Performance Analysis on Different Images using Reversible Data Hiding Technique and its Application

Khan Amrin Naaz
University of Mumbai
Terna Engineering College
Nerul,Navi mumbai

Imdad Rizvi
University of Mumbai
Terna Engineering College
Nerul,Navi mumbai

M.M. Kadam
University of Mumbai
Terna Engineering College
Nerul, Navi mumbai

ABSTRACT

Communicating securely is what everyone wants. Earlier it was simply data hiding then reversible data hiding and currently its encrypted data hiding reversibly. Introducing new challenge is always as important as keeping it unreachable to the hacker. In proposed work security is enhanced by encrypting data and then embedding the encrypted form of data. Reserve Room before encryption gives an added advantage for enough space for data hiding. Haar wavelet is best suitable wavelet amongst other wavelet like symlet, bior, coiflet and contourlet, when the input image is encrypted image rather than a plain image. The quality of image has been evaluated by performance analysis like MSE, PSNR and hiding capacity on different types of color images and results were compared. Minimum errors with high SNR rate at various data hiding capacity were seen.

General Terms

Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords

Reversible data hiding, chaos encryption, LSB replacement, RSA key encryption, Haar Wavelet transform, LWT, PSNR etc..

1. INTRODUCTION

Communication is must in everyday life and more over secure communication is must. Today various techniques are available to transmit data securely. Evolution of a simple data hiding from cryptography to Visual cryptography and various steganography methods from audio, video to digital images were seen. And again from simple data hiding to reversible data hiding has taken place. While hiding data the cover image gets slightly altered. Reversible Data Hiding (RDH) interprets a method where data can be camouflaged in any cover media example digital image and can get back the cover image without any alteration that means during recovery of secret data, the cover image is also recovered losslessly i.e. without degradation. It is more advanced than a simple data hiding technique like one way hiding with respect to cryptography or steganography. Many applications such as law enforcement, Medical application for example keeping patient's information secret, military application where the invisibility of secret hidden data is of high demand. Also these application requires lossless recovery of original image and hence the need of reversibility.

There are two types of Reversible data hiding: 1) Vacating room after Encryption (VRAE) 2) Reserve room before Encryption (RRBE).

1) VRAE: Reversible data hiding by vacating room after Encryption technique. Previous method used to embed data by reversibly vacating room from the encrypted images, that may subject to some errors while data extractions and / or image restorations. Also space is limited for embedding data.

2) RRBE: Reversible data hiding Reserving room before Encryption technique. Instead of vacating room after encryption process it is done prior to encryption giving an advantage of spacious room to embed data.

Data can be hidden in color images or grey level images. A color image improves hiding capacity and hence gives better PSNR. Reversible data hiding (RDH) has many different techniques such as Difference Expansion method (DE) in [1] and [2], Histogram modification method in [3] and [4], Lossless compression methods in M. [5] and [6].

—In difference expansion method a new LSB plane is created by calculating the difference between two adjacent pixels and then the difference is doubled. In Histogram technique with respect to image processing, refers to a histogram of the pixel intensity values. This histogram is a graphical representation showing the number of pixels in an image at each different intensity value of that image.

—In [3], number of pixel at each different intensity value is further used to evaluate and construct the histogram.

— [4] says Plus point of histogram method are: High payload and Distortion is quite invisible.

—Limitations of histogram are: limited capacity is achieved by the frequency of peak pixel value in the histogram and also it takes long time to search the image several times, that makes the algorithm more time consuming.

—In [7] lossless compression method, room or space to embed the secret data is done by compressing exact bit plane that gives minimum redundancy to maintain secret information. Condition is image must be noiseless while selecting the lowest bit plane that provides lossless compression

2. EXISTING SYSTEM

Authors in [8] investigated the Reversible data concealment in encoded image. The methodology is still improved with encryption of text messages using an asymmetric key method along with the encryption of images. This can be the rationale for an advanced brand new security approach called reversible data concealing arises. This is a fashion of hiding the existence of data in another transmission medium to achieve a goal of secret communication. The application of Reversible data hiding are such as Patient's medical reports, confidential data in military, electronic data, finger print identification etc or any host image where permanent distortion of original image after extracting the embedded data is never entertained. In [9], Authors used AES algorithm to convert original image into cipher form. [10] uses reserve room before encryption approach to solve the problem of previous ways such as vacating room after encryption and pixel difference expansion. This spatial domain technique distorts an image quality wherever the secret message bits were hidden. With the thought of these issues, the system proposes the reserve room approach with lifting wavelet transformation to maintain image quality and improve the secure transmission. The technique lifting wavelet decomposes an image into frequency sub bands which contains approximation and detailed coefficients. The system will reserve the coefficients from detailed components which have texture, edges and region boundary. It's insensible region for human eye. In [11], Authors modified the Vacating room after encryption to reserve room before encryption. Authors were successful in getting enough space to embed data bits into the encrypted image but reduces the image artifacts and still it fails to reconstruct an image with free of loss due to data hiding under spatial domain. J. Tian in [2] uses pixel difference expansion for reversible data hiding, the secret bits are concealed into the differences of neighbouring pixels by increment or decrement the difference. It causes complexity in algorithm and gives high error rate at minimum hiding capacity. Taking this issue into consideration, proposed system chooses reliable and flexible methods to overcome this constraints and yields better quality during image reconstruction after the extraction of embedded data. X. Zhang in [8] proposes the reversible data hiding approach based on vacating room after encryption. In this method, the content owner encrypts the original image and it is then passed to data hider. The data hider hides secret data by replacing some encrypted pixels causes image distortion at data recovery. Kalker & Williams in [12], proposed "a rate-distortion model" and "a recursive code construction"for data hiding reversibly, and proved that rate-distortion bounds of RDH for memory less covers but the proposed "recursive code construction" failed to approach the bound. A general framework for RDH technique is proposed by J. Fridrich & M. Goljan in [13] Where, compressible features of original cover was extracted and then those extracted features were compressed losslessly so that free space can be utilized for embedding auxiliary data. In [14], Authors chose binary cover for embedding data. The recursive code construction was improved to prove that this construction can reach the rate-distortion bound as long as the compression algorithm reaches entropy, making equivalence between data compression and RDH for binary covers. Authors Sushil Kumar & S.K. Mutttoo in [15] chose contourlet for stegnanography but the image is plain and not encrypted. Nowhere the author has mentioned about encrypted image. In proposed paper this is not possible to use counterlet because the cover image is encrypted.

From the above literature survey ,can be concluded ,there are roughly 3 techniques widely used Difference expansion, Histogram method and lossless compression method.

3. PROPOSED WORK

Proposed work is divided into three modules namely 'content owner', 'Data hider' and 'Receiver'. Color image is taken as an input cover image which is then separated into number of blocks locally and lifting wavelet will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption method. The chaos encryption technique is used to encrypt the image. Image encryption enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After image encryption, image is compressed using Haar wavelet. The data hider will embed the secret data into the detailed coefficients which are reserved before encryption. Here image compression is done on already Encrypted image hence the only suitable wavelet is Haar. Sushil Kumar & S.K. Mutttoo in [16] showed that "Haar wavelets are best for the imperceptibility and security of image as compared to other wavelets". Encryption might have some security issues, but they make the secret messages meaningless text. Adaptive least significant bit replacement method is used to conceal the bits of secret data into the the encrypted image. In the receiver module, the authorized person will decrypt the image losslessly from encrypted stego image, extract the data and finally decrypt the data using the relevant keys. Lastly the performance analysis like MSE, PSNR, Correlation time and Elapsed time were done to check the efficiency of this proposed method. Haar wavelet was found best because other conventional wavelet filters like morlet, slantlet etc often have floating point co-efficient and therefore the reconstructed image is distorted image. Haar wavelet is based on lifting scheme and they map integer to integer. Thus there is no need of conversion from floating point to integer. Hence the reconstructed image is the lossless recovered original image.

3.1 The Proposed system is basically divided into three modules

i) Content owner ii) Data hider iii) Receiver

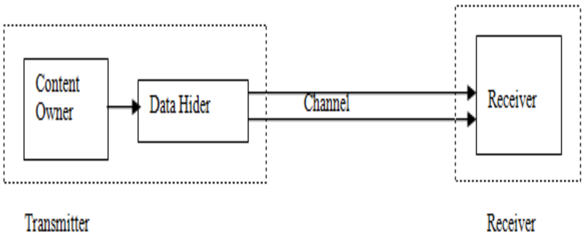


Fig 1: Frame work of proposed Reversible Data Hiding

i) Content owner module:

Content owner part deals with a) choosing an image b) Reserving room for embedding c) image encryption

a) Choosing image as Input: Color image is taken as the original cover image.

b) Reserving room: Room or space is reserved for hiding the secret data before encryption.

c) Image encryption: Image is encrypted by the content owner.Encrypted image so formed is passed as an input to the data hider.Next module is data hider, where actually the secret data is hidden.

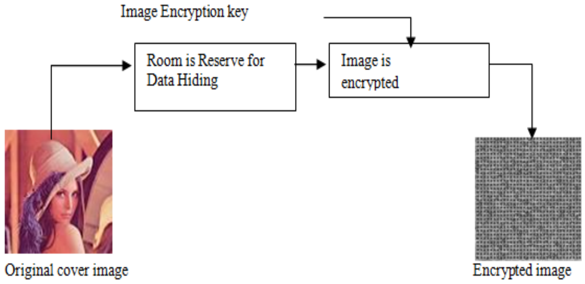


Fig 2: Frame work of content owner module.

ii) Data hider module:

In data hider, this section deals with Text encryption and embedding. Refer Fig 3.

a) Encrypted image as Input: Encrypted image from the content owner modules is given as an input to data hider module. In addition to this, data to be hidden is also taken as another input.

b) Encryption of Data: Data to be hidden is encrypted using RSA asymmetric encryption key to form encrypted data.

c) Data embedding: Secret data to be embedded is concealed using data hiding key into the encrypted image to form an encrypted stego image.

Encrypted stego image so formed is passed as an input to the receiver.

Next module is Receiver module. Where actually the information is received or extracted.

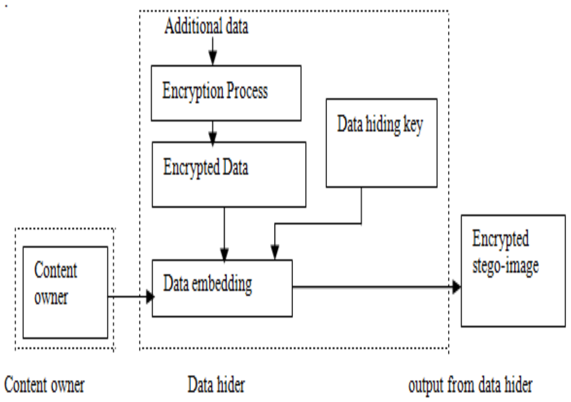


Fig 3: Frame work shows block diagram for Data hider

iii) Receiver Module:

Receiver can be either the content owner or any authorized person having the key. Since this paper uses asymmetric key for encryption and decryption of text, the receiver will have different key for decryption..

a) Image decryption: Encrypted stego image so formed from the data hider is received by the receiver. Image is decrypted using decryption key.

b) Data extraction:

After the image is decrypted, text is extracted in encrypted form only.

c) Data decryption:

Lastly the data is decrypted using the relevant key.

The decrypted image is the lossless recovery of original image.

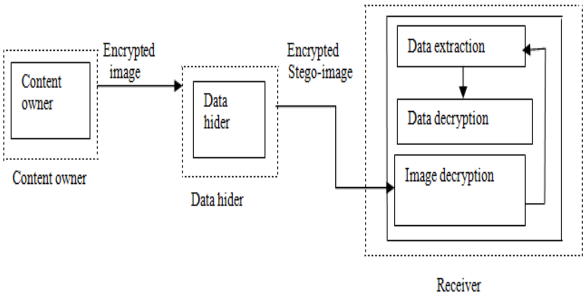


Fig 4: Frame work shows block diagram for Receiver.

3.2 Process Flow of Proposed Work

3.2.1 Process flow for Data encryption and embedding

This section explains the algorithm for the step by step process of Data embedding. Ref Fig: 11

Algorithm1: For Data embedding

Step1: Selection of cover image.

Step 2: Plane separation is applied to the cover image to get red, green and blue plane.

Step: 3 Lifting wavelet transform (LWT) is applied to reserve space by decomposition of LWT into approximation and detail coeffients.

Step4: Detail coefficient is extracted to embed data and approximation coefficient is used for Image encryption.

Step 5: secret data is encrypted using RSA asymmetric key algorithm.

Step 6: Data concealed using LSB substitution

Step7: Image is encrypted using chaos encryption ref fig 9. Encrypted image so formed after 4, 5 and 6 is Encrypted stego image.

Step8: Performance Analysis like PSNR, MSE, correlation time and elapsed time is calculated for checking efficiency.

3.2.2 Process flow for Image and text decryption.

Image and data can be recovered in two ways:-

Case1: First image is decrypted → Text is extracted → Text is decrypted → Original image is recovered.

Case2: First Text is extracted →Text is decrypted → Image is decrypted →Original image is recovered.

Following is the process flow diagram of data extraction and image extraction.

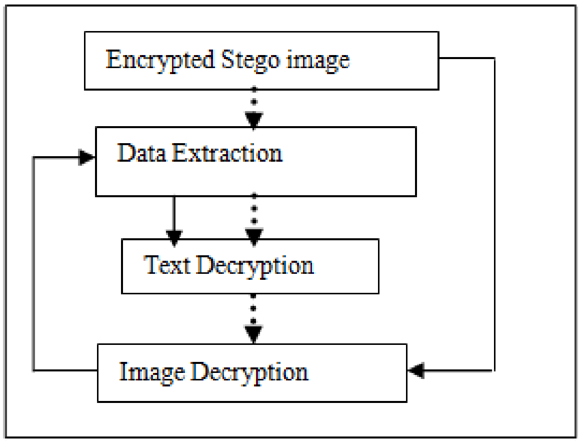


Fig 5: Decryption of Text and Image

Algorithm 2: For data and image extraction

Step 1: encrypted image is extracted from Encrypted stego image and is then decrypted

Step 2: Encrypted data is extracted from the decrypted image

Step 3: Finally the encrypted data is also decrypted using the relevant key.

The proposed method is employed with case1

So the whole idea can be described in

A. Image Encryption. B. Concealment of secret data. C. Data extraction and Image recovery. D. Performance Analysis.

A. Image encryption

This process is sub divided into four steps

1) Selection of cover image 2) Plane separation of original image 3) Reserving room for embedding

4) Encryption using chaos method.

1) Selection of cover image: The input color image (.jpg, .bmp, .tiff etc) is selected. It is used in the form of carrier where the secret text can be embedded. Proposed method have used different format (.jpg, .bmp, .tiff etc) and different types (Low contrast, high contrast, facial, low component and high component image) of images. After selection, images are carried out for further process.

2) Plane separation: The input image is a true color image consisting of 24-bit image. Color image comprises of three sub colors that together forms a color image, namely Red(R), Green (G) and Blue (B). Each color is of 8-bit. Hence 3 bit per pixel can be stored. The Red and Green planes are highly sensitive one for simple pixel variations. The red plane contains the brightest components of the image, the green plane contain the moderate one and the blue plane for darkest one. To preserve the image quality we choose the blue plane for data hiding process.

3) Lifting Wavelet Transform (LWT): Lifting wavelet transform using haar filter is applied to the blue plane image. It is done to decompose the image to get four detailed coefficient sets. Refer Fig 6.

Of four sub band images respectively say ‘LL,LH,HL and HH’ Where first letter L and H stands for low pass and high pass filter where as second letter L and H corresponds to the filter applied to the column. LL contains significant part of spatial domain where as High frequency sub bands LH, HL and HH contains edge information of input image. Thus secret message is embedded into this high frequency sub bands since they are non- sensitive to human visual system. LWT has an advantage that it converts the DWT coefficients into Integer coefficients without losing any information.

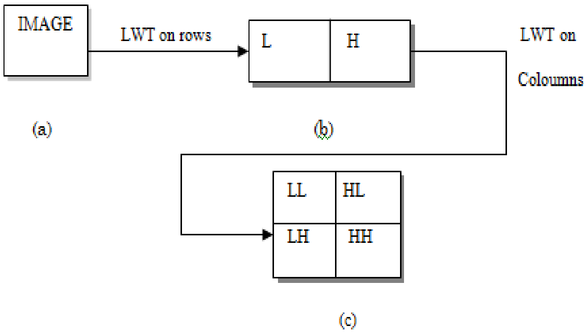
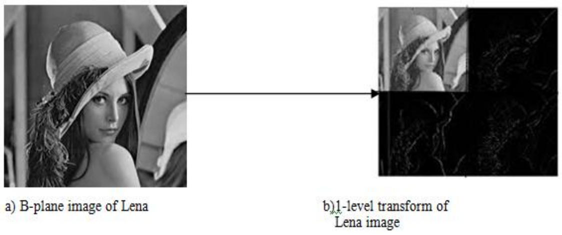


Fig 6: Diagram of DWT (a) Original Image (b) Output image after the 1-D applied on Row input (c) Output image after the second 1-D applied on column input.


a) B-plane image of Lena

b)1-level transform of Lena image

Fig 7: a) B-plane image b) 1-level transform of Lena image.

Further it can be decomposed from one level to two levels and from two levels to three.

Decomposition of LWT and its flow:

Image is taken as an input. Of this image first the columns is transformed by using a filter bank vertically and the same is then applied to each row horizontally. One-level of wavelet decomposition produces four filtered and sub sampled images, referred to as sub bands. These filters are applied separately on the even odd location.

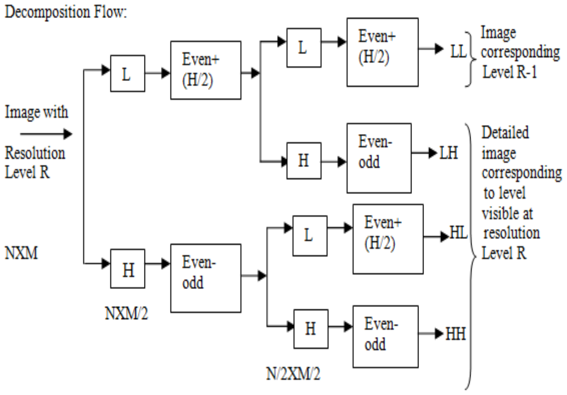


Fig 8: Decomposition flow using LWT.

Hence detailed co-efficient of the image is extracted.

4) Image encryption:

Image is encrypted using chaos encryption. Encryption is a process of scrambling original information into unknown form using either symmetric or asymmetric key standard. Here it is one of the advanced encryption standard called chaos crypto system used. Original image is taken. Initially constant factor 255 is considered. To the chaotic sequence threshold function is applied. This chaotic sequence is now performed bit XOR with the pixel value of original image ‘Pij’. The resulting encrypted pixel is given by ‘Eij’. Output of bit XOR block is Encrypted image.

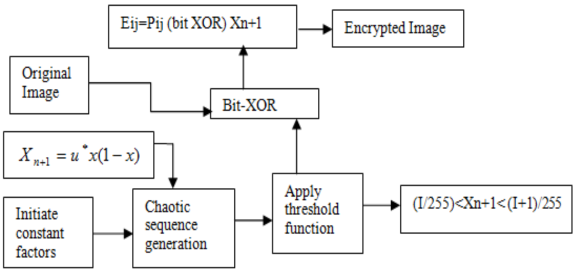


Fig 9: Block diagram of Image Encryption using chaos crypto system

Chaotic map sequence: chaotic map is created using logistic map.

The secret image must be transmitted securely through unsecure channel in order to prevent data hacking. These chaotic systems are expounded on a complex or real number space which is called as boundary continuous space.

$$c_{n+1} = u * c_n^* (1 - c_n)$$

Let, the c_{n+1} be X_{n+1} and c_n be x

and encrypted pixel so formed is defined by the equation, $E = bitxor(P, c_{n+1})$

B. Concealment of secret data before encryption:
This part is again divided into 1) secret message encryption 2) Data concealment and

1) Secret message encryption: Secret message is encrypted using RSA algorithm

Here RSA public key is used to encrypt data. Algorithm for RSA encryption is:

1. Choose any two prime number $p \quad and \quad q$, where $p \neq q$.

$p \quad and \quad q$ Can be any integer and may be of same bit-length chosen randomly or by using primarily test.

2. Calculate the modulus 'n': $n = pq$ .Modulus parameter is same for public key and private key.

3. Calculate $\Phi(n)$: $\Phi(n) = (p-1)(q-1)$.

4. Choose public key exponent 'e': Any integer can again be randomly selected that lies between 1 and $\Phi(n)$ i.e. $1 < e < \Phi(n)$ greatest common divisor of

$(e, \Phi(n)) = 1$ .Means only "1" is the common divisor for $e \quad and \quad \Phi(n)$.

5. Calculate private key exponent'd': $d = e^{-1}(\bmod \Phi(n))$

by rearranging the above equation $d^* e = 1 \bmod \Phi(n)$

i.e. $\dfrac{(d^* e - 1)}{(p-1)(q-1)} = k$ or $\dfrac{\Phi(n)k + 1}{e} = d$ for $k = 1,2,3.....$

Public Key is a pair of (n, e) and private Key pair is (n, d).

Let's see flow chart of the above algorithm:

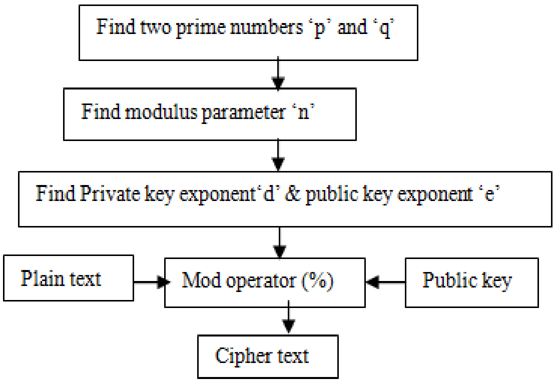

Find two prime numbers 'p' and 'q'
Find modulus parameter 'n'
Find Private key exponent'd' & public key exponent 'e'
Plain text
Mod operator (%)
Public key
Cipher text

Fig 10: Text Encryption using 8-bit key

2) Data Concealment:

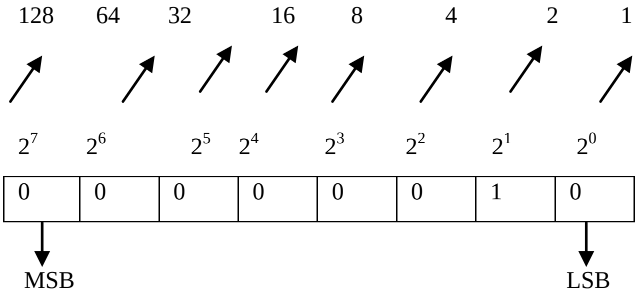
Main purpose of proposed work is to conceal secret data successfully and recover original cover image losslessly. For embedding purpose LSB technique is used .In LSB algorithm, bits of the secret data is embedded into the least significant bit of the pixel value of image. Such that first bit of secret data is embedded into least significant bit of first pixel. Second bit of message is embedded into LSB of second pixel and so on. Least significant bit is always the right most bit. Blue plane is chosen for embedding data. Blue plane is an 8-bit image. Modification in the least significant bit of the pixel value in image will not damage the image and so the bits can be hidden easily. That's why the resulting stego image looks like the original cover image. Stego image and the cover image are color image. It's very difficult for the human to differentiate between the two. But there is always a slight difference between the stego image and the original image. This difference is called as error and can be calculated as MSE. One pixel can hence display 28=256 variations or hues. The weighting configuration block diagram of an 8-bit number is illustrated in below example. For enhancing the security the secret message is encrypted and then embedded using above LSB method.

Example 1:

For decimal number '2', binary is 00000010

For decimal number '3' binary is 00000011

Weighting configuration for 2 is:



The weighting configuration of 2 shows the LSB (Right most bit) is '0' with value 1

And MSB of 2 is also '0' with value 128.

The same weighting configuration can be seen in pixels of image:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Any modification in the LSB of pixel value of image will keep the MSB same hence the cover image remains unchanged. See example 2

Example 2:

- Blue Plane image is having 8 bit pixel

B_1=00000001 B_2=00000010 B_3=00000100 B_4=00001000 B_5=00000101

B_6=10000001 B_7=10010001 B_8=01110110

- Simple Secret Data is A

Binary value of ‘A’ is 01000001

- LSB substitution: First bit of secret data is replaced by LSB of first pixel value i.e.

B_1=00000001 B_1=00000000

0 1 0 0 0 0 1 0

Original Pixel Modified pixel

Similarly the second bit ‘1’ of character ‘A’ is embedded into LSB of B_2

B_2=00000011

- Image is made of several pixels, each pixel of 8 bits
- For true color image each pixel consists of 24 bits (8bit for red, 8bit for green and 8 bit for blue). Therefore, 3bits per pixel can be substituted. The proposed work done using 24bit color image.

From the above example the MSB of the Pixel is unchanged. Hence the image is losslessly recovered.

Also proposed work the character ‘A’ is encrypted first and then the each bit is embedded into the LSB of the each pixel value.

C. Data extraction and image recovery:
This section is divided into 1) Image decryption 2) Extraction of data 3) Data decryption

At receiver side, receiver can be the content owner it’s self or any third authorized person. Authorized can have 3 conditions such as follows:

Case I: Data hiding key only- With only data hiding key, receiver only extract the data where as the original image remains unreadable.

Case II: Encryption key only- With encryption key alone, receiver can only retrieve the original image and not the data.

Case III: Both data hiding and encryption key- can Retrieve data as well as the original image.

1) Image decryption: If the receiver or the authorized person knows the encryption key, he will be able to decrypt the image. The scrambled pixels so formed come to its original place. Thus the original image is recovered losslessly. Difference between the original image and the stego image known as MSE is calculated.

2) Data extraction: Using the data hiding key the secret message is extracted from the decrypted image.
3) Data decryption: Data is decrypted using the equation,
Plain_text = Cipher. ^d mod n

D. Performance Parameter analysis
Performance analysis is done based on Hiding capacity, MSE, PSNR mainly and along with this correlation time and elapsed time is being calculated.

1. *Hiding Capacity:* Maximum data that can be hidden in a media e.g. cover image in a way that the cover image is not disturbed or degraded. In this proposed paper the message is encrypted and then embedded using advance LSB substitution and hence the hiding capacity increase which increase the amount of data to be hidden. The main point of this paper is if the input is taken as gray scale image, its 8 bit image but the true color image is of 24 bit so we get 8 bit from each color for embedding.

MSE: Mean square error means it is the square of error between the Original cover image and the encrypted stego-image.low MSE means less error.

MSE=1/M*NΣM,N[I(M,N)-J(M,N)]2

M*N – No. of Rows and Columns in an image.

I(M, N) – Original Image.

J(M,N) – Marked Image.

3. *PSNR:* It is the Peak Signal to Noise Ratio is the ratio between the signal variance and reconstruction error variance. PSNR is calculated between original image and the reconstructed image.

Its formula is

PSNR= 10 log10 (Peak val^2/ MSE)

i.e. PSNR= 10 log10 (255^2/ MSE)

in worst case scenario when MSE=1, PSNR=48.13dB.

From above it can be seen that PSNR is inversely proportional to MSE i.e. if low MSE means less error and and so PSNR is higher. PSNR is better .In other words, PSNR means signal to noise ratio so as signal increases noise decreases , if value of PSNR is better so is the signal with reduced noise value.

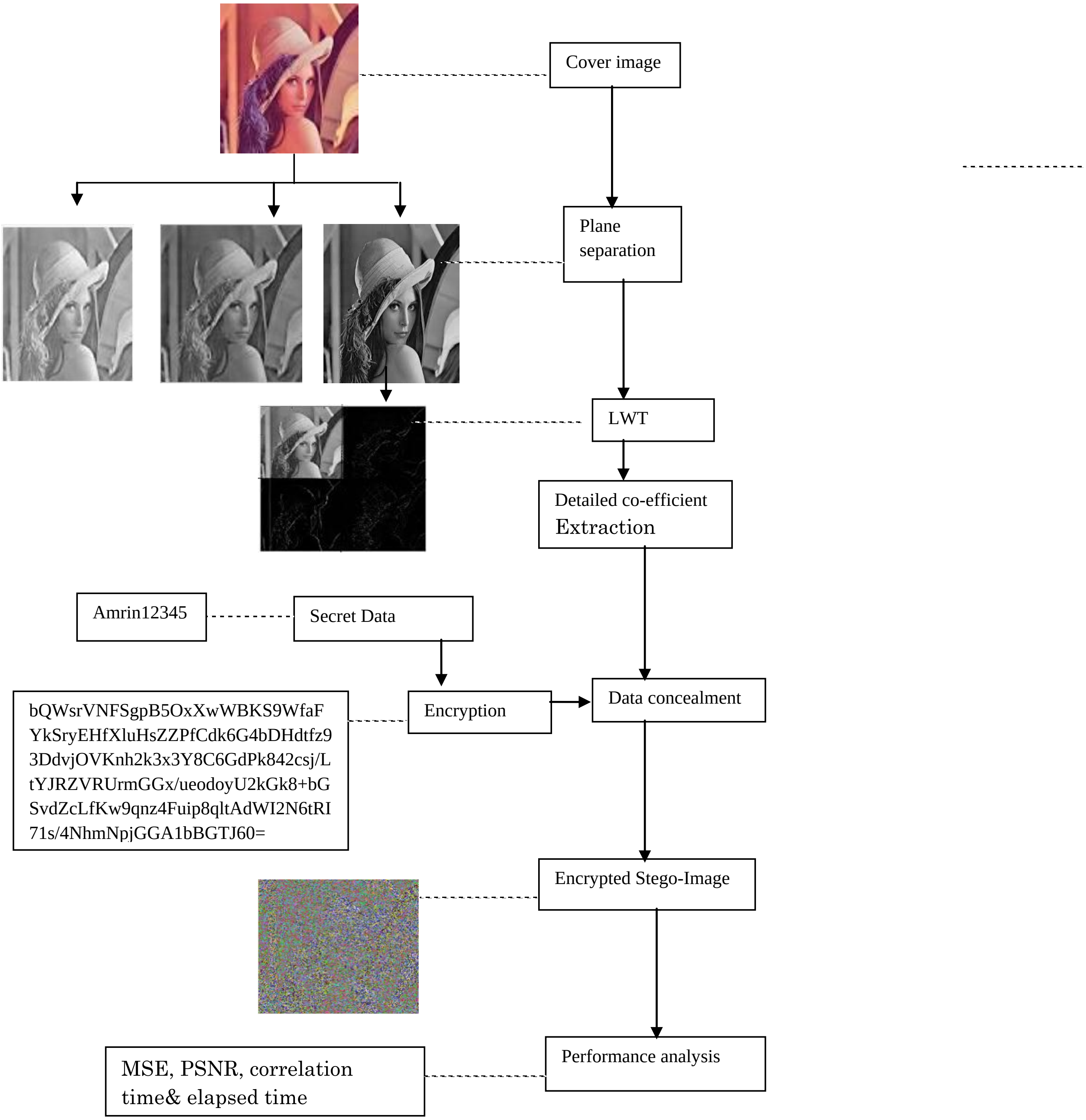

Cover image
Plane separation
LWT
Detailed co-efficient Extraction
Amrin12345
Secret Data
bQWsrVNFSgpB5OxXwWBKS9WfaF
YkSryEHfXluHsZZPfCdk6G4bDHdtfz9
3DdvjOVKnh2k3x3Y8C6GdPk842csj/L
tYJRZVRUrmGGx/ueodoyU2kGk8+bG
SvdZcLfKw9qnz4Fuip8qltAdWI2N6tRI
71s/4NhmNpjGGA1bBGTJ60=
Encryption
Data concealment
Encrypted Stego-Image
Performance analysis
MSE, PSNR, correlation
time& elapsed time

Fig 11: Process flow diagram for data encryption and embedding

4. RESULT AND ANALYSIS

The Proposed work is coded and tested in a system installed with MATLAB R2010a.Test images namely Lena, Baboon, Tulip and satellite images etc, each of size 256×256 were used. The receiver has both decrypting key for data and image decryption and the PSNR of all directly decrypted images were observed to be above 48.13dB. The recovered image is exactly same as the original image as in [11]. As compared to [11], the proposed method yields a better result. For e.g. PSNR for Lena image yields 67.17dB but proposed paper yields 68.70dB. Also [11] used 8-bit gray scale image where as proposed method used true color image of 24 bit giving an advantage in hiding.

Following sessions will explain the obtained results in different phases of the algorithm.

4.1 Image Results

Fig 12 shows the transformation of image at different stages in proposed algorithm while passing through different phase of algorithm. First column describes the original input color image taken at the content owner side. Second column is the blue plane image of the original true color (RGB) image. This is obtained during the plane separation process at the same content owner site. The third column is the encrypted image resulting from the chaos encryption. Pixels of the original color input image is shuffled with respect to chaos sequence generated with defined key called encryption key. The fourth column is the Encrypted stego-image resulting after the bits of secret data is embedded in the reserved place of encrypted image .This Encrypted stego-image is obtained from the data hider module. Before embedding into encrypted image the data is also encrypted for strong security purpose. Encryption process is hence completed here. Next is the decryption part. Using the appropriate data hiding key, receiver or the content owner can now extract and decrypt the text also can decrypt the original image i.e. retrieved losslessly.

Original Input Image/ **Cover mage**	**B-Plane**	**Transformed /** **Encrypted Image**	**Encrypted stego-image**	**Recovered image**

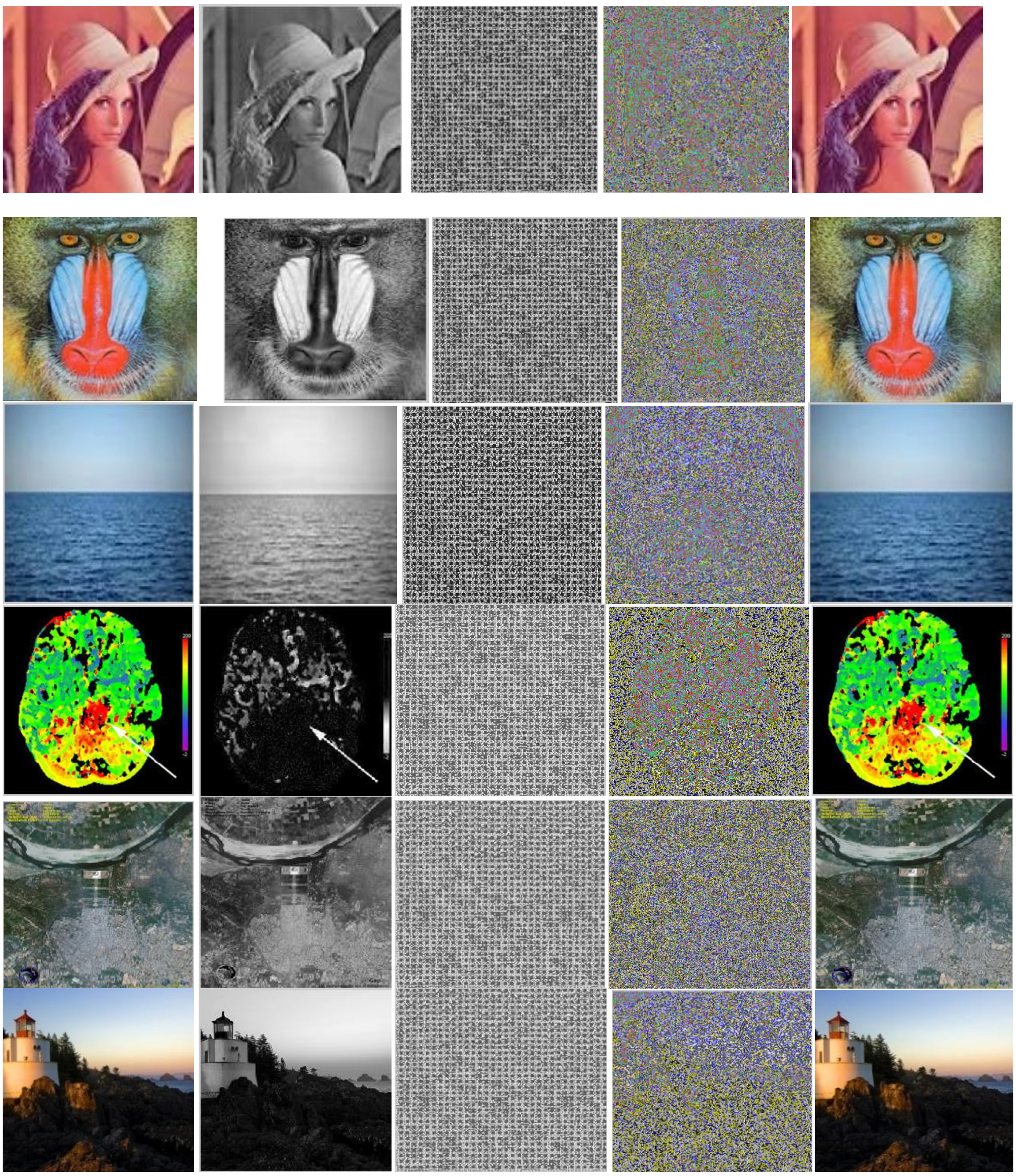


Fig 12: Images obtained at different stages of proposed algorithm

Most suitable is haar wavelet since other wavelets like debauches db2, db3 etc, slantlet, morlet etc distorts the original cover after data is extracted.

For say result of recovered image from haar and db2 is as follows:

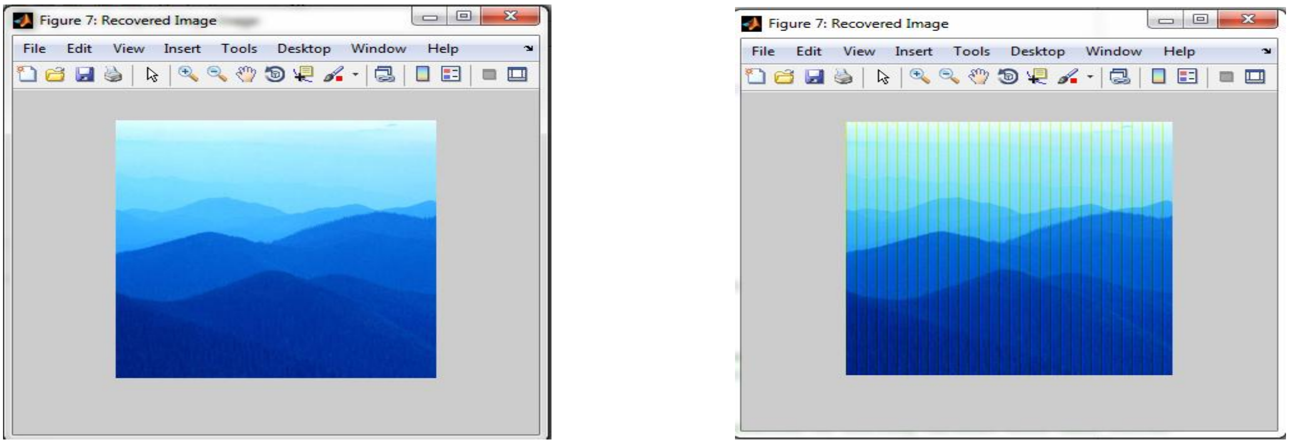


Figure 7: Recovered Image
File Edit View Insert Tools Desktop Window Help
Figure 7: Recovered Image
File Edit View Insert Tools Desktop Window Help

(a) **(b)**

Fig 13.1: scenery image (a) Recovered original image using haar (b) Recovered original image using db2

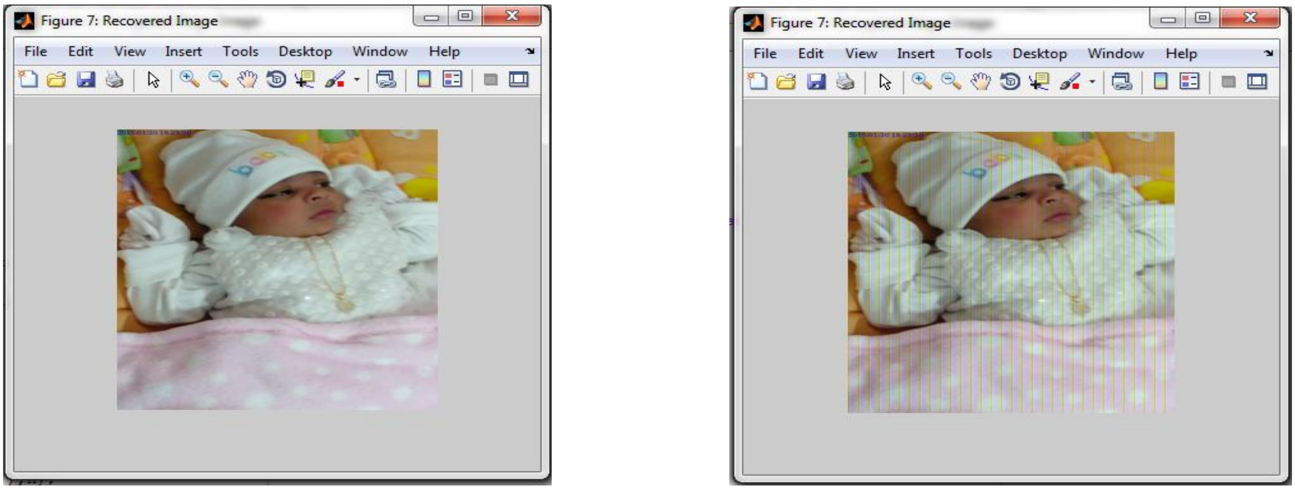


Figure 7: Recovered Image
File Edit View Insert Tools Desktop Window Help
Figure 7: Recovered Image
File Edit View Insert Tools Desktop Window Help

Fig 13.2: Aizah image (a) Recovered original image using haar (b) Recovered original image using db2

This is because the data is camouflaged in Encrypted image and not plain image; the resulting recovered image gets distorted using wavelets other than haar. Also problem comes in floating point conversion.

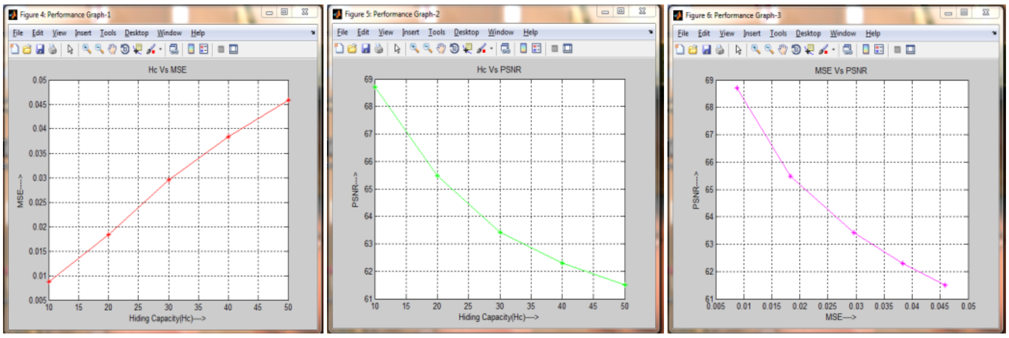
Table1: Performance analysis of cover image: PSNR, MSE, Correlation time and elapsed time

Sr. No.	Cover/ Input image	MEAN	PSNR	Correlation Time	Elapsed Time
1	lena.tif	0.008	68.70	0.002	5.4374
2	Pepper.jpg	0.0135	66.8262	0.0028	6.6845
3	Scenary.jpg	0.0024	74.3090	0.0012	7.4981
4	Light house.jpg	0.007	69.583	0.0023	5.6273
5	Tulip.jpg	0.019	65.2507	0.0018	5.5315

Justification: Above table just shows the different PSNR, MSE, Correlation time and Elasped time for each input cover image. As all cover images are different.

Performance analysis curve for different images

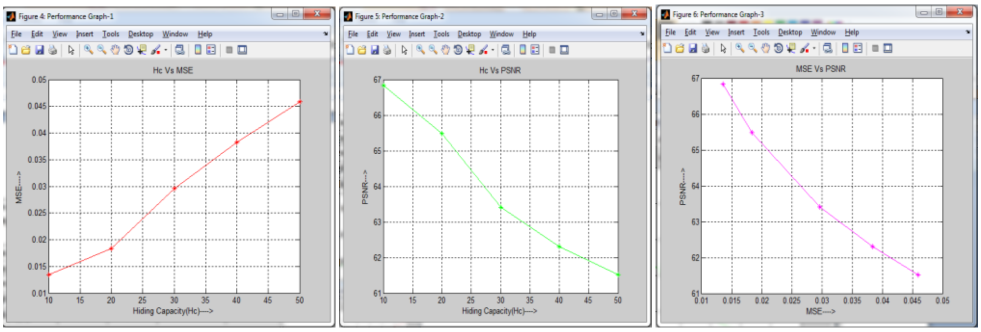
Image 1: Lena Fig



(a) HC vs MSE (b) HC vs PSNR (c) MSE vs PSNR

Fig 14.1: Performance analysis curve for Lena image.

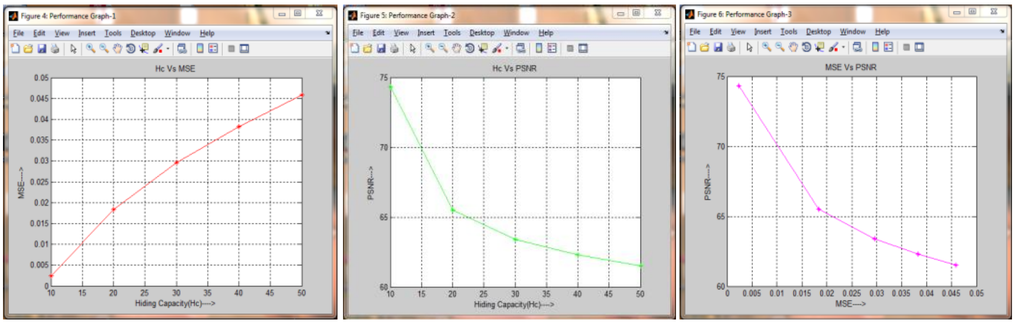
Image 2: Pepper



(a) HC vs. MSE (b) HC vs. PSNR (c) MSE vs. PSNR

Fig 14.2: Performance analysis curve for Pepper image.

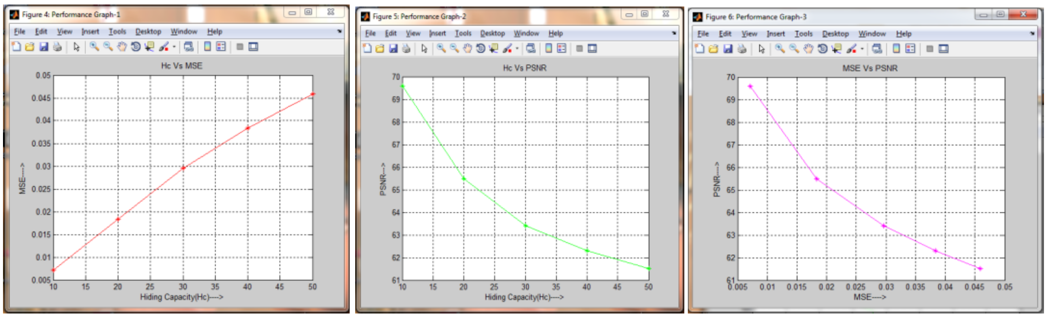
Image 3: scenery



(a) HC vs. MSE (b) HC vs. PSNR (c) MSE vs. PSNR

Fig 14.3: Performance analysis curve for Scenery image.

Image 4: Light house



(a) HC vs. MSE (b) HC vs. PSNR (c) MSE vs. PSNR

Fig 14.4: Performance analysis curve for Light house image.

Finally, the stimulated result shows that the performance of system was evaluated with quality metrics such as Mean square error, PSNR, Correlation time and Elapsed time. For Each input the performance curve is different. This is due to difference in texture of each input image. Also as PSNR is inversely proportional to MSE, So as MSE decreases PSNR increases and vice a versa. Similarly, as No. of Payload decreases so will be decrease in MSE and hence PSNR will increase.

Let's see an example for Lena image.

Table 2: PSNR vs. Payload for Lena image

Case	No. of character	Character	Payload(no. of bits)	PSNR	MSE
1	20	Abcdefghij1234567891	696	66.6814	0.014
2	10	hjfkd12345	376	69.2199	0.007
3	5	amr12	152	73.2853	0.003
4	20	Abcdefghijklmnopqrst	696	65.8112	0.017
5	10	hjfkdltige	376	68.7065	0.0088
6	5	Amrin	152	72.0631	0.0040
7	3	Cat	88	73.9911	0.0026

Justification: From the standard formula of PSNR and MSE, it can be seen that PSNR is inversely proportional to MSE. AS seen in above table refer case 4, 5, 6 and 7 as the number of character of secret data is decreased i.e. the Payload which results in decrease of MSE. Hence, less character means less error and more character means more error. So less MSE means high PSNR. Above table is carried out for the same Lena.jpg image.

This means it's possible to vary the PSNR from low to high by just decreasing the payload.

Table 3: Performance analysis on low component, high component, low contrast and high contrast

Case	**Image Name**	**Type of image**	**PSNR**	**MSE**
1a	Low contrast6	Low contrast image	69.7828	0.0068
1b	Low contrast2	Low contrast image	67.7891	0.010
1c	Low contrast3	Low contrast image	70.3627	0.0060
2a	Bird	High contrast image	68.08	0.0101
2b	High contrast5	High contrast image	67.7042	0.011
2c	High contrast 3	High contrast image	67.9961	0.0103
3	Aizah	Facial image	64.9379	0.020
4	Satellite2	Satellite image	65.2507	0.0194
5	Sea	Flat image	70.6608	0.005

Justification: From the above table it can be seen and judge that if the input cover image is a low component image as sea image the better is the PSNR compared to high component image like satellite image, checker image.

Compared to high contrast image, low contrast is much better refer to compare 1a, 1b and 1c with 2a, 2b and 2c where 69.7828dB and 70.3627dB are higher PSNR of low contrast as compared to high contrast respectively.

Comparing to crowded image like satellite, flat image is much better with 70.6608dB as higher value. Flat image has highest PSNR with reference to above table.

Table 4: Performance analysis on satellite images.

Sr. no.	Types of satellite imagery/ name	PSNR	MSE
1	Geoeye1-Tajmahal	64.6283	0.0224
2	Geoeye1-Disneyland-tokyo japan	65.2473	0.0194
3	Quickbird-brussel-HR	65.4036	0.0187
4	Quickbird-ukraine	66.2869	0.0153
5	Worldview-2-dallas-texas	65.4677	0.0185
6	Worldview-2-Sydney	66.9607	0.0131
7	Pleaides-1-beijing-china	68.0349	0.0102
8	Pleaides-1-dubai	68.6464	0.0089

Justification: Above table shows analysis on different satellite images. All satellites images are High resolution images .It can be concluded that pleaides-1 shows better result comparatively. Pleaides-1-dubai shows minimum error and highest PSNR

Table 5: Performance analysis on different color medical images:

Case	Type of image	Name of image	PSNR	MSE
1	X-ray image.	X-ray-Human-color	69.6680	0.0070
2	CT-scan	Color-CT-scan-thrombolysis	69.7828	0.0068
3	Ultra sound image	3D-ultra sound	69.7828	0.0068
4	MRI scan	Brain scan	69.7828	0.0068

Justification: Compared to [17], the proposed method can be used in medical applications with better PSNR. Above table shows almost same PSNR for all Medical images given in above table.

Applications: Reversible data hiding today has wide applications where ever secure communication is expected. The fact is all this algorithm mite give you 100% security but always an individual can make their personal data secure by making it secure by themselves i.e. 90% of security can be made by individual with proper knowledge.

1) Tamper proofing: Tamper proofing is done to protect modification of software or hardware. It also saves them from illegal distribution. Even in digital images the modification of image is possible.

2) Medical image: Data such as patient's information is hidden into the medical image example: X-ray, CT-scan etc; Patients information such as

Gender, name, address, health issue, date of admission and discharge to hospital

3) Copy right protection: There are lots of images available on the internet. But some are copy right protected. Image can be copyrighted with just an invisible watermark. For more robustness it is embedded securely with the proposed technique.

4) Identity information in banks, colleges etc- This include Debit card-Credit card PIN, date of birth, Monthly income information, Address etc.

5. CONCLUSION AND FUTURE SCOPE

Conclusion

Punching line of the above proposed work is RDH which is done in encrypted images by vacating room before encryption because by doing so the room will be spacious giving an advantage of hiding the data effortlessly using lifting wavelet transform and chaotic crypto system to protect image content for say patient's medical report with LSB based data concealment. For more robustness and security both Data and Image are encrypted. Image is encrypted using chaos encryption and Secret Data is encrypted using RSA asymmetric key encryption. Haar wavelet is used for transformation. Since original image is also encrypted, the best wavelet is Haar. Using other wavelet is not possible as per our experiment because they don't yield a better result and there are some wavelets that degrade the original image refer Fig 13.1 and 13.2. This is because for data hiding other wavelets can be used only if the original image is plain image. If the original image is encrypted then applying wavelet other than haar results in distortion of the recovered image. Haar is simple to use, compactly supported, orthogonal, symmetry and results good quality image. Also there is problem in conversion of floating point into integer values. Daubechies wavelet is a family of wavelet where db1 is same as haar. The limitation in using Debauches (other than db1) and Coiflet is asymmetric that may cause artifacts at the border. Even Contourlet may be possible to use in stegnanography where the image is a normal image. Mostly embedding process is based on integer points and wavelets are based on floating value hence difficulty comes in conversion. The project presented protection of image quality that can be understood from PSNR and MSE. Also the above project shows Flat cover image like Sea image is best then high component image like satellite.

Hiding capacity is also measured. This system generated the stego image with less error under maximum data hiding capacity. It was better compatible approach and flexibility with better efficiency rather than prior methods in terms of high hiding capacity with minimum error rate.

Choosing a color image that is flat image like sea and hiding as low payload as possible can improve the PSNR of the image. Proposed method also showed how PSNR is dependent on Payload length. Also hiding the encrypted data into the cover image before encryption enhances security. Finally when the cover image is losslessly recovered it is an added advantage of proposed method.

The proposed method achieves better performance in reversibility, original image recovery at receiver without any loss of information rather than traditional methods. Also this paper concludes Haar wavelet is best suitable in the case where the Original image is encrypted one. This novel technique of Reversible data hiding can be deployed in any field may be medical, military or law enforcement etc. or any other where rendering of original image is desired or required.

Future scope

Reversible data hiding can be applied to video file or encrypted video file. New technique in reversible data hiding in encrypted images with better PSNR and min error along with increasing payload must be found.

6. ACKNOWLEDGEMENTS

I would like to express my profound gratitude to my co-guide Dr.Imdad Rizvi and my guide M.M Kadam for all guidance throughout my research. They being my guide is a feeling of proud. My parents and dear ones too were the back bone of my hard work. Special thanks to my friends.

7. REFERENCES

[1] A.M. Alattar. 2004. Reversible watermark using difference expansion of quads. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 3, (May 2004), 377–380,4pagesDOI:http://dx.doi.org/10.1109/ICASSP.2004.1326560

[2] J. Tian. 2003. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology 13 (8), (August2003), 890–896,7pagesDOI:http://dx.doi.org 10.1109/TCSVT.2003.815962

[3] Princy Raj and sreekumar k. 2014. A Survey on Reversible Data Hiding in Encrypted images. International Journal of Computer Science and Information Technologies, 5 (6),(2014),77487751.http://www.ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506187.pdf

[4] Sukhdeep kaur and manshi shukla. 2014. Reversible Data Hiding and its Method: A Survey. International Journal of Computer Science and Mobile Computing, 3 (5), (May 2014), 821-826. http://ijcsmc.com/docs/papers/May2014/V3I5201499a60.pdf

[5] M. Arslan, S.A. Malik and A. Khan. 2012. Intelligent reversible watermarking in integer wavelet domain for medical images. Journal of Systems and Software 85(4), (April 2012)) 883–894.DOI:http://dx.doi.org/10.1016/j.jss.2011.11.005

[6] M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber. 2005. Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing 14 (2), (Feb 2005), 253–266.DOI:http://dx.doi.org /10.1109/TIP.2004.840686

[7] Masoud Nosrati, Ronak Karimi and Hojat Allah Hasanvand. 2012. Spatial and Transform Domains RDH Methods. World Applied Programming, 2(6), (June 2012), 373-376, ISSN: 2222-2510 ©2011 WAP journal. www.waprogramming.com.http://waprogramming.com/papers/50af8125c1b596.75214390.pdf

[8] X. Zhang. 2011. Reversible data hiding in encrypted image. IEEE Signal Process. Lett., 18(4), (Feb 2011), 255–258.DOI:http://dx.doi.org /10.1109/LSP.2011.2114651

[9] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari. 2012. Performance Evaluation of Cryptographic Algorithms: DES and AES. IEEE Trans. on Electrical, Electronics and Computer Science, (March 2012), 1-5.DOI:http://dx.doi.org /10.1109/SCEECS.2012.6184991

[10] P. Tsai, Y. C. Hu, and H. L. Yeh. 2009. Reversible image hiding scheme using predictive coding and histogram shifting. In Signal Process, 89(6), (June 2009), 1129–1143.DOI:http://dx.doi.org /10.1016/j.sigpro.2008.12.017

[11] Kede Ma, Weiming Zhang and Xianfeng Zhao. 2013. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. Inf. Forensics Security, 8(3), (March 2013), 553-562.DOI:http://dx.doi.org/10.1016/j.sigpro.2013.06.023

[12] T. Kalker and F.M.Willems. 2002. Capacity bounds and code constructions for reversible data-hiding. In Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 71–76.DOI: http://dx.doi.org/10.1106/icdsp.2002.1027818

[13] J. Fridrich and M. Goljan. 2002. Lossless data embedding for all image formats. In Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA,4675,572–583.DOI:http://dx.doi.org /10.1117/12.465317

[14] W. Zhang, B. Chen, and N. Yu. 2011. Capacity-approaching codes for reversible data hiding. In Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, Springer-Verlag, 255–269.DOI:http://dx.doi.org /10.1007/978-3-642-24178-9_18

[15] Sushil Kumar and S.K. Mutttoo. 2011. Steganography based on contourlet transform. (IJCSIS) International journal of computer science and information security, 9(6), 215-220.

[16] Sushil Kumar and S.K. Mutttoo. 2013. Image Steganography based on wavelet families. Journal of Computer Engineering and Information Technology, 2(2), 1000105.DOI:http://dx.doi.org/10.4172/2324-9307.1000105

[17] Muhammad Arsalan, Sana Ambreen Malik and Asifullah Khan. 2012. Intelligent reversible watermarking in integer wavelet domain for medical images. The Journal of Systems and Software 85, 883–894.DOI:http://dx.doi.org /doi:10.1016/j.jss.2011.11.005.