A Comprehensive Review on Advance Mechanism For Secure Image Data Transmission

Ayoushi Kaul[1], Omkar Bhosale[2], Ambika Shastri[3], Prajit Karande[4], Varsha Dange (Guide) [5]

[1]UG Student, Dhole Patil College of Engineering, Pune, Maharashtra, India.
Ayoushi.kaul20@gmail.com

[2]UG Student, Dhole Patil College of Engineering, Pune, Maharashtra, India.
Omkarbhosalek15@gmail.com

[3]UG Student, Dhole Patil College of Engineering, Pune, Maharashtra, India.
Ambikashastri6@gmail.com

[4]UG Student, Dhole Patil College of Engineering, Pune, Maharashtra, India.
Karandeprajit@gmail.com

[5]Professor, Computer Department, Dhole Patil College of Engineering, Pune, Maharashtra, India.
Dange.varshar@gmail.com

---***---

Abstract: - *Traditional encryption techniques are just converting the readable images into some unreadable format i.e. cipher text format. This encrypted cipher text can be very conveniently transmitted over the network, but anyone who gets the key can easily get the secret encrypted message from cipher text. But the new Secret sharing scheme is a process of sharing and transmitting the images over the network. But the major drawback over here is that transmitting images over network pulls attackers attention as the images are in noise like format. In the recent study, many researchers tried to make the VSS system more secure. This paper presents the survey of the studies done earlier and thereby analyses the drawbacks and proposed a new technique considering VSS.*

Keywords: **- Cryptography, Encryption, Natural image Steganography, Visual Secret Sharing Scheme.**

1. Introduction: -

The rapid growth of internet and internet services which needs connecting multiple devices , computers together so that the transmission of the data can be carried out needs a higher level of security in this stage. Traditional encryption techniques are just converting the readable images into some unreadable format i.e. cipher text format. Encryption process is the process of using the hash function and indirectly a mathematical function that makes the data get converted into unreadable format which is safe for transmitting over the internet.

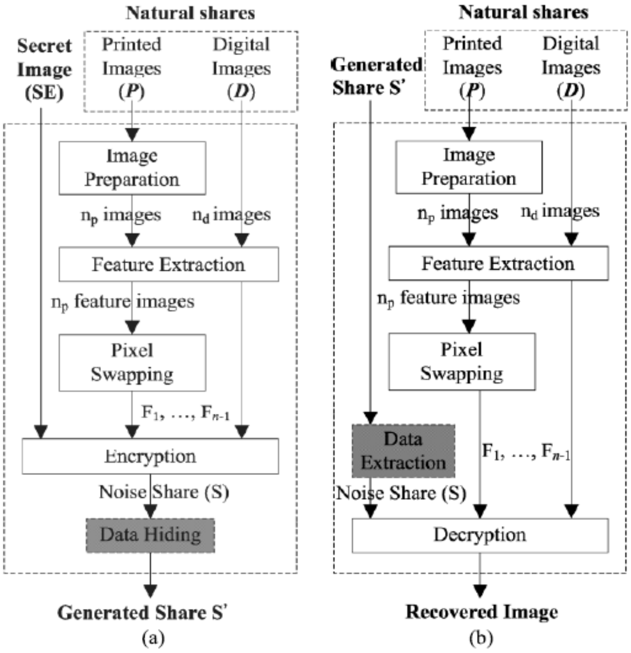


Figure 1. System working of [1] system

Using the conventional Image sharing, which can contain several random and useless pixels, even if these image sharing techniques satisfy the security requirement for safeguarding the secret data, but it is prone to some issues such as attackers attention as the images are noise like, and second issue is that these noise like meaningless shares are very user unfriendly. If the count of the shares being shared and the share quality is enhanced, then it can become trickier and difficult to expose the necessary information.

The process in which n pieces of images or shares carry each share into it is called as Visual Cryptograph (VC). Secret images can be in the form of handwritten documents, images, photographs and so on. Sharing and delivering secret images over the internet in the non-computer environment is a process of Visual Secret Sharing [1].

2. Literature Survey: -

P. L. Chiu and K. H. Lee presented a pixel-expansion-free value VCSs method on the basis of optimal binarization technique for visual cryptography of binary images. To grade the evaluation of the quality of the extracted or recovered image, author considered the black pixels or blackness as the metric to measure quality.

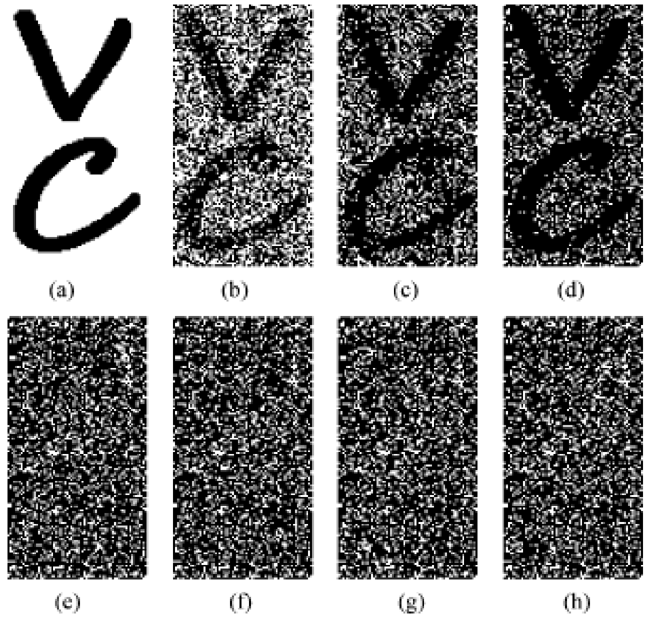


Figure 2. Image stages in [2] system

Their contribution is proposed as a two-fold method, first fold is formulating the problem as an optimization using mathematics and in return to highly increase the contrast of extracted images that are lead to blackness constraints and density-balance, and second they proposed a new AI based simulated-annealing algorithm to solve this VSS problem. The proposed optimization-based approach efficiently competes existing techniques in terms of both the display quality of recovered images and pixel expansion factor [2].

K. H. Lee and P. L. Chiu presented visual cryptography faces an uncontrollable display quality issues or a pixel-expansion problem, for extracted images. To resolve these issues in paper, author proposed a systematic and general method without convenient codebook design. This presented technique can be definitely used for binary secret images in non-computer controlled decryption environments. So To encrypt secret data pixels author proposes a set of column vectors method rather than using the traditional VC-based method to address issue of pixel expansion [3].

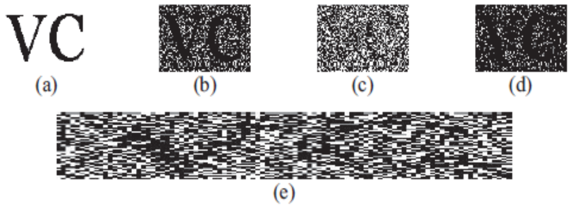


Fig. 4. Comparison between other approaches and the proposed study on the worst case result (i.e., set {1, 2, 3}) of access structure {{1, 2, 3}, {1, 4}, {3, 4}}, (a) Secret image with 96 × 64 pixels (192 DPI), (b) the recovered images of this study (contrast $\alpha_{\min} = 2/9$, blackness $\beta = 1$), (c) the recovered image of Hsu's study ($\alpha_{\min} = 0.15$, $\beta = 0.75$), (d) the recovered image of Lee's study ($\alpha_{\min} = 1/8$, $\beta = 1$), (e) the recovered image of Ateniese's study (pixel expansion factor = 5, $\alpha_{\min} = 1/5$, $\beta = 0.8$).

Figure 3. Comparison with existing and system [3]

Z. Wang, G. R. Arce, and G. D. Crescenzo presented a novel framework named as halftone visual cryptography to obtain visual cryptography through half toning. Based on blue noise dithering technique, the presented method makes use of the void and cluster algorithm to encrypt a secret binary image into halftone shares carrying significant visual information. The obtained visual quality is much better than all previous visual cryptography techniques. The presented technique has multiple visual secret sharing applications such as electronic cash, watermarking, which requires a very high-quality visual images [4].

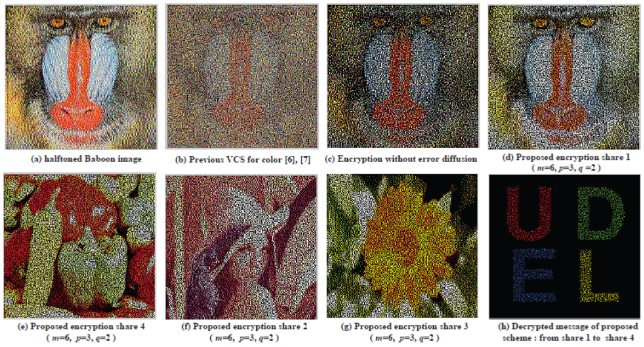

(a) halftoned Baboon image
(b) Previous VCS for color [6], [7]
(c) Encryption without error diffusion
(d) Proposed encryption share 1 (m=6, p=3, q =2)
(e) Proposed encryption share 4 (m=6, p=3, q=2)
(f) Proposed encryption share 2 (m=6, p=3, q=2)
(g) Proposed encryption share 3 (m=6, p=3, q=2)
(h) Decrypted message of proposed scheme : from share 1 to share 4

Figure 4. Comparison of existing system with system [4]

I. Kang, G. R. Arce, and H. K. Lee presented phenomenon known as a color visual cryptography process which prepares meaningful color n shares via error diffusion and Visual information pixel (VIP) synchronization for visual sharing recovered quality improvement. (VIP) Visual information pixel synchronization preserves the same original VIP values pre and post encryption and error diffusion then generates n shares with higher` visual quality. VIP synchronization or error diffusion mostly used in various visual cryptography schemes for color images. As compare with previous approaches proposed approach gives superior performance [5].

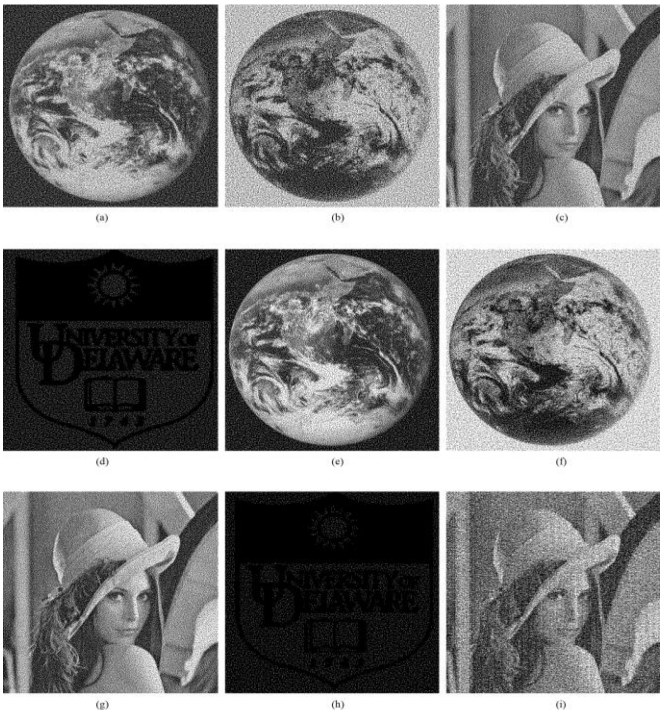


Figure 5. Comparison of existing systems with system [5]

T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le proposed a new secret sharing scheme for grayscale images. Proposed scheme is based on three approaches, block truncation coding (BTC), discrete wavelet transform (DWT) and vector quantization (VQ) technique. An original image is replaced with a set of much smaller shadows and each shadow does not reveal information about the original image. Due to this quality the security of the proposed scheme is guaranteed. This proposed scheme can be applied to both grayscale and color images. Results confirm that this scheme not only generates a high quality reconstructed original image but also generates small, random-like grayscale shadows [6].

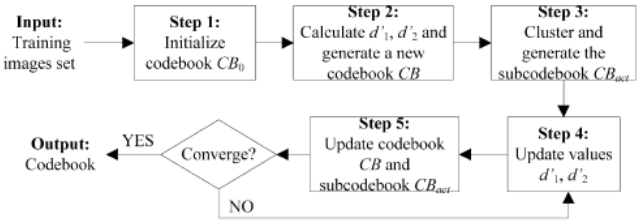

Input: Training images set
Step 1: Initialize codebook CB_0
Step 2: Calculate d'_1, d'_2 and generate a new codebook CB
Step 3: Cluster and generate the subcodebook CB_{act}
Step 4: Update values d'_1, d'_2
Step 5: Update codebook CB and subcodebook CB_{act}
Converge?
YES
NO
Output: Codebook

Figure 6. Codebooks generation algorithm [6]

D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang proposed a novel and efficient secret image sharing scheme for true-color secret images. By combing neural networks and variant visual secret sharing, the quality of the reconstructed secret image and disguise images are visually the same as the original images. Only proposed scheme supports true-color secret image with size constraint on shares as compare to other [7].

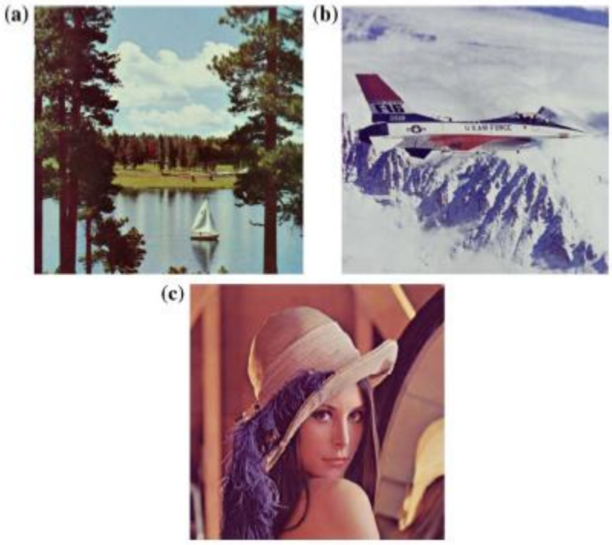


Figure 7. Camouflage images: (a) Boat, (b) F16 (size of both nine times that of the secret image). Reconstructed secret image (c) Lena.

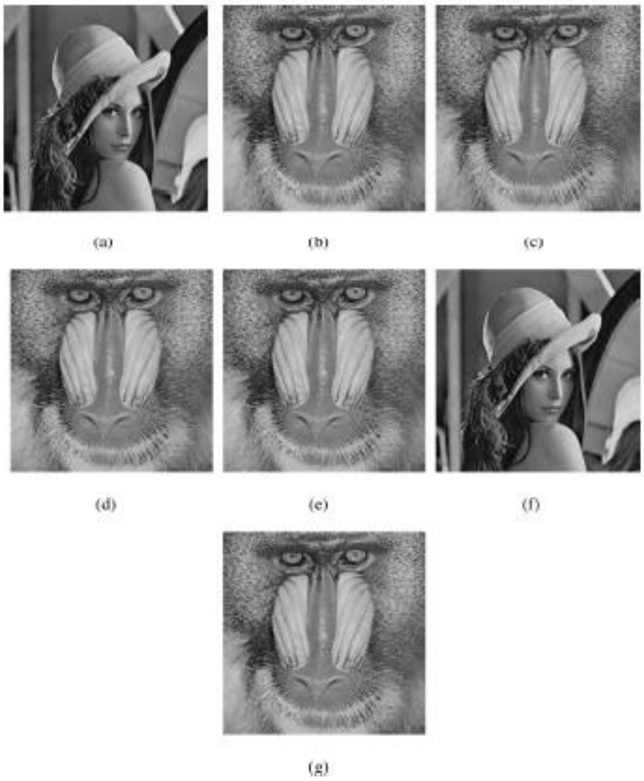


Figure 8. An example of the (4, 4)-threshold case with reversible steganography. (a) The secret image, (b) stego image S1, PSNR = 37.91 dB, (c) stego image S2, PSNR = 37.90 dB, (d) stego image S3, PSNR = 37.91 dB, (e) stego image S4, PSNR = 37.92 dB, (f) lossless reconstruction of the secret image, and (g) the distortion-free recovered cover image.

D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang proposed anew secret image sharing scheme with reversible steganography. A reversible cellular automaton with memory is added in the proposed scheme to produce shared data, which are implanted into cover image to form stego images. Computation cost of the proposed scheme is lower than other approaches. The proposed scheme is useless in differential attacks [8].

3. Conclusion:-

Thus this paper presented an all-inclusive survey of secret sharing scheme. The main features, the advantages and disadvantages of each are described. As per survey, strong need to develop the secure secrete scheme for sharing images over network. In proposed work is the combination of data hiding, random shuffling and the encryption technique. Using this we achieve the original image with security.

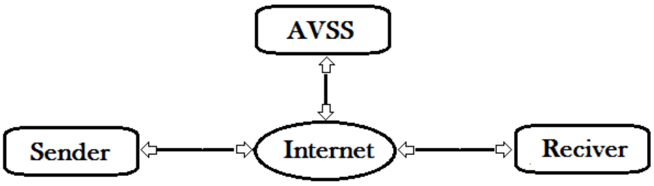
4. Acknowledgement:-

We would like to thank our Principal Dr. Satish B. Allampallewar for giving us the opportunity to work on this project. We would like to show our sincere gratitude to our guide Prof. Varsha Dange for her guidance and knowledge without which this paper would not be possible. She provided us with valuable advice which helped me to accomplish writing this paper. I am also thankful to my HOD Dr. Arati Dandavate, Department of Computer Engineering, for his constant encouragement and moral support.

5. Proposed System:-

The proposed system is a novel technique and not a part of any other software. In the proposed system splits the image to be sent into n number of small shares, then hide these pieces into n natural images and send these natural images to the intended person. Here to make the system more secure the n images are hidden into n natural images, the splitted image sequence is shuffled and the sequence of hiding the images into natural images thus gets varied. The additional requirement for the proposed system is availability of any mailing server through which the subordinate decryption and arrangement pattern can be sent to the receiver in order to obtain the original secret data from the steganographed images. It is then the receiver who has to extract the pieces of images from natural images and then combine the pieces in the original sequence by following the sequence sent by sender to his/her email id.

6. System Architecture:-



7. 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] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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. 734–745, Dec. 2011.

[7] 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. 3247–3254, Sep. 2009.

[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. 1852–1863, Aug. 2012.