An Advanced Image Visual Cryptography By Multilevel Decomposition For Data Hiding

Miss. Pradnya S. Nagdive
Master of Engineering
Computer Science and Information Technology Department.
H.V.P.M. College of Engg. Amravati, India

Prof. Anjali. B. Raut
Head of CSE Department
Computer Science and Engineering Department.
H.V.P.M. College of Engg. Amravati, India

***Abstract*— To maintain the privacy and certainty of pictures is a spirited area of research, with two totally different approaches being followed, the first approach is encrypting the pictures through encoding algorithms using keys and the secondary approach is hiding the data using data hiding algorithms to take care of the pictures secrecy. A content owner encrypts the original image by using an encoding key, and an information-hider can embed further data into the encrypted image employing a data-hiding key although he doesn't recognize the original content. With an encrypted image containing further data, a receiver could initially decode it with the encoding key, then extract the embedded information and recover the original image with the data-hiding key.**

In this paper, we proposed a novel technique that is the combination of Visual Cryptography and Steganography. As the combination of Visual cryptography and Steganography is used, so this technique provides benefits of both methods.

***Index Terms*— Visual Cryptography, Steganography, Information Concealing, Information Extraction, Image Encryption, Image Decryption.**

I. INTRODUCTION

The security of data is presently one in each of the foremost pressing issues thereto many researchers have paid lots of attention. To attain security, two techniques are most generally used. These techniques are none other than the Cryptography and Steganography.

Cryptography may be a well method for securing the key information. Sender encrypts the message with the assistance of key then sends it to the receiver. The receiver decrypts the message to get the non-public information. Cryptography focuses on keeping the content of the message secret.

Steganography is the practice of concealing info "in plain sight". This method depends on a message being encoded and hidden during a transport layer in such a way as to create the existence of the message unknown to an observer. Significantly, the transport layer – the carrier file - isn't secret and may thus be viewed by observers from whom the key message itself ought to be hide. The facility of steganography is in concealing the key message by obscurity, concealmentits existence within a non-secret. Whereas info concealing(also known as as steganography) concentrates on keeping the existence of the message secret. The word steganography combines the traditional Greek words steganos which means "covered, concealed, or protected", and graphein which means "writing". Information Concealing is another technique for secured communication. Information Concealing involves concealment the information so it appears that no data is hidden. If a person or many persons views the item among that the data is hidden then he or she is going to don't have any concept there's any hidden information, that's why the person won't conceive to decode the data. Information Concealing is that the method of concealment a secret message among cowl medium such as image, video, text, audio. Hidden image has several applications, particularly in today's modern, hi-tech world. Privacy and secrecy could be a concern for many folks on the net. Hidden image permits for two parties to speak in secret and covertly.

The strength of information concealment gets amplified if it combines with cryptography. The terminologies employed in information concealing are cover-image, hidden image, secret message, secret key and embedding algorithm. Cover-image is that the carrier of the message like image, video or audio file. Cover-image carrying the embedded secret information is that the hidden image. Secret message is that the info that's to be hidden within a cowl image. The secret key is used for embedding the message depending on hiding algorithm. The embedding formula is that the approach, thatis employed to infix the secret info within the cowl image.

The security of the transformation of hidden information will be obtained by two ways: secret writing and data concealing. A mixture of these two techniques will be accustomed increase the info security. In cryptography, the message is altered in such a way that no information will be disclosed if

ISSN: 2278 – 7798

it's received by an intruder. Whereas in info concealing, the secret message is embedded into a picture typically known as cowl image, so sent to the receiver who extracts the key message from the quilt image. Once the key message is embedded into cowl image then it's known as a hidden image. The visibility of this image mustn't be distinguishable from the quilt image, in order that it nearly becomes not possible for an intruder to get any embedded message.

II. LITERATURE SURVEY

Tung-Hsiang Liu and Long-Wen Chang [1] have proposed a simple data hiding technique for binary images in 2004.The proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes. Therefore, data is stored in the edge portion of binary image; as the modification of edge pixels is more difficult to be recognized by human eyes. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality.

In order to improve the capacity of the hidden secret data and to provide am imperceptible stego image quality H. C. Wu, N. I. Wu, C. S. Tsai and M. S. Hwang [2] have proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods in 2005.Pixel Value Differencing (PVD) method is used to discriminate between edge areas and smooth areas of cover image. In Wu and Tsai's steganographic method, a grey-valued cover image is partitioned into non- overlapping blocks of two consecutive pixels, states pi and pi and pi+1.From each block we can obtain a different value di by subtracting pi from pi+1. All possible different values of di range from -255 to 255, then $|di|$ ranges from 0 to 255. Therefore, the pixel pi and pi+1 are located within the smooth area when the value $|di|$ is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. From the aspect of human vision it has a larger tolerance that embeds more data into edge areas than smooth areas. 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 2005 M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco & A. Neri [3] have proposed a no-reference video quality metric that blindly estimates the quality of a video. They had used Block based Spread Spectrum embedding method to insert a fragile mark into perceptually important areas of the video frames. They used a set of perceptual features to characterize the perceptual importance of a region that are Motion, Contrast and Color. The mark is extracted from the perceptually important areas of the decoded video on receiver side. Then a quality measure of the video is obtained by computing the degradation of the extracted mark. So, in this way quality of a compressed video is estimated by using simple embedding system on perceptually important areas of the video frame.

In 2007 Hsien-Wen Tseng, Feng-Rong Wu, and Chi-Pin Hsieh [4] have 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 [5]discussedthe art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. Digital Images are represented in bits. The idea of playing with 0's and 1's seem quite simple but a slight change in value may transform an image completely ,in other words it distorts image completely. Therefore this technique chops the data in 8 bits after the header and used LSB to hide data. So, they proved LSB method is the most recommended for hiding data than other techniques which require masking and filtering.

M.B. Ould Medeniand & El Mamoun Souidi [6] have proposed a novel stenographic method for gray level images on four pixel differencing and LSB substitution in 2010. The proposed approach works by dividing the cover into blocks of equal sizes and split each pixel into two parts .Then it counts number of one's in most part and embeds the secret message in the least part according to the corresponding number of bits in most part. As shown in following fig. 2.1

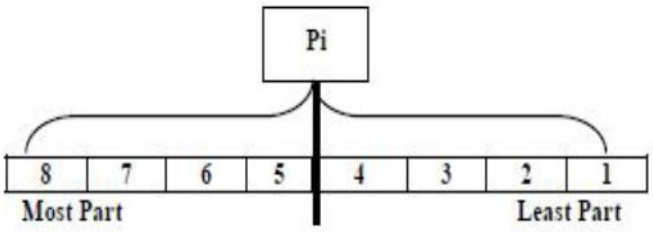


Figure 2.1: Split Process

$number-1-(MSB)$	$number-to-embeded$
$4or3$	$3bits$
2	$2bits$
$1or0$	1

Table: 2.1 number of 1 and the corresponding number of bits to embed

ISSN: 2278 – 7798

Therefore, it embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. They used K-bit LSB substitution method for hiding the secret data into each pixel where K is decided by the number of one in the most part of pixel. This method gave best values for the PSNR measure which means that there were no big difference between the original and the stegno image.

In 2012 Tasnuva Mahjabin,Syed Monowar Hossain and Md. Shariful Haque [7] have proposed a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This method achieved an increased embedding capacity and lower image degradation with improved security as compared to LSB substitution method and some other existing methods of data hiding. This system used a dynamic method of image data hiding based on LSB Substitution method and Pixel Value Differencing method. The whole process of selecting eight pixels block for a sixteen pixels region and the embedding method for each eight pixels block is different for different cover images. That is, depending on the quality of the cover image the embedding procedure takes this decision in run time. This feature of this method provides security of the hidden secret data. In order to extract the secret data it is mandatory to know that the cover image is divided into regions of sixteen pixels and also the type of eight pixels block for these regions and type of method for each of these blocks. Moreover, if any one becomes aware of the techniques that have been used to insert data in one image, he cannot use the same technique to other images. For example, depending on the quality of the cover image the embedding technique can select horizontal block for inserting data in the first sixteen pixels region for one image whereas vertical eight pixels block for the other image. Thus the decision for steganalysis becomes difficult and this method becomes a secure one.

Ankit Chaudhary and JaJdeep Vasavada [8] have proposed an improved stenography approach for hiding text messages in RGB lossless images in 2012.The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. The first step towards the random distribution of the message in image is using indicator values. They used MSB bits of Red, Green and Blue channel as pixel indicator values instead of utilizing an entire channel. The MSBs indicate in what sequence the message is hidden using the LSBs. In addition to this, this scheme is applied after applying compression to the original message; therefore it would be make it extremely difficult to break, even after suspicion of the message within an image. The scheme works as follows: The MSB remains unchanged when an LSB of a byte is utilized for storing a message. This scheme enables us to fully utilize all the LSBs of every channel of the cover image to store the hidden message and hence improve its capacity. Moreover the varying indicator values introduce a security aspect as it becomes increasingly difficult to decode the message even if its presence is suspected. They increased storage capacity by utilizing all the color channels for storing information and providing the source text message compression. The degradation of the images can be minimized by changing only one lease significant bitper color channel for hiding the message, incurring avery little change in the original image. So, this method increased the security level and improved the storage capacity while incurring minimal quality degradation.

Kousik Dasgupta & J.K. MandalandParamartha Dutta [9] have proposed a secured hash based LSB technique for video stenography in 2012.This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Video Steganography deals with hiding secret data or information within a video. In this paper, a hash based least significant bit (LSB) technique has been proposed. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3, 3, 2 and embedded into the RGB pixel values of the cover frames respectively. As shown in following fig: 2.2

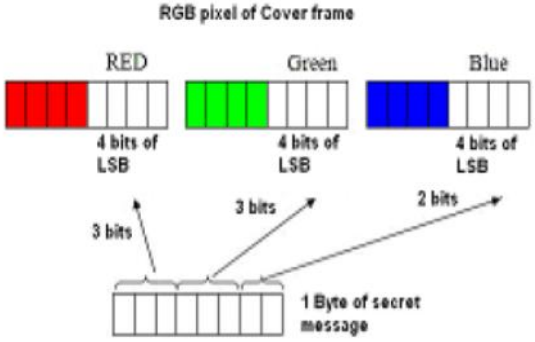


Figure: 2.2 shows secret data embedded in 4 bits of LSB in 3, 3, 2 order in corresponding RGB pixels of carrier frame

A hash function is used to select the position of insertion in LSB bits. The proposed technique takes eight bits of secret data at a time and conceal them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order respectively. Such that out of eight (08) bits of message six (06) bits are inserted in R and G pixel and remaining two (02) bits are inserted in B pixel. After comparing the proposed technique with LSB technique it is found that the performance analysis of proposed technique is quite encouraging. The advantage of this method is that the size of the message does not matter in video stenography as the message can be embedded in multiple frames.

In 2012 Poonam V Bodhak and Baisa L Gunjal [10] have proposed a method to hide data containing text in computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. LSB is the lowest bit in a series of numbers in binary. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image.

ISSN: 2278 – 7798

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

RigDas and Themrichon Tuithung [11] have proposed novel technique for image stenography based on Huffman Encoding in 2012. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. This paper presents a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. As shown in fig: 2.3

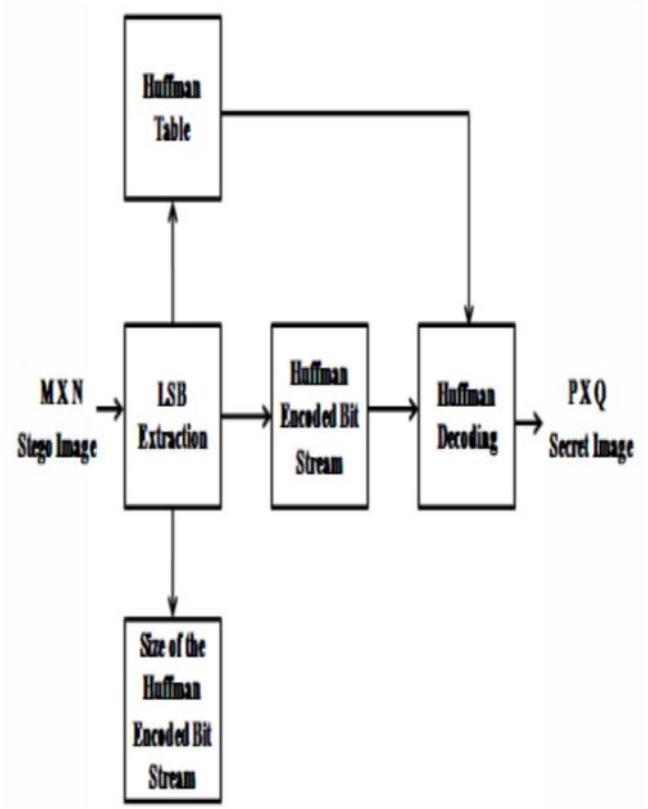


Figure: 2.3 Insertion of the Secret Image/Message into a Cover Image

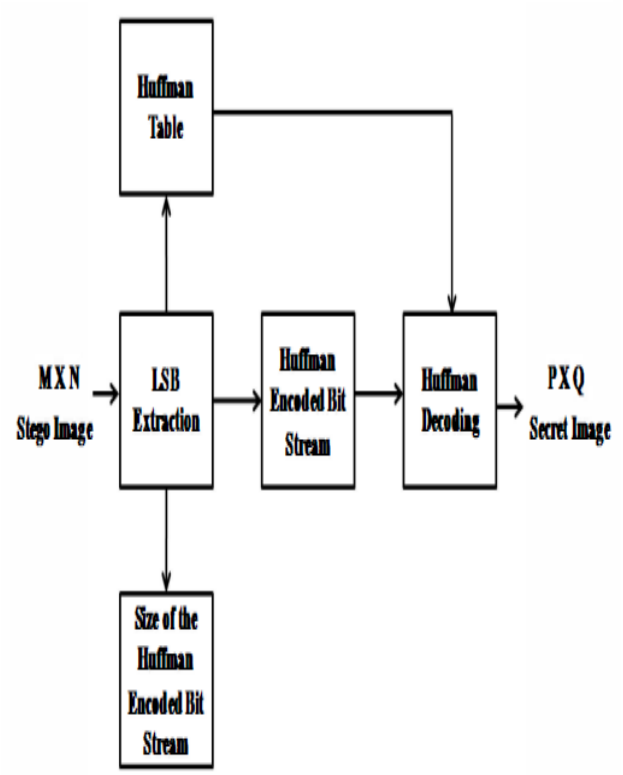


Figure: 2.4 Extraction of the Secret Image from the Stego Image

Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

In *2013 Ming Li,Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama,* and *Michael J. Medley* [12] have considered the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video).We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

In 2013, Yi-Chong Zeng and Chi Hung Tsai [13] have proposed multiscale image sharing scheme to hide multiple images to two meaningful sharing images. The proposed method combines conventional 2-out of-2 visual cryptography with data hiding technique. The overall effort of the proposed scheme is the achievement of decrypting or extracting multiple secret images and reference images from sharing images at different scale levels. It is not only applied to monochromatic images but also color Halftone images.

III. PROPOSED METHODOLOGY

In the proposed method, we used two algorithms

A. Data Hiding

B. Data Extraction

ISSN: 2278 – 7798

Data Hiding Algorithm is used for hiding data in the image. For hiding data, 5 bits(LSB) out of 8 bits of each R, G, B channel are used. Overall we used 15 bits out of 24 bits(ie. 1 pixel) for data hiding.

Data Extraction Algorithm is used for extracting data from the image .For extracting data the key by using which we hide data must be required because without key we can't extract data from the image.

A. Data Hiding

1. Select an Image
2. Split an Image into segments.
3. Select an image segments.
4. Select Secrete data for hiding.
5. Encrypt data with Shifting method
6. Split data into segments.
7. Apply Higher LSB Method for replacing pixels bits with encrypted data bits by taking one image segment & secret data segment.
8. Repeat Step 3 & Step 7 until all encrypted data segments are not hidden within image segment.
9. Generate and select key OR Add own key
10. Encrypt image segments.
11. Join Segments (Level 2)
12. Join Segments (Level 1)
13. Join Segments (Level 0)
14. Stop

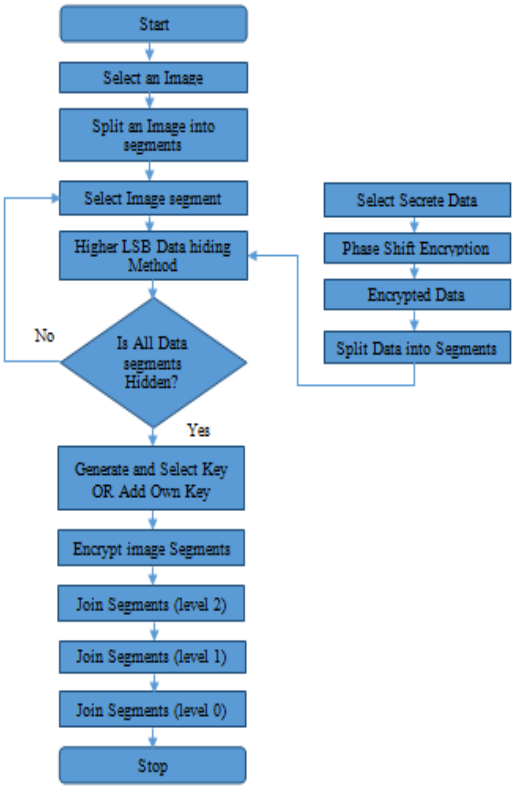


Fig.1 Data Flow diagram of Data Hiding

B. Data Extraction

1. Select a Stego Image.
2. Split stego Image.
3. Generate and Select Key OR Use Previous Key
4. Decrypt Image Segments
5. Apply Higher LSB Extraction algorithm.
6. Extract data bits from 1 to 5 LSB color pixels bits using Stego Key.
7. Decrypt Data using Phase Shift Decryption
8. Assemble Data.
9. Stop

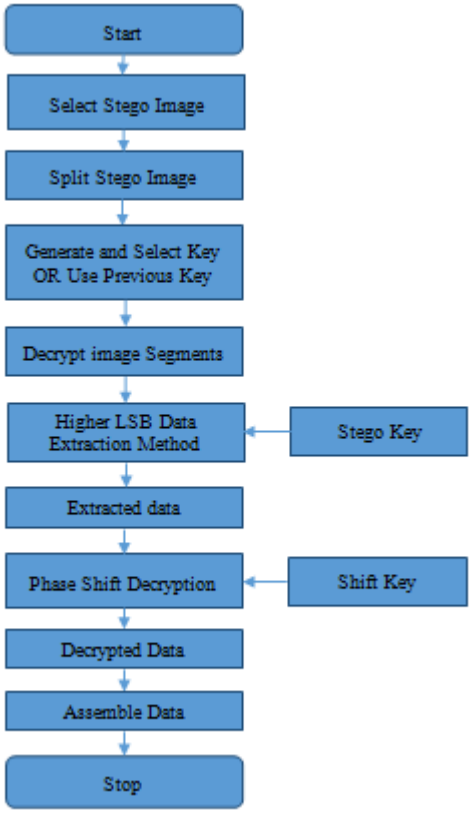


Fig. 2 Data Flow diagram of Data Extraction

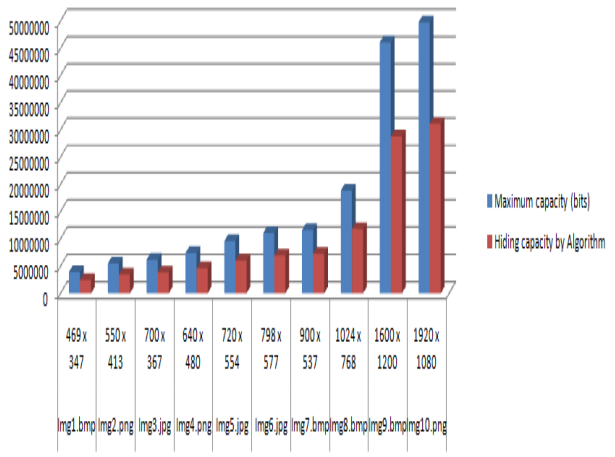
IV. RESULT ANALYSIS

Image Name	Image Size	Maximum capacity (bits)	Hiding capacity by Algorithm
Img1.bmp	469 x 347	3905832	2441145
Img2.png	550 x 413	5451600	3407250
Img3.jpg	700 x 367	6165600	3853500
Img4.png	640 x 480	7372800	4608000
Img5.jpg	720 x 554	9573120	5983200
Img6.jpg	798 x 577	11050704	6906690
Img7.bmp	900 x 537	11599200	7249500
Img8.bmp	1024 x 768	18874368	11796480
Img9.bmp	1600 x 1200	46080000	28800000
Img10.png	1920 x 1080	49766400	31104000

Table I Comparison of Maximum Capacity & Hiding Capacity of Different Images

This table shows the maximum capacity as well as hiding capacity by using algorithm of different types of images such as .jpg, .bmp, .png etc.

ISSN: 2278 – 7798



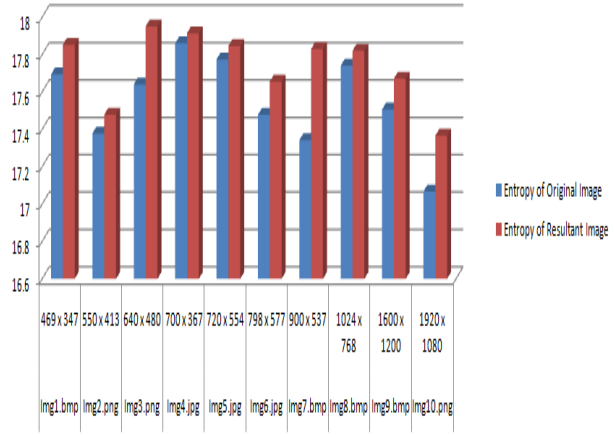
Graph I Relation between maximum and hiding capacity of different images

Above graph shows relation between maximum capacity and hiding capacity by using algorithm of different types of images.

Image Name	Image Size	Entropy of Original Image	Entropy of Resultant Image
Img1.bmp	469 x 347	17.694	17.8527
Img2.png	550 x 413	17.3783	17.4785
Img3.png	640 x 480	17.6409	17.951
Img4.jpg	700 x 367	17.8605	17.9145
Img5.jpg	720 x 554	17.7744	17.8456
Img6.jpg	798 x 577	17.4777	17.6555
Img7.bmp	900 x 537	17.342	17.8305
Img8.bmp	1024 x 768	17.7402	17.8206
Img9.bmp	1600 x 1200	17.5065	17.6718
Img10.png	1920 x 1080	17.0678	17.3657

Table II Comparison of Entropy of Original Image & Resultant Image

This table shows the Entropy of Original and Resultant image. Resultant image is nothing but the Original image containing hidden data.



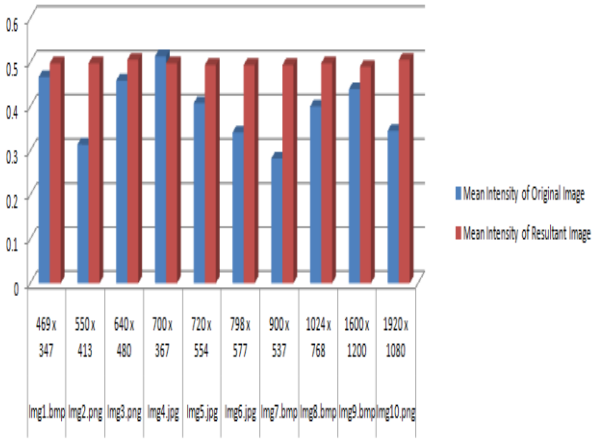
Graph II Relation between Entropy of Original Image & Resultant Image

This graph shows the relation between Entropy of Original Image and Resultant Image

Image Name	Image Size	Mean Intensity of Original Image	Mean Intensity of Resultant Image
Img1.bmp	469 x 347	0.46667	0.49804
Img2.png	550 x 413	0.31373	0.49804
Img3.png	640 x 480	0.45882	0.50588
Img4.jpg	700 x 367	0.51373	0.49804
Img5.jpg	720 x 554	0.40784	0.49412
Img6.jpg	798 x 577	0.34118	0.49412
Img7.bmp	900 x 537	0.28235	0.49412
Img8.bmp	1024 x 768	0.4	0.49804
Img9.bmp	1600 x 1200	0.43922	0.4902
Img10.png	1920 x 1080	0.3451	0.50588

Table III Comparison of Mean Intensity of Original image & Resultant image

Above table shows the Mean Intensity of Original Image and Resultant Image.



Graph III Relation between Mean Intensity of Original image & Resultant image

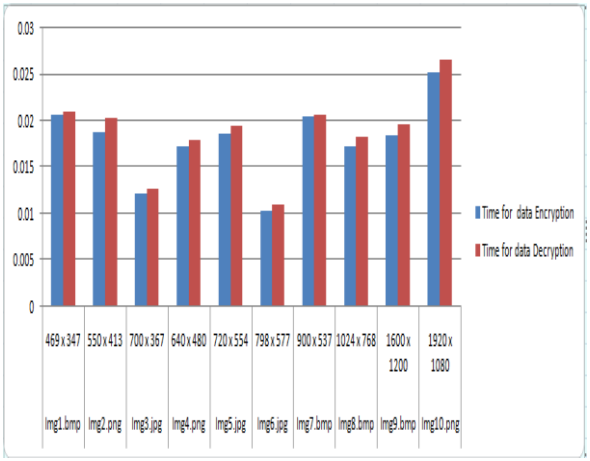
This graph shows the Mean Intensity of Original image and Resultant Image.

Image Name	Image Size	Time for data Encryption	Time for data Decryption
Img1.bmp	469 x 347	0.041976	0.0206551
Img2.png	550 x 413	0.018894	0.0204027
Img3.jpg	700 x 367	0.012137	0.0126767
Img4.png	640 x 480	0.030223	0.0178937
Img5.jpg	720 x 554	0.018681	0.0195636
Img6.jpg	798 x 577	0.010371	0.0110994
Img7.bmp	900 x 537	0.041439	0.0206901
Img8.bmp	1024 x 768	0.018298	0.0172508
Img9.bmp	1600 x 1200	0.018421	0.0196975
Img10.png	1920 x 1080	0.025286	0.0266696

Table IV Comparison of Time required for Data Encryption & Data Decryption

ISSN: 2278 – 7798

This table shows the time required for Encrypting and decrypting hidden data.



Graph IV Relation between Time required for Data Encryption & Data Decryption

This graph shows the relation between time required for data encryption and data decryption.

V. CONCLUSION

In this way, we have proposed a new method by using the combination of visual cryptography and steganography. In this method, if hacker has got the image in which data is hidden, he can't recognize the presence of message in the image due to steganography and if in case he recognized that message is present in the image, he can't retrieve the message because different keys known to only owner are used to hide different parts of message and also that message is convert into an another form that is not understandable to hacker, this is done by using visual cryptography.

ACKNOWLEDGMENT

I would like to thank my guide for motivating me to do research in this domain and also guiding me in proper way.

REFERENCES

[1] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04) 2004.J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 1959.

[2] 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", IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[3] M. Carli , M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri, "QUALITY ASSESSMENT USING DATA HIDING ON PERCEPTUALLY IMPORTANT" *IEEE* AREAS0-7803-9134-9/05/$20.00 ©2005.

[4] Hsien-Wen Tseng, Feng-Rong Wu,and Chi-Pin Hsieh," Data Hiding for Binary Images Using Weight Mechanism",*IEEE* 2007.

[5] Beenish Mehboob and Rashid Aziz Faruqui," A StegnographyImplementation", *IEEE* 2008

[6] M.B. Ould MEDENI, El Mamoun SOUIDI," A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "*IEEE* 2010

[7] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque," A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", *IEEE* 2012.

[8] Ankit Chaudhary, JaJdeep Vasavada,"A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGBImages" , *IEEE* 2012.

[9] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta3," HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY (HLSB)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 2, April 2012.

[10] 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.

[11] RigDas, Themrichon Tuithung," A Novel Steganography Method for Image Based on Huffman Encoding", *IEEE* 2012.

[12] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley*,"* Extracting Spread-Spectrum Hidden Data From Digital Media", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 8, NO. 7, JULY 2013.

[13] Yi-Chong Zeng and Chi Hung Tsai, "HIGH CAPACITY MULTI-SCALE IMAGE SHARING SCHEME BY COMBINING VISUAL CRYPTOGRAPHY WITH DATA HIDING " IEEE 2013

ISSN: 2278 – 7798