http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-10, Issue 11, October 2021

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-05

A LITERATURE SURVEY OF DIFFERENT DATA HIDING FOR SECRET DATA ENCRYPTION AND DECRYPTION

Sonal Karade[1], Prof. Savita Chouhan[2],

[1]M.Tech Scholar, [2]Assistant Professor,

[1,2]Department of Electronics & Communication Engineering

[1,2]Bhopal Institute of Technology (BITS), Bhopal (M.P), INDIA,

[1]karadesonal86@gmail.com, [2] Chouhansavita@gmail.com

***Abstract*— In this survey paper discuss the different data hiding techniques in image encryption and decryption. In the last era worm black hole is increase exponential day to day. Due to this large number of secret data hiding techniques are introduced. In this survey discuss the different data hiding techniques in image processing. In this survey paper shows literature review on different data hiding techniques. Data hiding in the image is art of science in which embedding the secret data into the image using different methods like image stenography, cryptography and visual cryptography. Also discuss the quality check parameters like SSIM, visual quality of the images in terms of edges and others human perception.**

***Keywords*—Steganography, cryptography, Structural similarity index measurement (SSIM) and Image data hiding. etc.**

I. INTRODUCTION

In the field of image processing image for data security various traditional approaches like Cryptography, Steganography, and Data Hiding can be used. Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data integrity, and of data authentication. In cryptography a plain message is encrypted into cipher text and that might look like a meaningless jumble of character whereas in case of steganography, the plain message is hidden inside a medium that looks quite normal and does not provide any reason for suspecting the existence of a hidden message. Such an image is called as stego-image. Data hiding conceals the existence of secret information while cryptography protects the content of messages. More and more attention is paid to reversible data hiding in encrypted images. The hidden data in the cover image may be any text related to the image such as authentication data or author information. Reversible data hiding represents a technique where the data is embedded in the host media and at the receiving end the secret data and also the host media will be recovered loss less level.

Reversible data hiding Reversible data hiding can be defined as an approach where the data is hidden in the host media that may be a cover image. A reversible data hiding is an algorithm, which can recover the original image loss less after the data have been extracted.

The transmitter side of such systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data. The reversibility means that not only the embedded secret data but also the encrypted cover image must be extracted lossless at the receiver side.

II. BACK GROUND

Image data hiding processes are essentially part for any secret data communication. When hide the secret data in an image quality of image degrade. Hence techniques that ask for to enhance the interpretability or perception of images for the human viewers and providing higher input for the automated image process techniques. In this paper focused on different data hiding techniques.

Visual Cryptography –

Visual Cryptography is an emerging crypto-graphic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visual system, without the aid of computers. It uses a simple algorithm unlike the complex. It needs neither cryptography knowledge nor complex computation. Visual cryptography technique (for black and

ISSN(ONLINE):2278 - 3814

white images) is introduced by Naor and Shamir in 1994 during EUROCRYPT'94. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information. Basic visual cryptography is expansion of pixels. Visual cryptography is a method of sharing a secret image among a group of participants, where certain group of participants is called as qualified group who may combine their shares of the image to obtain the original, and certain other group is defined as forbidden group who cannot obtain any information on the secret image, even if they combine knowledge about their parts. The scheme gives an easy and fast decryption process that is done by stacking the shares onto transparencies to reveal the shared image for visual inspection.

Steganography –

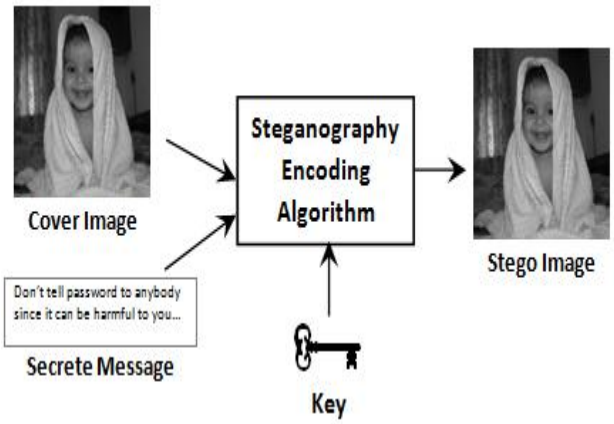
Image steganography terminologies are as follows:-

Cover-Image: Original image which is used as a carrier for hidden information.

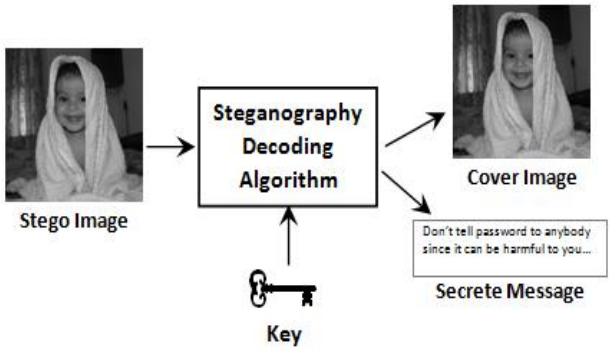
Message: Actual information which is used to hide into images. Message could be a plain text or some other image.

Stego-Image: After embedding message into cover image is known as stego-image.

Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.



(a) Stego Image Generated at Sender Side



(b) Message extraction at receiver side

Fig.1. Concept of Steganography

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [19]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm un-hides the message from stego-image.

II.LITERATURE SURVEY

Karolin, M.,et. al "Authentic secret share creation techniques using visual cryptography with public key encryption." [2021], In this paper, shares of the secret image in visual cryptography process are created by using the multiple share creation method with VSS. The Existing AES algorithm compared with RSA algorithm purpose of the image encryption and decryption of the secret image. The shares are separately created by encryption and decryption techniques with VSS. In the encryption process is generated by the public key and decryption process is generated by the private key. Decryption process is generated by private key and RSA (Rivest Shamir and Adleman) optimization techniques. PSNR values for the different secret images are 156.32, 123.44, and 132.27. The MSE values are minimized in all images 0.5031, 0.3277 and 0.2156. The Number of Pixel Changing Rate value is 69.44, 65.21 and 67.03. The Unified Averaged Changed Intensity value is 13.88, 11.26 and 12.01. The performance of the secret image can be increased by using the other method is instead of VSS. The PSNR value is improved by using this image quality and improve the all images minimized Mean Square Error values. So, the Visual Cryptography secret share creation technique is one of the essential the cyber world to transfer the information with confidential. The final result of the paper reveals that the proposed RSA method is improved

than existing method. This result suggests that RSA algorithm is suitable for send and receive the information with high quality and security. The encryption and decryption time is faster than existing method. It is time saving in the machine life. Finally, the RSA algorithm gives highly secured image encryption and speed decryption [1].

Kukreja, et.al. "Curvelet transform based robust copyright protection scheme for color images using extended visual cryptography" [2020], In this paper, a secure and robust copyright protection scheme for color images is proposed. The non fine scale layers of curvelet transform coefficients of Y channel of the image have been utilized to provide high robustness to the scheme. An additional watermark is created from Cb, Cr channels of the image to handle the false positive cases. To prove the copyright, the watermarks can be retrieved by OR-superimposition of ownership share with master share and its rotated version. Experimental results have been performed on different images for different attacks. NC value of the extracted watermark is maintained at 0.99 or more while BER is maintained below 0.1, which proves that the scheme has outstanding resistance to attacks. The advantages of the proposed copyright protection scheme are that the watermark's size is not restricted to the size of the protected image; the self constructed watermark handles false positive cases, and meaningful shares ensure security of the scheme. Comparison with the other exiting copyright protection schemes for color images reveals that the proposed scheme gives better performance [2].

Fatahbeygi, Ali,et. al . "A highly robust and secure image watermarking based on classification and visual cryptography." [2019], In this paper a new scheme for copyright protection based on block classification and visual cryptography has been presented. Our method is completely imperceptible because the binary watermark is concealed without modifying the original image, and it can be revealed for rightful ownership by stacking two share images without the aid of computers. Also, the combination of canny edge detector, block classification and visual cryptography was used to improve the security of the proposed watermarking scheme. Due to the use of local and robust features of different regions of the image and avoidance of some weak blocks for watermarking, the robustness of the proposed scheme has been improved. The experimental results show that the presented technique can effectively resist common image processing attacks, such as JPEG compression, Gaussian noise, average filtering, histogram equalization, median filtering, gamma correction, rotation, resizing and sharpening [3].

Kulkarni, Pranesh, et. al "Visual cryptography based grayscale image watermarking in DWT domain." [2018], Watermarking is a technique to protect the copyrights of digital media like image, audio, video, etc. Visual Cryptography (VC) is a scheme for hiding information in still images. The Visual Cryptography Scheme splits the secret image into unintelligible images, these images are called shares. The shares are distributed to 'n' participants. Any 'k' shares out of 'n' reveal the secret image and less than 'k' shares recover no information about secret. Amalgamating Visual cryptography with watermarking yields the best solution for resolving image ownership disputes and detection of infringements of copyrights. In this paper, (2,2) VC scheme is employed, one of the shares is embedded in the low frequency domain of DWT and the other share is registered with the Trusted Authority(TA). The secret image is obtained by performing XOR operation on the two shares. The experimental results revealed that the proposed scheme can not only prove the ownership of image but also withstand various image processing attacks [4].

Mirko Köhler, et. al "Protecting Information with Sub-codstanography" [2017], In modern communication systems, one of the most challenging tasks involves the implementation of adequate methods for successful and secure transfer of confidential digital information over an unsecured communication channel. Many encryption algorithms have been developed for protection of confidential information. However, over time, flaws have been discovered even with the most sophisticated encryption algorithms. Each encryption algorithm can be decrypted within sufficient time and with sufficient resources. The possibility of decryption has increased with the development of computer technology since available computer speeds enable the decryption process based on the exhaustive data search. This has led to the development of steganography, a science which attempts to hide the very existence of confidential information. However, the stenography also has its disadvantages, listed in the paper. Hence, a new method which combines the favorable properties of cryptography based on substitution encryption and stenography is analyzed in the paper. The ability of hiding the existence of confidential information comes from steganography and its encryption using a coding table makes its content undecipherable. This synergy greatly improves protection of confidential information. [5]

B. Pushpa Devi, et. al, "A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography" [2016], This work proposes a new watermarking algorithm based on the shuffled singular value decomposition and the visual cryptography for copyright protection of digital images. It generates the ownership and identification shares of the image based on visual cryptography. It decomposes the image into low and high frequency sub-bands. The low frequency sub-band is further divided into blocks of same size after shuffling it and then the singular value decomposition is applied to each randomly selected block. Shares are generated by comparing one of the elements in the first column of the left orthogonal matrix with its corresponding element in the right orthogonal matrix of the singular value decomposition of the block of the low frequency sub-band. The experimental results show that the

proposed scheme clearly verifies the copyright of the digital images, and is robust to withstand several image processing attacks. Comparison with the other related visual cryptography-based algorithms reveals that the proposed method gives better performance. The proposed method is especially resilient against the rotation attack.[6].

Priyanka Singh, et. al, "A Reversible Robust Watermarking Scheme Based on Two out of Two Visual Cryptography Approach" [2016], A reversible visual cryptography based robust watermarking scheme has been presented in this paper. Reversibility has been maintained in the scheme as such no changes are made into the cover image. The image information is obtained based on its homogeneity using the quad tree based decomposition setting a threshold criteria. Thereafter based on the largest singular values, features are obtained and classified using kmedoid clustering. A master share is thus obtained based on the clustering result which together with the secret image furnishes the ownership share. The ownership share thus obtained is managed by the certificate authority to verify the rightful ownership if any dispute arises in future. The robustness of the scheme has also been tested against comprehensive set of attacks and was found to be comparatively efficient as compared with the existing state of art approaches.

A reversible watermarking based on the two out of two visual cryptography has been proposed here. It exploited the homogeneity and singular values of the cover image to obtain image specific information and build the master share. Consequently, combined with the secret image, the ownership share was built and stored with the certificate authority along with the private key. If any dispute situation arises, the registered share could be stacked with the master share obtained from suspected image to prove the claim. The scheme demanded no resources or heavy computations for decryption and was found to be robust against various attacks like JPEG compression, histogram equalization, rotation, noises etc. Future study may be focused on exploring k out of n visual cryptography for addressing multiple owner problem. [7]

IV.CONCLUSION

In this survey paper discus the different data hiding process of images. In this survey discuss about data hiding and also reversible data hiding schemes. A short discuss on steganography, cryptography and visual cryptography. Finally discuss the visual cryptography based different methods and it advantages. In the above discuss visual cryptography is better method for data hiding as compare to steganography and cryptography. In the future work proposed a new method for data hiding that is based on the visual cryptography (VC). Visual cryptography based data hiding methods provide double layer of security and better authentication process as compare to other methods that is discuss in this paper.

REFERENCE

[1] Karolin, M., and T. Meyyappan. "Authentic secret share creation techniques using visual cryptography with public key encryption." Multimedia Tools and Applications 80.21 (2021): 32023-32040.

[2] Kukreja, Sonal, Geeta Kasana, and Singara Singh Kasana. "Curvelet transform based robust copyright protection scheme for color images using extended visual cryptography." Multimedia Tools and Applications 79.35 (2020): 26155-26179.

[3] Fatahbeygi, Ali, and Fardin Akhlaghian Tab. "A highly robust and secure image watermarking based on classification and visual cryptography." Journal of information security and applications 45 (2019): 71-78.

[4] Kulkarni, Pranesh, and Girish Kulkarni. "Visual cryptography based grayscale image watermarking in DWT domain." 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2018.

[5] Mirko Köhler, Ivica Luki, and Višnja Kri Danovi Hik "Protecting Information with Sub-codstanography", Hindawi Publishing Corporation, Security and Communication Networks, Volume 2017,1 -13, 2017.

[6] B. Pushpa Devi, Kh. Manglem Singh and Sudipta Roy, "A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography" Springer plus, 1 -22, 2016.

[7] Priyanka Singh, Balasubramanian Raman and Manoj Misra, "A Reversible Robust Watermarking Scheme Based on Two out of Two Visual Cryptography Approach", IEEE Region 10 Conference (TENCON) -Proceedings of the International Conference, 1628 – 1633, 2016.

[8] .Mirko Köhler, Ivica Luki, and Višnja Kri Danovi Hik "Protecting Information with Sub-codstanography", Hindawi Publishing Corporation, Security and Communication Networks, Volume 2017,1 -13, 2017.

[9] .B. Pushpa Devi, Kh. Manglem Singh and Sudipta Roy, A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography" Springer plus, 1 -22, 2016.

[10] .Y. Jina Chanu and T. Tuithung, "A Watermarking Scheme for Digital Images Based on Visual Cryptography", Contemporary Engineering Sciences, Vol. 8, no. 32, 1517 - 1528, 2015.

[11] .Geum-Dal Park Dae-Soo and Kim Kee-Young Yoo, "Lossless Codebook-Based Digital Watermarking Scheme with Authentication" 11th International Conference on Information Technology: New Generations, 2014.

[12] Rawat, S, and Raman B, "Visual-crypto graphy-based blind watermarking scheme for copyright protection", International Journal of Signal and Imaging Systems Engineering, vol.6, no.3, pp. 158-163, 2013.

[13] Th. Rupachandra Singh, Manglem Singh and Sudipta Roy," Image Watermarking Scheme based on Visual

Cryptography in Discrete Wavelet Transform", International Journal of Computer Applications, 0975 – 8887,volume 39– No.1, February 2012.

[14] .S. Radharani and Dr. M.L. Valarmathi, Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptography, International Journal of Computer Applications, volume 23, No.3, June 2011.

[15] .F. Liu and C.-K. Wu, "Robust visual crypto graphy-based watermarking scheme for multiple cover images and multiple owners" Published in IET Information Security Received on June 2010, vol. 5, issue. 2, pp. 121–128, 2010.

[16] .Wang, M.S. and Chen, w.e. "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography", Computer Standards & Interfaces, vol. 31, pp. 757-762, 2009.

[17] .Chen, T.H., Chang,e.e., Wu, e.S. and Lou, D.e., "On the security of a copyright protection scheme based on visual cryptography", Computer Standards & Interfaces, vol. 31, pp. 1-5, 2009.

[18] .Sleit, A., and Abusitta, A., "A visual cryptography based watermark technology for individual and group images", Systems Cybernetics and Informatics, vol. 5, no. 2, pp. 24- 32, 2008.

[19] .Lou, D.e., Tso, H.K., Lin, J.L, "A copyright protection scheme for digital images using visual cryptography technique", Computer Standards & Interfaces, vol. 29, pp. 125-131, 2007.

[20] .Zhi Zhou, Member, Gonzalo R. Arce and Giovanni Di Crescenzo," Halftone Visual Cryptography" IEEE Transactions on Image Processing, Vol. 15, No. 8, 2441 – 2453, August 2006

[21] .Hsu, e.S. and Hou, Y, "Copyright protection scheme for digital images using visual cryptography and sampling methods, Optical Engineering, vol. 44, 2005.

[22] .Chang, e.e. and Chung, J.e. "An image intellectual property protection scheme for gray level images using visual secret sharing strategy", Pattern Recognition Letters, vol. 23, pp. 931-941, 2002.

[23] Wang,e.e., Tai, S.e., and Yu, C.S., "Repeating image watermarking technique by the visual cryptography", IEICE Transactions on Funda -mentals , pp. 1589-1598, 2000.

[24] .Hou, ye and Chen, P.M., "An asymmetric water marking scheme based on visual cryptography", In Proceedings of the 5th Signal Processing Conference, vol.2, pp.992-995 ,2000.

[25] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February, 1998.

