http://ijea.jctjournals.com/ ISSN(ONLINE):2320 – 0804

Volume-10, Issue-12, December, 2021

International Journal of Engineering Associates (IJEA)

Page Number: 01-06

A VISUAL CRYPTOGRAPHY BASED DATA HIDING TECHNIQUE FOR SECRET DATA ENCRYPTION AND DECRYPTION

[1] Sonal Karade*(M.Tech Scholar),* [2] Prof. Savita Chouhan*(Associate Professor)*

[#1]Department of *Electronics &* Communication Engineering

Bhopal Institute of Technology (BITS), Bhopal(M.P), INDIA

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

ABSTRACT – In this research paper discuss the noble secret data hiding techniques in image encryption and decryption. In the last era cybercrime is increasers rapidly. Due to this large number of secret data hiding techniques are introduced. In this research paper shows visual cryptography based data hiding technique. In this technique hide the secret data hiding in the image in two parts that is master and slave. After that embedded the secret data into the image using stenography. Also discuss the quality check parameters like PSNR, MSE, RMSE, MAE and SSIM. Visual quality of the images in terms of edges and others human perception. The proposed robust method shows better result as compare to other method in terms of different attacks. For the measurement of performance of proposed method use different attacks and apply of image and check result.

***Keywords*— Steganography, cryptography, Structural, peak signal to noise ratio, mean square error, mean absolute error and Image data hiding**

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. One of the known techniques has been attributable to Moni Naor and Adi Shamir, who developed it in 1994.Visual cryptography, may be a science technique for securing images. In visual cryptography images are divided into n-number of shares which give security for the images and stacking or overlapping of those shares reveal the initial secret image. Initially, it was developed for binary images. Different schemes are used to generate shares for secret images. Later in visual cryptography several advance ways are came into exist, those are extended visual cryptography, Visual cryptography for color images i.e. gray and RGB/CMY images. These ways are meant just for revealing the complete secret image.

Visual cryptography hides secrets inside the images i.e. image is split into multiple shares and subsequently rewrite with none computation .This decoding is completed by superimposing the shares which can reveal the key image or text by the human sensory system. Initially the model which was developed consists of a page of cipher text and a page of transparency (secret key). The clear text (original text) is obtained by superimposing the transparency with the key over the cipher text. Later on this model is extended by k out of n secret sharing scheme where secret sharing is a technique in which secret shares are distributed among the participant. Thus the secret is able to reveal only when adequate number of shares are stacked together. In (k, n) secret sharing scheme secret image is revealed only when k or more than k shares are stacked. But shares less than k will not reveal any information. Later visual cryptography is advanced for color images. Several techniques are developed supported the color decomposition technique for color images and RGB/CMY images. Image or a text used in secret sharing may be a combination of black and white pixels. These white and black pixels seem in n changed version known as shares.

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.

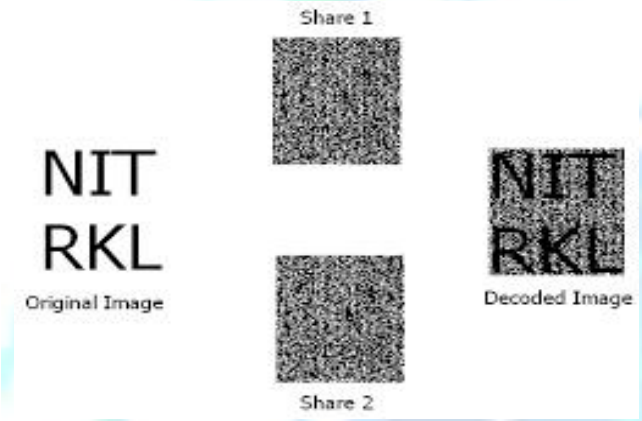

Fig. 1. Shows the visual Cryptography

II. IMAGE PROCESSING

Image process is nothing however the study of sequence of image pixels, i.e. Digital image process is nothing however the study of images or process of images by electronic device .When victimization digital instrumentality to capture, store, modify and think about photographic images, they have to 1st be regenerate to a group of numbers in an exceedingly method known as digitisation or scanning. Computers are superb at storing and manipulating numbers, thus once your image has been digitized you'll use your computers to archive, examine, alter, display, transmit, or print your images in a fantastic sort of ways in which.

2.1 Types of Digital Images

For photographic functions, there are 2 necessary styles of digital images colour and black & white. color images are created of color pixels and whereas black & white images are manufactured from pixels in several reminder grey.

Black and White Images

A black and white image is formed of pixels every of that holds one range like the grey level of the image at a specific location. These grey levels span the complete vary from black to white in an exceedingly series of very fine steps, commonly 256 completely different grays. Since the attention will barely distinguish regarding two hundred completely different grey levels, this can be enough to offer the illusion of a step less tonal scale as illustrated below:

Figure 2: Different Gray Levels

Assuming 256 grey levels, every black and white constituent are often hold on during a single computer memory unit (8 bits) of memory to show them. A greyscale image (also known as gray-scale, gray scale or gray-level) could be an information matrix whose values represent intensities inside some vary. MATLAB stores a greyscale image as a private matrix, with every part of the matrix like one image picture element. The matrix is often of sophistication uint8, uint16, int16, single, or double. Whereas greyscale images are seldom saved with a colour map, MATLAB uses a colour map. Following figure shows constituent Values during a Greyscale Image outline grey Levels.

Figure 3: Pixel Values in a Greyscale Image Define Gray Levels

Colour Images

A colour image is formed from pixels every of that holds 3 numbers cherish the red, green, and blue levels of the image at a specific location. Red, green, and blue (sometimes stated as RGB) are the first colours for commixture lightweight these thus known as additive primary colours are completely different from the reductive primary colours used for commixture paints (cyan, magenta, and yellow). Any color is often created by commixture the proper amounts of red, green, and blue lightweight. Presumptuous 256 levels for every primary, every colour constituent is often kept in 3 bytes (24 bits) of memory. This corresponds to roughly 16.7 million completely different attainable colours. Note that for images of an equivalent size, a black and white version can use thrice less memory than a colour version. A real colour image is an image within which every constituent is such by 3 values one every for the red, blue, and inexperienced parts of the pixel's colour.

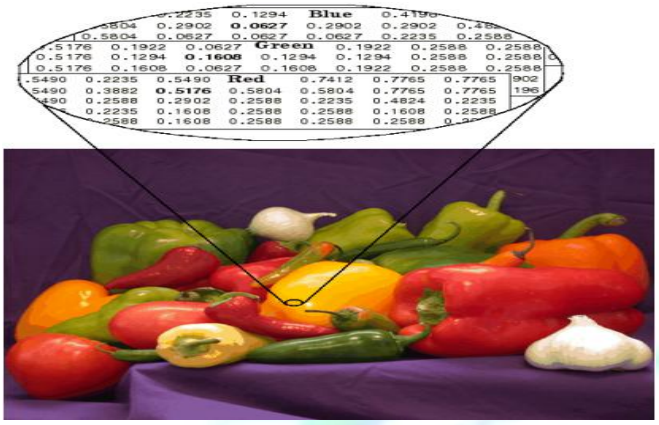

Figure 4: The colour Planes of a True colour Image

III. PROPOSED METHOD

The structure of proposed Visual Cryptography based data hiding method is divided into the three parts. Transmitter end, receiver end and communication channel. The flow charts of both end is also described in this chapter. First describe the transmitter end. The transmitter end is based on the encoder part. Second describe the communication channel describe and then receiver end.

3.1Transmitter end (Encoder Part)

Transmitter End , receiver End and communication channel. The flow charts of each side are additionally represented during this chapter. initial describe the transmitter end. The transmitter end relies on the encoder part .Second describe the communication channel and then describe the receiver end.

The transmitter end is that the necessary a part of the planned methodology. The transmitter end is additionally called an encoder part of the planned methodology. During this part we produce the Visual Cryptography 2 major components Master and slave.

- Secret data (SD)
- Visual Cryptography Image (VCI) – Master and slave
- Cover image (CI)

Secret Data (SD)

Secret information is that the information that we would like to protect. The standard of planned work relies on the secret data. Secret information is generated at the user side and embedded into the small image. Similar that secret information is obtained at the receiver end. There's completely different sort of secret information probable supported user end. Normally secret information is in binary type, images and additionally code primarily based information on the market. Figure 4.1 shows the key information in image type.

Figure 5 The Secret Data

3.2 Steps of Transmitter End

In this a part of presented methodology shows the steps of implementation of projected work. within the below shows the various steps of transmitter end and figure 4.6 shows the flow chart of Encoder end (Transmitter end)

First Step – In the stage take the information that want to cover (Hide) such as secret data, banking password and one time password etc. that's shown in figure 4.1 image.

Second Step – In the Second step produce a visible cryptograph images. Which are in the form of master and slave. Shown in figure 4.3.

Third Step – After the creation of VCI, which is combination of master and slave images, now add the secret VCI into the cover images. This cover image is select from data set. That's shown in Figure 4.5. Generation of SI with the assistance of random generation methodology. Stego Image (SI), currently choose the cover image from the information set and apply preprocessing task after this cover image selection. Within the preprocessing of the image, some basic image operation can perform within the chosen image like grey scale changing, image resizing

Fourth Step – Send this Stego to the receiver side. Which is send via unsecure communication channel.

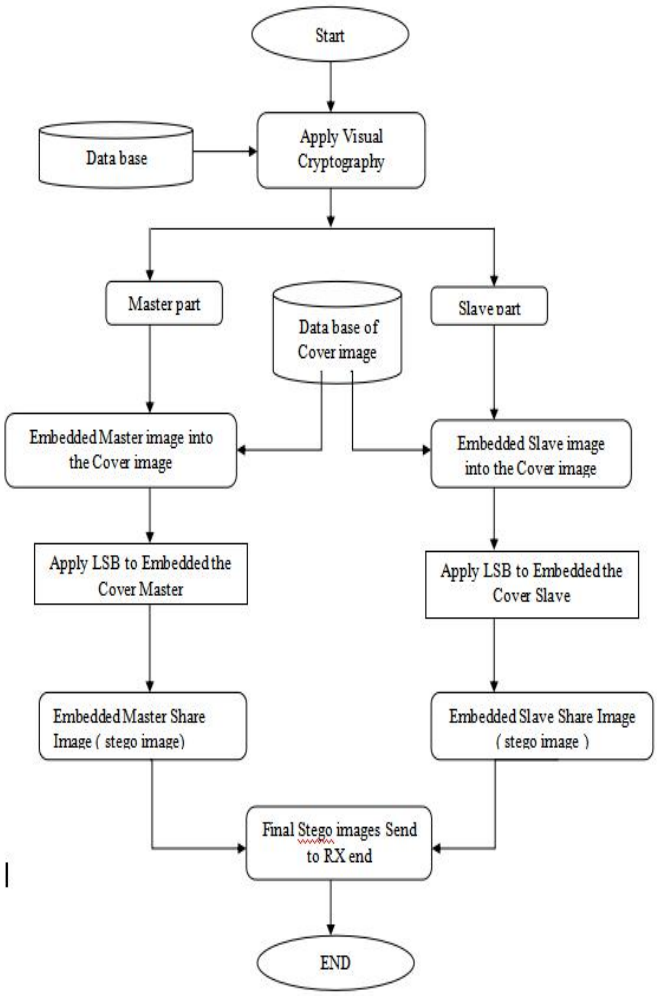

Figure 6 Flow diagram of steps of Encoder end

IV. SIMULATION AND RESULT

The result of our proposed method for data hiding of gray scale images shown in this section, simulation of our proposed method and result calculation. We have done our proposed work with the help the MATLAB R2012b software and simulate our whole proposed methodology. The performance of the proposed algorithm is tested for different gray scale images that is shown in below figure. Basic configuration of our system is: Processor: Intel (R) Quad Core (VM) i3–3110 Central Processing unit @, 2.40 GHz with 4GB RAM: System type: 64-bit Operating System. MATLAB based simulation result shows good PSNR value for stego image and better quality of stego image as compare to other method that is shown in table II. In the field of image data hiding, people normally have anxiety about the viscrtypro image. These criteria can be evaluated by PSNR in dB.

Mean Square Error (MSE): The MSE measures the standard amendment between the actual image (X) and the noised image (Y) and is given by:

$$\mathrm{MSE} = \frac{1}{N}\sum_{j=0}^{N-1}(X_j - Y_j)^2 \qquad 5.1$$

X_j Shows the cover image

Y_j Shows the stego image

The MSE has been extensively used to quantify image quality and once used alone; it doesn't correlate powerfully enough with sensory activity quality. It ought to be used, therefore in conjunction with alternative quality metrics and perception.

Peak Signal to Noise Ratio (PSNR): The PSNR is computed as:

$$\mathrm{PSNR} = 10\log_{10}\frac{s^2}{\mathrm{MSE}} \qquad 5.2$$

The PSNR is higher for an excellent worth image and lower for a poor quality image. It measures image fidelity, that is, however closely the distorted image resembles the actual image. In our research work on the basis of our image size 512x512.

First – Select the secret data in the form of image.

Fig .7 shows the different input images

Second – Select the secret image form different data set images.

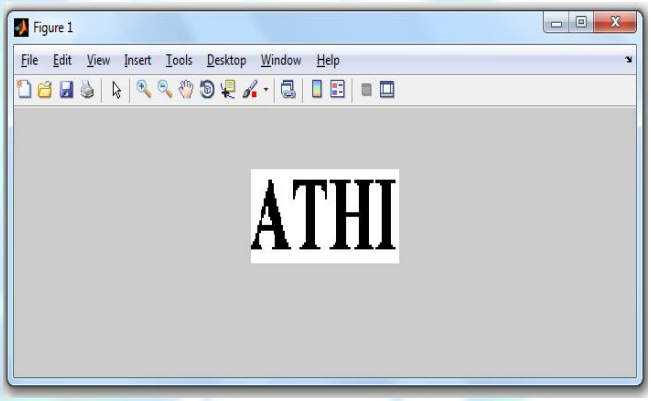

Fig. 8 Shows the input Secret image

Thired – After selection of the input image now convert in to master and slave that is shown in below figure.

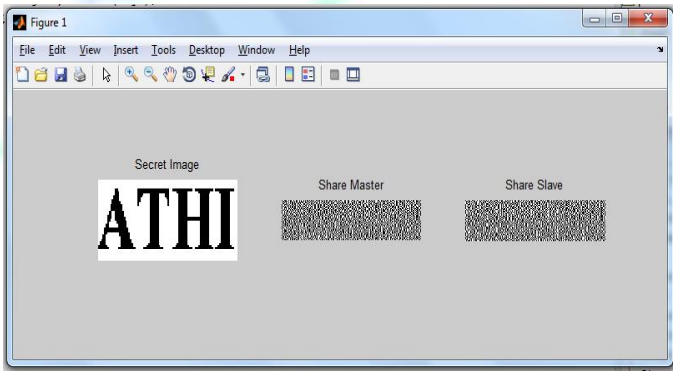

Fig.9 Master and Slave image

Fourth – Select cover image for sending the data. The result of secret image and cover image is also shown in the figure.

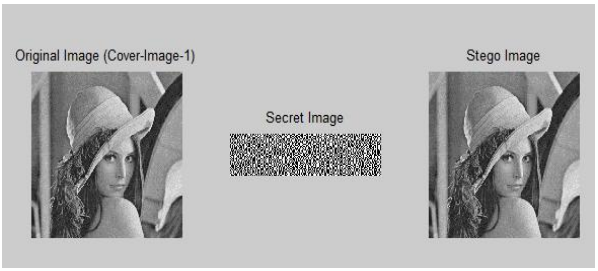

Fig. 10 Stego Image

Fifth – Send these master and slave image into the communication channel.

Fig.11 Shows the Receiver end received master and slave message

Fig.12 Retrived image

Now discuss the comparsionof result for different images using resultant parameters like PSNR and MSE. That is shown in below table 1.

Table 1. Comparison of result using different cover and secret images

Secret Image	Cover Image		Transmission End		Receiver End	
	Master Cover	Slave Cover	PSNR	MSE	PSNR	MSE
ATHI	Leena .jpg	Mandril .jpg	66.0837	0.016	35.40	18.75
			66.0837	0.016		
VIVEK	Leena .jpg	Mandril .jpg	66.1504	0.158	36.00	16.31
			66.1024	0.016		
1	Leena .jpg	Monkey .jpg	66.2588	0.0154	36.60	14.22
			66.2374	0.0155		
A	Lady . jpg	color Monkey .jpg	66.591	0.0143	35.75	17.29
			57.1854	0.1243		
twitter sing	zcover 360.jpg	vivekimage.jpg	55.5165	0.1826	34.72	21.89
			57.1687	0.1248		

In the above table shows the comparison of the result of the proposed method for different images.

Now compare the proposed method with previous method on the different resultant values. In this table compare the result on different attacks and is shown in below

Table 2 Robustness Test Results Against Attacks

Attacks	NCC Value	PSNR (dB)	PSNR (dB)
JPGE	1	33.13	35.31
Re-sizing	0.99	28.13	30.23
Median Filter	1	25.21	26.23
Histogram Equalization	1	19.22	22.23
Average Filter	0.99	25.77	26.43

V. CONCLUTION

In this research paper present a brand new method for data hiding in the image. The proposed method shows good result for different type of secret images in terms of qualitative and well as visual results. For calculation the performance of proposed method use peak signal to noise ratio (PSNR) and mean square error (MSE). The proposed method shows good results under the different attacks that is shown the table 1.2. In this paper discuss about data hiding based different techniques and finally discuss the visual cryptography based 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 improved the proposed method result 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.

REFERENCES

[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] B. Pushpa Devi1, Kh. Manglem Singh, Sudipta Roy, 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.

[9] Geum-Dal Park Dae-Soo Kim Kee-Young Yoo, "Lossless Codebook-Based Digital Watermarking Scheme with Authentication" 11th International Conference on Information Technology: New Generations, IEEE, 301-307, 2014.

[10] S. Rawat and B. Raman, "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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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

[19] Ching-Sheng Hsu and Young-Chang Hou, "A Visual Cryptography and Statistics Based Method for Ownership Identification of Digital Images", World Academy of Science, Engineering and Technology, vol., 172-175, 2005.

[20] Chin-Chen Chang and Jun-Chou Chuang "An image intellectual property protection scheme for gray level images using visual secret sharing strategy", Pattern Recognition Letters, vol. 23, pp. 931-941, 2002.

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

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

