ISSN:0975-9646

Secret Information Transmission within Color Image using Wavelet Transformation

Gourav Tiwari
Student, M.Tech
CSE, VNSIT Bhopal

Rameshwar Nath Pathak
Computer Science and
Engineering, VNSIT Bhopal

Abstract-Steganography is art of hiding data in some cover medium, called as cover image. A typical carrier image can be used with color components such as red, green and blue in a multi bit data structure. There are different types of steganography techniques which are proposed in the literature. DWT based steganography technique is proposed in this work with the color image in multi bit plane for hiding the data in three different planes ie R plane, G plane and B plane. At the sender side, an owner of content encrypts the original uncompressed image using advanced Hill Cipher Algorithm then the data hider may hide the data inside the encrypted image. Due to security concerns, at the receiver side, the receiver can extract data from the stego image even the receiver has no information about the original contents of the image. Using the decryption key, the receiver can extract image similar to the original but cannot extract the additional secret data. If the receiver has both keys ie data hiding keys and encryption keys, the receiver can extract the additional data and the original image without any loss. In this proposed system data hiding in encrypted image using DWT for color image has been implemented.

Keywords Hiding, Cipher, Encryption, Decryption, Plane.

1.1 INTRODUCTION

In this paper Due to the rapid increase in network bandwidth, the Internet becomes a popular channel for transmitting different types of data like text, image, audio,video in digital form. Nevertheless, the more data to be transmitted over the Internet, the more security attack will be appeared from eavesdropping, data exposure and data tampering. Therefore, how to protect the secret data during transmission becomes an important issue. A common approach to provide the secure environment for important data transmission is the use of cryptographic techniques. Cryptography is about utilizing a particular cipher algorithm to transforming the secret messages into unrecognizable form so that only the intended receivers can recover the original messages using a cryptographic key. For the grabbers, who do not have a key, the encrypted messages will only look like a stream of meaningless codes. Although it is a good way to guard important data against illegal access while transmitting data, the use of cryptographic techniques still has a weakness. The transformed messages may attract the eavesdroppers attention. In order to overcome the weakness of cryptography, Steganography techniques are proposed to camouflage the existence of the hidden data. In Steganography, the secret messages are embedded into another meaningful and innocuous cover media, for example, text, image, audio and video, such that an unintended observer will not aware of the existence of the secret messages. Unlike the goal of cryptography, which attempts to conceal the content of data by transforming the secret data into messy and meaningless bit-streams, the aim of Steganography is to conceal the very existence of the secret data. Steganography, as derived from the Greek language, means ‘covered writing’, is not a new technology. A multitude of methods and variations has been used to protect the secret information throughout history. The use of invisible inks, which is another common form of invisible writing, has much success in both World War I and World War II. The secret message was written using materials, such as, milk, vinegar, fruit juices and urine, which will invisible at a later time. When heated or reacted to certain chemical, the hidden message can then be shown out. More examples can be found in for the historical Steganography. In general, Steganography techniques can be classified into two categories, Digital watermarking and data hiding according to the type of applications to which the techniques are applied. Digital watermarking is about ensuring the copyright or ownership of the digital data by embedding a distinguishable symbol.

1.2 Cryptography

The word cryptography comes from the Greek words hidden or secret and writing. Oddly enough, cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of untangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. This kind of cryptography can provide other services, such as

•Integrity Checking: Reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source.

•Authentication: Verifying someone’s (or something’s) identity But back to the traditional use of cryptography.

A message in its original form is known as plaintext or clear text. The distorted information is known as cipher text. The process for producing cipher text from plaintext is known as encryption.

1.3 Digital Watermarking

Digital watermarking technology is now drawing the attention as a new method of protecting copyrights for digital images. It is realized by embedding data that is insensible for the human visual system. The embedded information data is called watermark. So watermarking in digital images is the process by which a discrete data stream is hidden within an image imposing imperceptible changes of the image. The root of watermarking as an information hiding technique can be traced in ancient Greece as Steganography. The application of watermarking ranges from copyright protection, file tracking and monitoring. one of a main classification structures of watermarking techniques. This is shown in Figure: 1.2. From this classification, there are two types of watermarks, the visible ones, like different logos either on paper or on a TV screen and the most important one, the invisible or transparent watermarks, which cannot be perceived by the human sensory system. An invisible watermark can be either robust or fragile. The use of a fragile watermark is important when one wants to verity if the protected media was tampered with or not. The type of watermark is especially designed to be as fragile as possible, so even the slightest modification of the marked media will destroy it, indicating that someone tampered with the media in question. This type of watermark is like a CRC (cyclic redundancy code). On the other hand, robust watermarking is designed to provide proof of ownership of the media in question. Recently, it is used as one of the means of Digital Right Management. A watermarking system conceals information inside some other data. There are three criteria that can be used to measure the performance of a watermarking system. They are Embedding Effectiveness, Fidelity and Data payload, different application has different preferences based on its nature and requirements. We define embedding effectiveness of a watermarked work as a work that when input to a detector results in a positive detection. With this definition of watermarked works, the effectiveness of a watermarking system is the probability that the output of the sender will be watermarked. In other words, the effectiveness is the probability of detection immediately after embedding. This definition implies that a watermarking system might have an effectiveness of less than 100%.

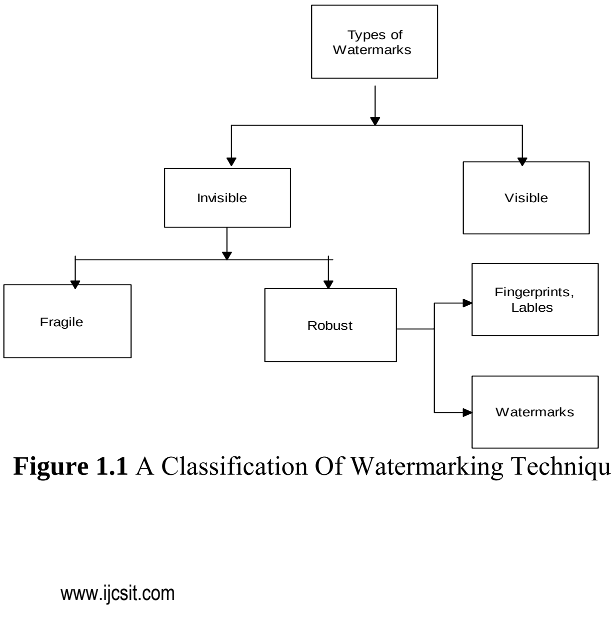

Figure 1.1 A Classification Of Watermarking Techniques

1.4 IMAGE FORMATS SUPPORTED BY THIS SYSTEM

The following image formats are supported by the proposed system:

- PNG(Portable Network Graphics)
- JPG (Joint Photographic Expert Group)
- BMP(Windows Bitmap Picture)
- TIFF(Tagged Image File Format)

Most images we catch on the Internet are Joint Photographic Expert Group (JPEG) images which is the name for one of the most widely used compression standards for images. If you have kept an image you can usually see from the suffix what format it is stored in. For example, an image named abc.jpg is stored in the JPEG format. The other class is called uint8 which assigns an integer between 0 and 255 to represent the brightness or color of a pixel. The value 0 corresponds to black and 255 to white. The class uint8 only requires around 1/8 of the storage compared to the class double. On the other hand, several mathematical functions can only be applied to the double class.

2. Previous Work

A joint encryption and reversible data hiding (joint encryption-RDH) scheme is proposed in this paper. The cover image istransformed to the frequency domain with integer discrete wavelet transform (integer DWT) for the encryption and data hiding.Additional data is hidden into the permuted middle (LH, HL) and high (HH) frequency sub-bands of integer DWT coefficientswith a histogram modification based method. A combination of permutations both in the frequency domain and in the spatialdomain is imposed for the encryption. In the receiving end, the encrypted image with hidden data can be decrypted to the imagewith hidden data, which is similar to the original image without hidden data, by only using the encryption key; if someone hasboth the data hiding key and the encryption key, he can both extract the hidden data and reversibly recover the original image.Experimental results demonstrate that, compared with existing joint encryption-RDH schemes, the proposed scheme has gainedlarger embedding capacity, and the distribution of the encrypted image with data hidden has a random like behavior.

3. Proposed System

In a few applications, a second rate right hand or a channel chairman plans to attach some extra message, for example, the source data, picture documentation or validation information, inside the scrambled picture however he doesn't know the first picture content. A few parameters are implanted into few scrambled pixels, and the of the other encoded pixels are packed to make a space for obliging the extra information and the first information at the positions possessed by the parameters. The proposed plan is comprised of picture encryption, information inserting and information extraction/picture recuperation stages. The substance proprietor encodes the first uncompressed picture utilizing an encryption key to create a scrambled picture. At that point, the information hider packs the minimum noteworthy bits of the scrambled picture utilizing an information concealing key to make an inadequate space to oblige the extra information. At the beneficiary side, the information implanted in the made space can be effortlessly recovered from the scrambled picture containing extra information as indicated by the information concealing key. Since the information implanting just influences the LSB, a decoding with the encryption key can bring about a picture like the first form. When utilizing both of the encryption and information stowing away keys, the implanted extra information can be effectively separated and the unique picture can be splendidly recouped by abusing the spatial relationship in characteristic picture.

As images are used in multimedia communication it is important to provide security for them. The main aim of the research work is to design a secure and robust model for ensuring image security using the approach of Data Hiding in Encrypted Image using DWT. The main research objective is to increase the capacity of data hiding and to reduce the distortion among the pixels of image. To achieve the above goals we state the objectives of this dissertation are as follows:

•To implement data hiding technique in encryption-decryption domain rather than plain spatial domain i.e. trying to join Steganography with cryptography. The cover media we use is the real world source image.

•To attempt to execute data hiding technique using the sequence encryption, hiding data and decryption.

•To implement a system that uses RGB-LSB mechanism allows hiding muchenough data in the image.

•To compute Quality measurements of the image and compare the results ofexisting technique with the new technique.

3.2 PROBLEM STATEMENT

In today's world there exist various techniques for securing data from unauthorizeduser. Here the new concept is proposed which will embed the additional data alongwith the color image. The initial idea of it was to extend traditional Steganography techniques to work with the color images and modify it to hide large amount of sensitive information. The key issues were how to modify the system to hide large amount of sensitive information and how to recover sensitive information in lossless manner. Overall process focuses on three parts: Cryptography data embedding and data extraction. The goal is to transform a given image and secret data into modified version that satisfies a given privacy requirement and preserves secret information communication from the intruder. Experimental results of algorithm must fulfill requirements in terms of less information loss, better response time and more privacy gain. To achieve this task here the system with combination of cryptography and Steganography which can encrypt, embed data and extract the data separately using separate keys is discussed.

3.3 PROPOSED SYSTEM ARCHITECTURE

There are two kinds of reversible data hiding techniques ie separable reversible data hiding technique and non-reversible data hiding technique. In non-separable technique i.e. reversible data hiding scheme, a content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image and then a data-hider embeds additional data into the encrypted image using a data-hiding key. Having an encrypted image containing additional data a receiver firstly decrypt it using the encryption key and can further extract the embedded data. Thus in non-separable technique it is compulsory to have both the keys.

But in separable technique it is not compulsory to have both the keys for retrieving data. In separable technique if the receiver has a data hiding key, then only he can extract the embedded or hidden data from the encrypted image containing additional data. In this dissertation the two activities are separated i.e. cover image decryption and pay load data extraction. In this dissertation one of the type of reversible data hiding method i.e. separable reversible data hiding method which consists of three main procedures Image encryption, Data embedding and Data extraction/image recovery is proposed.

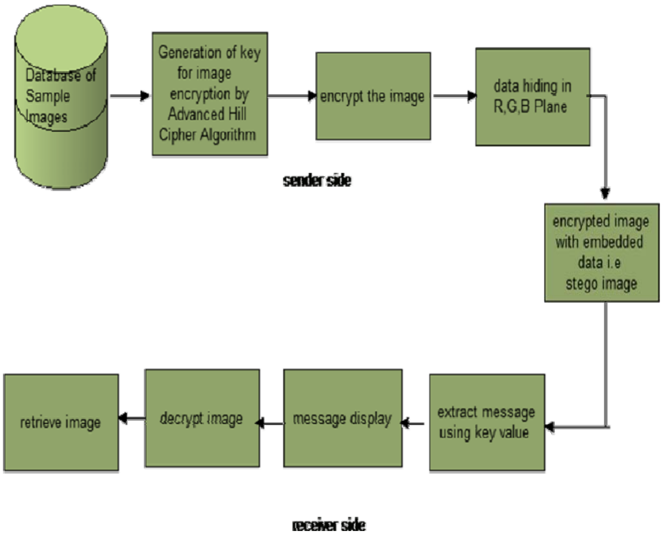
Database of Sample Images
Generation of key for image encryption by Advanced Hill Cipher Algorithm
encrypt the image
data hiding in R,G,B Plane
sender side
encrypted image with embedded data i.e stego image
retrieve image
decrypt image
message display
extract message using key value
receiver side

Figure 3.1: Proposed System Architecture

the content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then using a data-hiding key the data-hider hides the data in encrypted image by LSB method in RGB planes. At the receiver side the embedded data can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. As the data embedding only affects the LSB a decryption with the encryption key may result in an image similar to the original version. Here at the receiver side there exists three cases. With an encrypted image containing additional data which is hidden. Case one is when the receiver has only the data- hiding key, he is able to extract the additional data even if he does not know the image content. Case two is if he has only the encryption key, he can decrypt the received data i.e. encrypted image to obtain an image similar to the original cover media, but cannot extract the embedded additional data. Case three is if the receiver has both the keys i.e. data-hiding key and the encryption key, he can extract the additional data and recovers the original image without any error. The proposed scheme is describing the method in which the concept of data hiding in encrypted image is executed using LSB-DWT method. The existing approach of using data hiding involve simple LSB method in which the least significant bits of the single plane of the pixel value(representing one pixel as one byte or eight bits) is used for creating space. The space creation is for making room for external/additional confidential information which is to be hide/embedded. The author Xinpeng Zhang uses this simple LSB based compression. But this technique could not hide enough data the scheme is having limitation that at the receiver side receiver can extract the additional data and recover the original content when the amount of additional data is not too large. Thus the scheme is not suitable if anyone wants to embed the more data. So to overcome this problem we need a new method or new technique which can handle enough data to embed. An RGB image referred to as a "true-color" image is stored as an m by-n by 3 data array that defines red, green, and blue color components for each individual pixel. The color of each pixel is determined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location. Graphics file formats store RGB images as 24-bit images, where the red, green, and blue components are 8 bits each and the Least Significant Bits of this each 8 bit is called RGB-LSB. In general in LSB method hidden information is stored into a single plane of the pixel values. In our scheme hidden information are stored into three planes of RGB. Actually these three colors are represented as three matrices red, green and blue.

3.4 EXECUTION FLOW OF THE SYSTEM

Execution of proposed system at sender side is divided into three modules like Image encryption, data embedding and image recovery.

MAIN MODULES

1. Image Encryption

2. Data Extraction

3. Image Recovery

3.4.1 Image Encryption Using Advanced Hill Cipher For A Public Key Cryptosystem

The reversible data hiding in encrypted image is investigated in most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content, and it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content.In the Advanced Hill cipher, the basic equations governing the encryption and the decryption are given by

C = AP mod N …………………(4.1)

P = AC mod N ………………….(4.2)

where A is an involutory matrix which includes the key matrix. Since A is an involutory matrix, we have A-1 = A, where A-1 is the modular arithmetic inverse of A. Thus in the case of this cipher, we need not compute the modular arithmetic inverse of A separately, once A is known to us. The objective is to modify the Advanced Hill cipher and develop a enriched block cipher which includes an involutory matrix and a set of functions for creating confusion and diffusion, thus transforming the plaintext to a secure cipher.

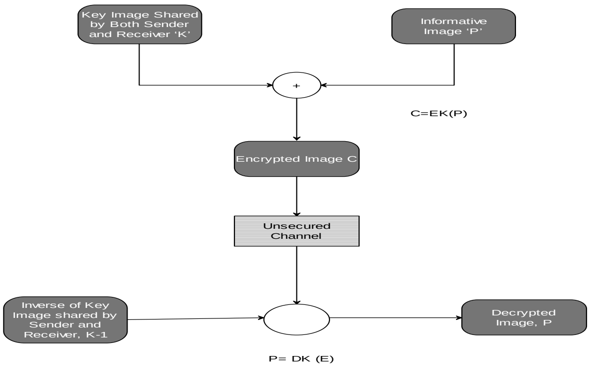
Key Image Shared by Both Sender and Receiver 'K'
Informative Image 'P'
+
C=EK(P)
Encrypted Image C
Unsecured Channel
Inverse of Key Image shared by Sender and Receiver, K-1
Decrypted Image, P
P= DK (E)

Figure 3.2: Block Diagram of Implementation of Hill Cipher Algorithm

3.5.2 Generation OfInvolutory Matrix

(AA-1) mod N = I ………………..(4.3)

AA-1= A …………………….(4.4)

where A is a square matrix of size n, From equation 4.1 and 4.2 we get equation as follows

A2 mod N = I ……………….(4.5)

inwhich I is an identity matrix. From (4.5), the matrix A can be obtained by representing it in the form

A=[■(A11&A12@A21&A22)] ………………....4.6

and taking A11=K, where K is the key matrix. The relations governing,A22, A12 and A21 are given by following equations

A22= -K ……………………………...4.7

A12= [d(I- K)] mod ………………………………4.8

A21= [λ(I+ K)] mod N ……………………………4.9

where $(d\lambda) \bmod N = 1$ ……………………………4.10

The cipher is developed by using the relations

$C = (AP + A_0) \bmod N$ ……………………………4.11

$P = (A(C - A_0)) \bmod N$ ……………………………4.12

HereA0=[■(A11&A12@A21&A22)] ………………4.13

is obtained by permuting the sub matrices of A. For a plaintext input, on using the involutory matrix, and from equations 4.11, 4.12 and 4.13, we get a 8x8 matrix. To the 8x8 matrix, we add the resulting value of the equation P'= (nPn-a mod 256)+P, to the first four rows of the matrix, and P'= (n+1Pn+1-a mod 256)+P, to the bottom four rows of the 8x8 matrix, where 'n' is the randomly generated public key of receiver and 'a' is the private key. After the calculation of P', the 8x8 matrix is scrambled twice by two unique and distinct patterns for better diffusion of the contents to get P"'. Further, we calculate the determinant of the P"' matrix and represent it in a symbol and transmit it to the receiver. The receiver again calculates the determinant from the transmitted cipher and compares it with the symbol transmitted earlier. If a match is found, it ensures that no data has been tampered by the adversary and the user authentication is successfully carried out. If there is a mismatch with the transmitted and the calculated value of determinant by the receiver, then the packet re-transmission request is sent.

Algorithm for Encryption

```
1. Read n,P,K,a,d,j
2. $A_{11}$ = K, $A_{22}$=(-K)
3. $A_0$ = permute(A)
4. P=(AP+$A_0$)mod256
5. For i=1 to j
{
P'= (nPn-a mod 256) +P
If i>4
P'= (n+1Pn+1-a mod 256) +P
 6. P"= Level 1 scramble
 7. P"'= Level 2 scramble
8. det [P"'] calculated
9. C=P"'
```

Algorithm for Decryption

```
1. Read n,C,$A_0$,a,d,j
2. $A_{11}$ = K, $A_{22}$=(-K)
3. $A_0$ = permute(A)
4. det [P"'] verified
5. C"'= Level 2 de-scramble
6. C"= Level 1 de-scramble
7. For i=1 to j
{
  C'= (nPn-a mod 256)-P
  If i>4
  C'= (n+1Pn+1-a mod 256)+P }
8. P= (A(C-$A_0$)) mod256
9.Write P
```

4. Result Analysis

Data Hiding in encrypted Image by using DWT which is also called lossless data embedding embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An exciting feature of this dissertation is the reversibility that one can remove the embedded data to restore the original image. Data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The performance of algorithm cans be measured by the following parameters.

4.1 EVALUATION PARAMETERS

Payload capacity limit

What is the maximal amount of information can be embedded? Since it may be measured in KB in case of embedding file or it may be measured in length of the string in case of text embedding or it may be measured in number of pixels in case of image embedding.

Complexity

What is the algorithm complexity? This is also one of the performance measurements to show how much the algorithm is complex.

Visual quality

How is the visual quality of the embedded image? To compare the quality of original image and recovered image, various evaluation parameters can be used which can provide indication about the correctness or percentage of data recovered in lossless manner. The following evaluation parameters are used. Since it may be measured by PSNR and SSIM. Here our scheme uses both parameters ie PSNR and SSIM to estimate the visual quality.

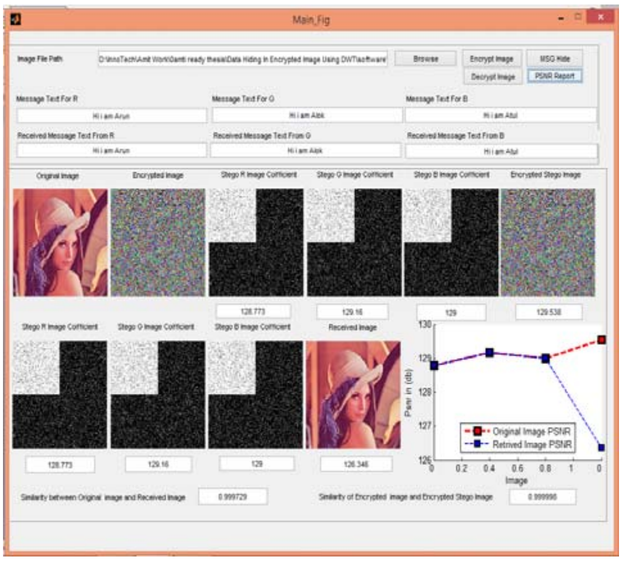

Image File Path D:\InnoTech\Amit Work\Samt ready thesis\Data Hiding In Encrypted Image Using DWT\software

Message Text For R: Hi i am Arun

Message Text For G: Hi i am Alok

Message Text For B: Hi i am Atul

Received Message Text From R: Hi i am Arun

Received Message Text From G: Hi i am Alok

Received Message Text From B: Hi i am Atul

Stego R Image Cofficient: 128.773

Stego G Image Cofficient: 129.16

Stego B Image Cofficient: 129

Encrypted Stego Image: 129.538

Stego R Image Cofficient: 128.773

Stego G Image Cofficient: 129.16

Stego B Image Cofficient: 129

Received Image: 126.346

Similarity between Original image and Received Image: 0.999729

Similarity of Encrypted image and Encrypted Stego Image: 0.999998

Figure 4.1 Decrypted Image**.**

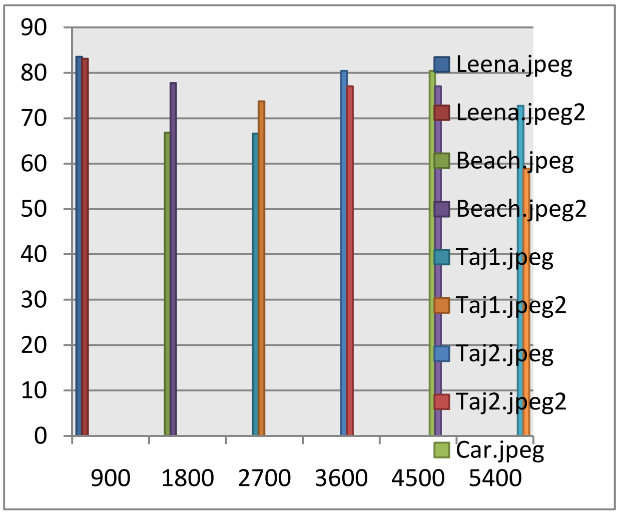

Figure: 4.2 Graph of PSNR of Stego Image and PSNR of Retrieved Image against Payload(Data Capacity) for JPEG Images

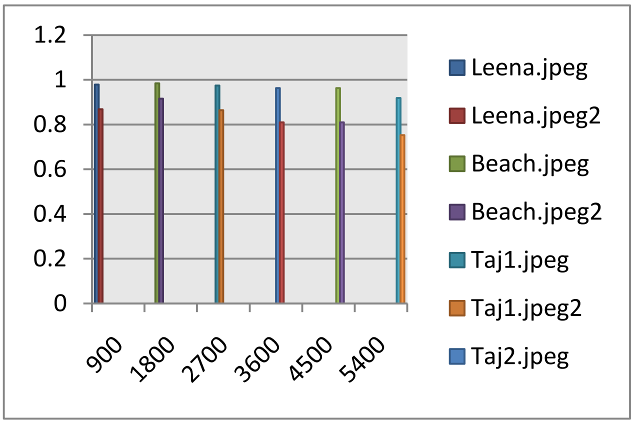

Figure:4.3 Graph of SSIM of Stego Image and SSIM of Retrieved Image against Payload(Data Capacity) for JPEG Images

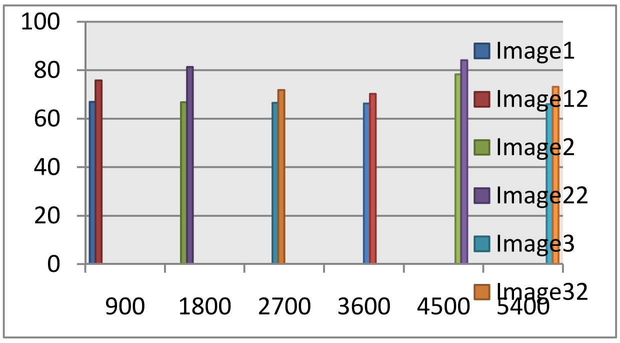

Figure: 4.4 Graph of PSNR of Stego Image and PSNR of Retrieved Image against Payload(Data Capacity) for BMP Images

5.CONCLUSION

In this paper the scheme of data hiding in encrypted image using Wavelet Transform method is discussed. This approach describes how the performance can be maintained after changing the type of the secure data. Here an approach of data hiding in encrypted image is found out, which is capable of hiding text data. The mechanism of data hiding is wavelet transform. Also by using the novel wavelet transform method for embedding the data the size of the net payload can be increased sufficiently. So after studying this novel technique it has been concluded that it is possible to hide more text as a data.In other words it is possible to hide enough or large amount of data without compromising security as well as quality of the coverimage. In this scheme the quality of cover media is not degrade. The original cover image has high quality index after it undergoes encryption, data hiding and decryption.High PSNR value is observed for the decrypted cover image. It is observed that the PSNR values of extracted image are higher enough and originality between cover image and retrieved image is very much similar.

REFERENCES

[1] Shun Zhang, TiegangGao, and Guorui Sheng,” A Joint Encryption and Reversible Data Hiding Scheme Based on Integer-DWT and Arnold Map Permutation”,Hindawi Publishing Corporation Journal of Applied Mathematics Volume 2014, Article ID 861782, 12 pages.

[2] A. Kaja Moideen1, K. R. Siva Bharathi2,” A Novel Method for Data Hiding In Encrypted Image and Video”, International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.

[3] Zhaoxia Yin, Bin Luo, and Wien Hong, ” Separable and Error-Free Reversible Data Hiding in Encrypted Image with High Payload ”,Hindawi Publishing Corporation the Scientific World Journal Volume 2014, Article ID 604876, Pp-1-8.

[4] Raman Gupta, DiptiBansal, Charanjit Singh,” A Survey on various objective Image Quality Assessment Techniques”, International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-2, Issue-7, July 2014, Pp 99-104

[5] Ma, Sch. Of Inf. Sci. &Technol, Univ. Of Sci. & Technol. Of China, Hefei, China Weiming Zhang ; Xianfeng Zhao ; Nenghai Yu ; Fenghua Li,” Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, Information Forensics and Security, IEEE Transactions on (Volume:8 , Issue: 3), 25 February 2013, 1556-6013,Pp-553 – 562.

[6] K. Arun Kumar & S.M. Riyazoddin,” Analysis of Data Hiding Techniques in Encrypted Images A Survey”, Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[7] Kadam, P. ; Nawale, M. ; Kandhare, A. ; Patil, M.,” Separable reversible encrypted data hiding in encrypted image using AES Algorithm and Lossy technique”, International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 21-22 Feb. 2013,Pp- 312 – 316.

[8] Deepthi Barbara Nickolasa ,Sindhuja.B , Sivasankar. A,” Enhancement of Data Hiding Process in Encrypted Image Using Advanced Encryption Standard”, International Journal of Current Engineering and Technology ISSN 2277 – 4106, Vol.3, No.2 (June 2013),Pp 366-368. [9] ZhenxingQian, Xiyu Han, Xinpeng Zhang,” Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification”, 3rd International Conference on Multimedia Technology（ICMT 2013),Pp 869-876.

[10] A. Gangwar and V. Shrivastava, “Improved RGB -LSB Steganography Using Secret Key”, International Journal of Computer Trends and Technology, vol. 4, Issue 2, pp. 85-89, 2013

[11] P. S. Kumar and C. BalaKrishnan,“Embedding of executable file in encrypted image using LSB mechanism”, International Journal of Emerging Technology and Advanced Engineering,vol.3,Special Issue 1, Pp. 432-438,Jan. 2013.

[12] SumanChandrasekhar, AkashH.P ,Adarsh.K, Mrs.SmithaSasi,” A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem”,IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), Pp10-14.