ISSN:0975-9646

Data Hiding & Visual Cryptography:A Review

Deepti B. Khasbage[1], Prof. DR .P.R. Deshmukh[2]
[1]*Master of Engineering Scholar,Information Technology Department*
[1,2]*Sipna College of Engg and Technology*
Amravati, India

Abstract- **In this paper, We emphasize on how to improve capacity of image carrier by hiding text data using combine approach of visual cryptography with data hiding technique. And to fulfill this requirement, the proposed system highlights a novel approach of an Optimize Multiple Bits Replacement Scheme with Multi-Layer Multi-Shares Visual Cryptography for Data Hiding. The proposed system hides textual data in a image carrier and achieve its encryption/decryption after going through visual cryptography. The overall effort of the proposed scheme is the achievement of encrypting/extracting multiple secret images and reference images from sharing images at different scale levels. The main aim of the proposed model is to improve security, reliability and efficiency of secret message by the combine use of data hiding and visual cryptography method.**

Keywords- Visual Cryptography, Data Hiding, Multi-layer Multi-Shares, Data Security, Optimize

I. INTRODUCTION

Visual cryptography, degree associate rising cryptography technology, uses the characteristics of human vision to rewrite encrypted photos. Visual cryptography provides secured digital transmission that is utilized just for just the once. the initial photos ar typically utilize by pattern this theme. As a method of special secret sharing technology, it utterly was used for many participants to code a black-and-white image. the initial image is also blazing by stacking the shares on. Its security is up to a one time pad and anyone will use it for decipherment with none science information and any computations.

Numerous confidential data like military maps and business identifications are transmitted over the net. Whereas pattern secret photos, security problems ought to be taken into thought as a result of hackers could utilize weak link over communication network to steal data that they need .To touch upon the security problems with secret photos, varied image secret sharing schemes are developed.

Secret Sharing permits sharing secret data among a bunch of participants such secret writing is potential providing all the participants unit gift with their shares. Secret are divided into any choice shares. An area of secret data is termed a share. Whereas secret writing the data, it's needed to want all the shares on transparency then produce them in correct order. There unit varied secret sharing schemes.

Digital knowledge embedding in digital media is associate data technology field of speedily growing industrial, similarly as national security of interest. The transmission of digital transmission product via web is obtaining additional and additional in style. as a result of the digital medium will be handily transmitted and lossless derived, they additionally cause a rise of digital piracy to unravel this drawback, completely different data hiding techniques square measure used [1]-[4]. Covert communication or steganography, which accurately suggests that “covered writing” in Greek, is that the method of activity knowledge underneath a canopy medium (also spoken as host), like image, video, or audio, to ascertain secret communication between trusting parties and conceal the existence of embedded knowledge.

The main objective of knowledge concealing is to speak firmly in such the way that actuality message that is embedded in anyone of the digital media isn't visible to the observer. That unwanted parties shouldn't be able to distinguish in any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that contains secret message). so the stego-image shouldn't deviate abundant from the first cowl image. completely different information concealing techniques are often evaluated on following four basic attributes of information |of knowledge |of data concealing (i) payload - information delivery rate; (ii) strength - hidden data resistance to noise/disturbance; (iii) transparency - low host distortion for concealment purposes; and (iv) security-inability by unauthorized users to detect/access the communication.

Recently, developing information concealing technologies, notably within the sort of steganography, area unit seen to cause a threat to private privacy, industrial and national security interests [5]. The steganalysis is that the method to reveal the confidential message even sure unsure media. The step technology to steganography security is usually spoken as steganalysis, which might be classified into 2 categories: Passive and active. the first task of passive steganalysis is to come to a decision the presence or absence of hidden information in given media objects (binary hypothesis testing problem). Active steganalysis (also referred to as forensics steganalysis) refers to the hassle by unintended recipients to extract/remove/modify the particular hidden information.

II. LITERATURE SURVEY

Naor and Shamir proposed a “(k, n)-threshold visual secret sharing scheme” in the year 1994, which is now commonly referred to as Visual Cryptography(VC) [1]. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system. Thus no knowledge of cryptography is required when a user uses a system employing visual cryptography. Each share looks

like a collection of random pixels and appears meaningless by itself. The generated shares alone do not reveal anything about the secret image.

Until the year 1997 visual cryptography schemes were applied to solely black and white pictures. Initial colored visual cryptography theme was developed by Verheul and Van Tilborg [2]. Colored secret pictures may be shared with the idea of arcs to construct a colored visual cryptography theme. In c-colorful visual cryptography theme one picture element is reworked into m sub pixels, and every sub picture element is split into c color regions. In every sub picture element, there is specifically one color region colored, and every one the opposite color regions are black. The color of 1 picture element depends on the interrelations between the stacked sub pixels. For a colored visual cryptography theme with c colors, the picture element growth m is c× three.

For sharing a secret color image and additionally to generate the significant share to transmit secret color image Chang and Tsai [3] anticipated color visual cryptography theme. For a secret color image 2 important color pictures ar chosen as cowl pictures that are a similar size because the secret color image. Then in keeping with a predefined Color Index Table, the key color image are hidden into 2 camouflage pictures. One disadvantage of this theme is that further house is needed to accumulate the Color index table.

When extra colors are there within the secret image the larger the scale of shares will become. To beat this limitation, Chin-Chen Chang et al [4] developed a secret color image sharing theme supported changed visual cryptography. This theme provides a additional economical method to cover a gray image in totally different shares through out this theme, size of the shares is fixed; it does not vary once the amount of colors showing among the key image differs. Theme doesn't need any predefined Color Index Table.

For reducing pixel expansion in color visual cryptography scheme S. J. Shyu [5] advised a more efficient colored visual secret sharing scheme with pixel expansion of [log2c*m] where m is the pixel expansion of the exploited binary scheme. Du-Shiau Tsai et al [6] devised a secret image sharing scheme for true-color secret images. In the proposed scheme through combination of neural networks and variant visual secret sharing, the quality of the reconstructed secret image and camouflage images are visually the same as the corresponding original images.

Tzung-Her Chen et al [7] anticipated a multi-secrets visual cryptography that is extended from ancient visual secret sharing. The codebook of ancient visual secret sharing enforced to come up with share pictures macro block by macro block in such manner that multiple secret pictures are became solely 2 share pictures and decrypt all the secrets one by one by stacking 2 of share pictures during a way of shifting. This theme will be used for multiple binary, grey and color secret pictures with constituent growth of four. F. Zhengx in Fu, Bin Yu [8] planned a theme supported correlative matrices set and random permutation, a brand new construction of rotation visual cryptography theme (RVCS) has been bestowed, which might be accustomed encrypt four secret pictures into 2 shares. For extending this theme for color image, exploiting color decomposition with high distinction is required.

Shyong Jian Shyu, Hung-Wei Jiang [9] provide formal definitions to threshold multiple-secret visual scientific discipline schemes, particularly MVCS and MVCS, exploitation solely superimposition with none further operation in decipherment method. General constructions for each schemes are designed exploitation the talents of applied math within which the target functions are to reduce the constituent expansions with the constraints satisfying the revealing, concealing and security conditions within the corresponding definitions. For a given setting of k , n and s, which revealing list could manufacture the tiniest constituent expansion and how will a revealing list have an effect on the resultant constituent expansion are still challenges.

Shyong Jian Shyu [10] introduced two novel and effective VCRG-GAS algorithms to resolve the problem of visual secret sharing for binary and color images. In this paper the algorithms do not require any extra pixel expansion. The approach of VCRG relieves the concern of pixel expansion, yet its reconstruction ability is not flawless as VCS.

In order to reinforce the ability of the hidden secret information associate degreed to manufacture associate out of sight stego image quality H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang [11] has planned a very distinctive handwriting technique supported Least important Bit (LSB) Replacement and half worth Differencing (PVD) ways in which in 2005.Pixel value Differencing (PVD) technique is employed to discriminate between edge areas and sleek areas of canopy image. In Wu dialect and Tsai's steganographic technique, a grey-valued cowl image is split into non-overlapping blocks of 2 consecutive pixels, states pi and pi and pi+1.From every block we'll acquire a unique worth di by subtracting pi from pi+1. All realizable totally altogether totally different values of di vary from -255 to 255, then | di | ranges from zero to 255. Therefore, the half pi and pi+1 are placed at intervals the swish space once the worth | di | is smaller and would possibly hide less secret information. Otherwise, it's settled on the edged house and embeds plenty of knowledge.

The secret data is hidden into the smooth areas of cover image by LSB method while using the PVD method in the edge areas. As, this proposed method not only store data in the edge areas but also in the smooth areas; therefore it can hide much larger information and maintains a good visual quality of stego image.

In *2007 Hsien-Wen Tseng, Feng-Rong Wu*, and *Chi-Pin Hsieh* [12] has proposed a novel method for hiding data in binary images. The binary cover image is partitioned into equal-sized, non-overlapping blocks and the watermark will be embedded into blocks by flipping pixels. For security consideration, the watermark data is firstly permuted into a meaningless bit sequence by using a secret key. The cover image is partitioned into blocks of predefined size n x n and then each block can be embedded one secret bit except the completely black or white blocks. The embedding rule is based on the odd-even information in a block. A Weight mechanism is used to select the most suitable pixel for flipping. Additionally boundary check is performed to

improve the visual quality of stego image as well as to prevent boundary distortion. This method achieved a good visual quality for watermarked image and has high capacity of embedding.

In 2008 Beenish Mehboob and Rashid Aziz Faruqui [13] discussed the art and science of steganography generally and projected a unique technique to cover information in a very colourful image exploitation least vital bit. Least vital Bit or its variants are wont to hide information in digital image. Digital pictures are delineated in bits. The thought of fiddling with 0's and 1's appear quite straightforward however a small amendment in worth might remodel a picture fully in different words it distorts image fully. Thus this system chops the information in eight bits when the header and used LSB to cover data.

In 2012 Tasnuva Mahjabin,Syed Monowar Hossain and Md. Shariful Haque [14] has projected knowledge concealment technique supported PVD and LSB substitution to enhance the capability of the key data still on build steganalysis an advanced task they created a trial to implement a sturdy dynamic technique of knowledge concealment. associate economical associated dynamic embedding rule was projected here that not solely hides secret information with an inaudible visual quality and enhanced capability however additionally build code breaking an honest annoyance for the aggressor. This system used a dynamic technique of image information concealment supported LSB Substitution technique and constituent price Differencing method. The full method of choosing eight pixels block for a sixteen pixels region and therefore the embedding technique for every eight pixels block is completely different for various cowl pictures. That is, looking on the standard of the quilt image the embedding procedure takes this call in run time. This feature of this technique provides security of the hidden secret information. So as to extract the key information it's obligatory to understand that the quilt image is split into regions of sixteen pixels and additionally the kind of eight pixels block for these regions and kind of technique for every of those blocks. Moreover, if anybody becomes tuned in to the techniques that are accustomed insert information in one image, he cannot use a similar technique to alternative pictures.

Ankit Chaudhary And JaJdeep Vasavada [15] has planned an improved stenography approach for activity text messages in RGB lossless pictures in 2012.The security level is hyperbolic by willy-nilly distributing the text message over the whole image rather than clump inside specific image parts. the primary step towards the random distribution of the message in image is victimization indicator values. They used MSB bits of Red, inexperienced and Blue channel as constituent indicator values rather than utilizing a whole channel. The MSBs indicate in what sequence the message is hidden victimization the LSBs. Additionally to the present, this theme is applied once applying compression to the initial message; so it might be build it extraordinarily tough to interrupt, even once suspicion of the message inside a picture. The theme works as follows: The MSB remains unchanged once AN LSB of a computer memory unit is employed for storing a message. This theme allows US to completely utilize all the LSBs of each channel of the duvet image to store the hidden message and thus improve its capability. What is more the variable indicator values introduce a security facet because it becomes more and more tough to decipher the message though its presence is suspected. They hyperbolic storage capability by utilizing all the color channels for storing data and providing the supply text message compression. The degradation of the pictures is reduced by ever-changing only 1 lease vital bit per color channel for activity the message, acquisition a awfully very little amendment within the original image. So, this technique hyperbolic the safety level and improved the storage capability whereas acquisition borderline quality degradation.

Kousik Dasgupta & J.K. Mandaland, Paramartha Dutta [16] have planned a secured has primarily based LSB technique for video stenography in 2012.This technique utilizes cowl video files in abstraction domain to hide the presence of sensitive information notwithstanding its format. Video Steganography deals with concealment secret information or info inside a video. During this paper, a hash primarily based least important bit (LSB) technique has been planned. A abstraction domain technique wherever the key info is embedded within the LSB of the duvet frames. Eight bits of the key info is split into3, 3, two and embedded into the RGB component values of the duvet frames severally. As shown in following fig: 21

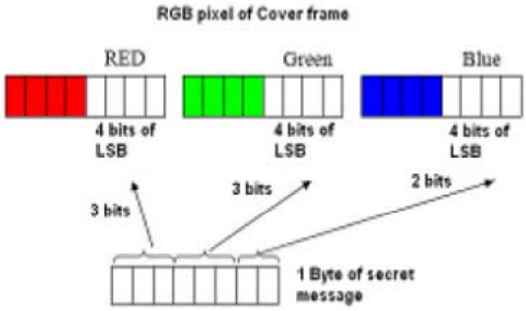

Figure: 2.1 shows secret information embedded in four bits of LSB in three, 3, two order in corresponding RGB pixels of carrier frame.

A hash perform is employed to pick out the position of insertion in LSB bits. The planned technique takes eight bits of secret information at a time and conceal them in LSB of RGB(Red, inexperienced and Blue) component price of the carrier frames in three, 3, two order severally. such out of eight (08) bits of message six (06) bits square measure inserted in R and G component and remaining 2 (02)bits square measure inserted in B component. When scrutiny the planned technique with LSB technique it's found that the performance analysis of planned technique is sort of encouraging. The advantage of this methodology is that the dimensions of the message doesn't matter in video stenography because the message are often embedded in multiple frames.

In 2012 Poonam V Bodhak and baiza L Gunjal [17] has projected a way to cover knowledge containing text in pc video file and to retrieve the hidden info. this may be designed by embedding the computer file in an exceedingly video move into such the way that the video doesn't lose its practicality victimisation DCT & LSB Modification

technique. LSB is that the lowest bit in an exceedingly series of numbers in binary. The LSB based mostly Steganography is one in all the steganographic ways, accustomed imbed the key knowledge in to the smallest amount vital bits of the picture element values in an exceedingly cowl image. DCT coefficients are used for JPEG compression. It separates the image into elements of differing importance. It transforms an indication or image from the spacial domain to the frequency domain. It will separate the image into high, middle and low frequency elements.

This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

CONCLUSION

In this paper, various data hiding schemes are studied and also visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated.

Sr. no	Author name	year	No. of secret images	Pixel Expansion	Image format	Type of Share Generated
1	Naor and Shamir	1995	1	4	Binary	Random
2	Verheul and Van Tilborg [2].	1997	1	C*3	Binary	Random
3	Chang and Tsai [3]	2000	1	529	color	Random
4	Chin-Chen Chang et al [4]	2005	1	4	Binary	Meaningful
5	S. J. Shyu [5]	2006	1	[log c*m]	color	Random
6	Du-Shiau Tsai et al [6]	2009	1	9	color	Meanin-gful
7	Tzung-Her Chen et al [7]	2008	2	1	Binary	Random

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography,"Advances in Cryptology - EUROCRYPT'94, pp. 1-12, 1995.
2. E.Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes And Cryptography, 11(2) , pp.179–196, 1997
3. C. Chang, C. Tsai, and T. Chen. " A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.
4. Chin-Chen Chang , Tai-Xing Yu , "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.
5. S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K.Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651,2007
6. Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 20096.
7. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.
8. Zhengxin Fu, Bin Yu, "Research On Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, pp 533-536, 2009.
9. Shyong Jian Shyu, Hung-Wei Jiang: General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes. IEEE Transactions on Information Forensics and Security 8 733-743 (2013)
10. S.J. Shyu, "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39 (5) , 866–880, 2006.
11. H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEEE Proc.-Vis. Image Signal Process.*, Vol. 152, No. 5,October 2005.
12. Hsien-Wen Tseng, Feng-Rong Wu,and Chi-Pin Hsieh," Data Hiding for Binary Images Using Weight Mechanism" ,*IEEE* 2007.
13. Beenish Mehboob and Rashid Aziz Faruqui," A Stegnography Implementation", *IEEE* 2008
14. Tasnuva Mahjabin, Syed Monowar Hossain, Md Shariful Haque," A Block Based Data Hiding Methoin in Images Using Pixel Value Differencing and LSB Substitution Method", *IEEE* 2012.
15. Ankit Chaudhary, JaJdeep Vasavada,"A Hash Based Approach For Secure Keyless Image Steganography in Lossless RGB Images" , *IEEE* 2012.
16. Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta3," HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEOSTEGANOGRAPHY (HLSB)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 2, April 2012.
17. Poonam V Bodhak, Baisa L Gunjal," Improved Protection In Video Steganography Using DCT & LSB", *International Journal Of Engineering and Innovative Technology (IJEIT)* Volume 1, Issue 4,April 2012.