307322, Jun. 2011.
3. 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. 32473254, Sep. 2009.
4. 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 grayscale images, Digit. Signal Process., vol. 21, no. 6, pp. 734745, Dec. 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. 38303841, Oct. 2013.
6. C. Guo, C. C. Chang, and C. Qin, A multi-threshold secret image sharing scheme based on MSP, Pattern Recognit. Lett., vol. 33, no. 12, pp. 15941600, Sep. 2012.

7. 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.
8. 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, pp. 18521863, Aug. 2012
9. Z. Wang, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography via error dif- fusion, IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383396, Sep. 2009.
10. 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. 132145, Jan. 2011.
11. A. Nissar and A. H. Mir, Classification of steganalysis techniques: A study, Digit. Signal Process., vol. 20, no. 6, pp. 17581770, Dec. 2010.
12. J. Fridrich, M. Goljan, and D. Soukal, Perturbed quantization Steganography with wet paper codes, in Proc. Workshop Multimedia Sec., Magdeburg, Germany, , pp. 415,Sep. 2004.
13. J. Fridrich, M. Goljan, and D. Soukal, Perturbed quantization steganography with wet paper codes, in Proc. Workshop Multimedia Sec.,Magdeburg, Germany, Sep. 2004, pp. 415.
14. 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.

BIOGRAPHY

Rekha V. Sarawade She has completed Bachelor of Engineering in Computer Engineering from Savitribai Phule Pune University.Currently pursuing Master of Engineering from Savitribai Phule Pune University.

Ashish B. Manwatkar He has completed Bachelor of Engineering in Computer Engineering from Nagpur University and ME from Savitribai Phule Pune University.Currently pursuing P.hd from Savitribai Phule Pune University.