Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

Research Paper

Robust Method of Data Hiding Using Reserve Room Approach Based on Haar.

Engineering

KEYWORDS : Reversible data hiding, chaos encryption, LSB replacement, RSA key encryption, Haar Wavelet transform

Khan Amrin naaz	Department of Electronics and Telecommunication Engineering, Terna engineering college, Mumbai, Maharashtra, India
Dr.Imdad Rizvi	Department of Electronics and Telecommunication Engineering, Terna engineering college, Mumbai, Maharashtra, India
Prof. M. M. Kadam	Department of Electronics and Telecommunication Engineering, Terna engineering college, Mumbai, Maharashtra, India

ABSTRACT

Much progress can be seen till today. Earlier it was simply data hiding then reversible data hiding and now its Encrypted data hiding. In this paper Encrypted Data is hidden in Encrypted image using Reserve Room Approach is done based on texture analysis with Haar wavelet is proposed here. Another big question is the compression part. Even though wavelet transform are widely used ther is still a question mark , which one to use. In this paper we analyze some of them like symlet, biorNr.Nd, coiflet and contourlet and found Haar wavelet is much effiecient.

The quality of image has been evaluated using factors like MSE, PSNR and Hiding capacity. generated minimal error with high SNR rate at various data hiding capacity.

I. INTRODUCTION

With the growth of ways of communication ,there must also be growth in ways of communication securely ie the techniques for secure communication. Data hiding has been an interesting topic since the early 1990's . Every one wants to communicate securely. But how ? is a big question mark. There are several ways to communicate secretly for eg: Cryptography, stegnanography and water marking technique. Many applications of such communication such as law enforcement, Military and Medical application require not only to communicate securely but to restore the original cover image. Hence the need for Reversible data hiding. There are Reversible and Irreversible data hiding techniques. Irreversible data hiding means once embedded data is , the original image is lost but in Reversible the original image or the cover image is recovered. extracted and hence has attracted more and more attention in both researches and application. Data can be hidden in color or grey scale images. Color images improves Hiding capacity. Again further reversible data hiding comes with two approach (1) Reversible data hiding by vacating room after encryption (VRAE): All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. (2) Reversible data hiding by vacating room before encryption (RRBE) : Here instead of vacating the room after encryption , a space is reserved for embedding the data before encryption. In this process for image compression wavelet is best suited but which one to chose is a challenging part ie actually depends on application , image quality and computational complexity.

II. LITERATURE REVIEW

In [1] existing, pixel difference expansion based Reversible data hiding (RDH) is the spatial domain process to conceal secret text messages within a cover image. This will be overcome by the method of least significant bit replacement algorithm. The Reversible data hiding in encrypted image is investigated in [2] this system is still improved with encrypt messages using an asymmetric key method. This is the reason a new security approach called reversible data hiding arises. It is the way of hiding the existence of data in another transmission medium to achieve secret communication. The application of Reversible data hiding are such as medical images, military electronic data, remote sensor data, or any host image should not be permanent distortion after extracting the embedded data [3]. In Vacating room after encryption, the secret messages are concealed into encrypted domain by replacement of some pixel intensities. Also Vacating room from the encrypted images losslessly is relatively difficult and also sometimes inefficient and hence we proposed reversible data hiding before encryption. Image encryption using AES algorithm [5] converts original image into cipher form. The system uses reserve room before encryption approach [6] to overcome the problem of prior methods such as vacating room after encryption and pixel difference expansion. This spatial domain technique [6] distorts an image quality wherever the secret message bits were hidden. With the consideration of these problems, the system proposes the reserve room approach with lifting wavelet transformation for preserving an image quality and improve the security of 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 is insensible region for human visual system. [7] Kede Ma, Weiming, Xianfeng Zhao modified the VRAE using reserve room approach. It reduces the image artifacts and still it fails to reconstruct an image with free of loss due to data hiding under spatial domain. In [8], J. Tian uses pixel differences expansion for reversible data hiding, the secret digits will be concealed in the differences of neighbouring pixels by increment or decrement the difference. It causes an algorithm complexity and high error rate at minimum hiding capacity. With the consideration of these problems, proposed system chooses reliable and flexible methods to overcome this constraints and yields better quality during image reconstruction after the extraction of embedded data.

In [9], X. Zhang proposes the reversible data hiding approach based on vacating room after encryption. In this method, the content owner encrypts the original image and it hand over to data hider. The data hider hides secret data by replacing some encrypted pixels causes image distortion at data recovery.

In [10],Kalker and Willems found a rate-distortion model for Reversible data hiding, and proved that rate-distortion bounds of RDH for memoryless covers and also proposed a recursive code construction which, however, does not approach the bound .In [11] J. Fridrich and M. Goljan constructed a general framework for RDH. Authors first extracted compressible features of original cover and then compressed them losslessly so that spare space can be saved for embedding auxiliary data. W. Zhang, B. Chen, and N. Yu in [12], [13] worked to improve the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression

Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers. In [20-21] Authors chose contourlet and slantlet for stegnanography but the image is plain and not encrypted. Nowhere the author has mentioned about encrypted image. Our present paper this is not possible because of the cover image is encrypted.

III. DESIGN THEORY

The Proposed reversible data hiding approach is done based on reserve coefficients before encryption under transformed domain. Here the image is 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 encryption technique here uses the key to encrypt an image and not only 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 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. Also in[19] , the result shows that Haar wavelets are best for the imperceptibility and security of image as compared to other wavelets. Although encryption has security effects, they make the secret messages unreadable and unnatural or meaningless. In addition with this approach, of chaos crypto system, adaptive least significant bit replacement will be used for image encryption and message embedding. In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted pixels to extract the data. By using the decryption keys, the image and extracted text data will be extracted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery. Data recovery is the reverse process of the encryption and embedding to get lossless extracted image and messages. In [19] says the conventional wavelet filters often have floating point co-efficient and couldn't realize lossless reconstruction. The second generation wavelet transforms are based on lifting scheme and they map integer to integer. Thus they realize the lossless compression of image data with minimal memory usage and low computational complexity.

1. LIFTING WAVELET TRANSFORM

Lifting wavelet transform is the second generation transform. Lifting scheme was introduced by wim sweldens for constructing bi-orthogonal wavelets. Lifting scheme is basically used to design wavelets and to perform discrete wavelet transform, where this wavelet transform is widely used in signal processing and in image compression research. They map integer to integer.

Algorithm for lifting wavelet scheme.

- First splits data into odd and even functions.
- Predict odd set from even set.

- to ensure polynomial cancellation in high pass.
- Update even set using wavelet coefficients to calculate scaling functions.

- It is done to ensure preservation in low pass.

Advantage of lifting scheme.

- Faster implementation of wavelet transforms.
- Requires half computation as compared to traditional convolution based discrete wavelet transform.
- Very efficient for real time low power application.
- Allows reversible integer wavelet transform.
- Perfect reconstruction is possible for loss- less compression.

DWT has the ability to transform an image into frequency domain from spatial domain.

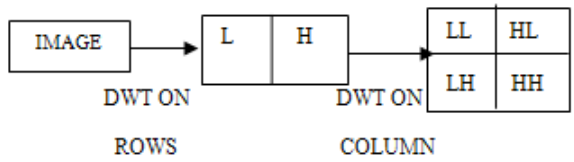


Fig1 : *Application of DWT on Input image*



Fig2 a) Original image and b) Image after wavelet decomposition.

Forward transform

Step1: Column wise processing to get H and L

H = (Co-Ce); L = (Ce+*H*/2)

Where Co and Ce is the odd column and even column wise pixel values

Step 2: Row wise processing to get LL,LH,HL and HH, Separate odd and even rows of H and L,

Namely, Hodd – odd row of H, Lodd- odd row of L, Heven- even row of H

Leven – even row of L

LH = Lodd-Leven; LL = Leven + (*LH* / 2)

HH = Hodd – Heven; HL = Heven + (*HH* /2)

Reverse Lifting scheme

Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

LWT uses to decorrelate the pixels into two kinds of frequency subbands such as low frequency 'L'contains structural components (image approximation) and high frequency 'H'contains textural components (Image sharpening). These detailed coefficients called sharpening details utilized to reserve it for efficient data hiding.

1.a Wavelet families and choice of correct one:

The wavelet transform has a short but spectacular history. It has been the subject of much research in the 1980s and 1990s and has found many applications in the fields of digital signal processing, data compression, and communications. The wavelet transform concentrates the fine image details in the HH, HL, and LH subbands. Specifically, information about edges and textures is concentrated in those sub bands. It is known that the eye is sensitive to small changes in a uniform area. If even one pixel is modified in an otherwise uniform area, it sticks out and is easily visible. On the other hand, if one pixel in a sharp edge is modified, it is harder for the eye to notice it. This means that adding the watermark components to the wavelet coefficients in subbands HH, HL, and LH affects mostly image features such as

edges and can be made visually imperceptible [18]

Wavelet families	Wavelet name
Haar	Haar
Daubechies	Db1
Symlets	Sym
Coiflets	coif
BiorSplines	bior
ReverseBior	rbio
Meyer	meyr
DMeyer	dmey
Gaussian	gaus
Mexican_hat	mexh
Morlet	morl
Complex Gaussian	cgau
Shannon	shan
Frequency B-Spline	fbsp
Complex Morlet	cmor

Fig3Reference from matlab

Wavelet	Compactly supported orthogonal	Compactly supported bi-orthogonal	Symmetry	Fast Computation	Vanishing Moments	Filters
Bior <Nr.Nd>	No	Yes	Yes	Yes	Arbitrary	FIR
Coif<N>	Yes	No	Near	Yes	Arbitrary	FIR
Db<N>	Yes	No	No	Yes	Arbitrary	FIR
Haar	Yes	No	Yes	Yes	Two	FIR
Meyer	No	No	Yes	No	Infinite	FIR
Sym<N>	Yes	No	Near	Yes	Arbitrary	FIR

Fig 4 Reference from matlab and [19]

1.a HAAR WAVELET TRANSFORM

Haar wavelet was introduced in the year 1910 by Alfred Haar. Haar transform is very simple to perform with good speed of computation. There are two co-efficient of haar wavelet ie one from coarse approximation calculated by averaging two adjacent samples. Other is fine detail calculated by subtracting two adjacent samples. Haar transform also involves forward and reverse transform. In forward transforms, computation of scaling co-efficient (φ) is calculated by adding two adjacent sample values and divide by 2. Whereas, computation of wavelet co-efficient (φ) is calculated by subtracting two adjacent samples values and divide by 2. Also haar wavelet can be easily applied to encrypted images.

2. IMAGE ENCRYPTION

It is 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. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bitxor operation.

Here logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The chaotic systems are defined on a complex or real number space called as boundary continuous space.

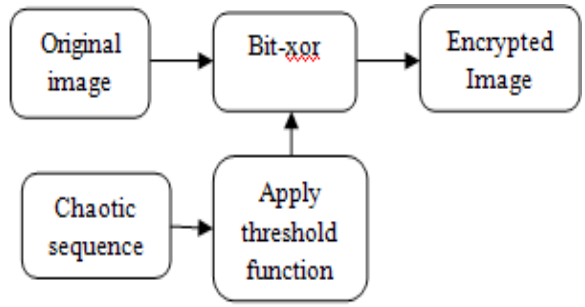


Fig 5: Process flow of Image Encryption using chaos crypto system.

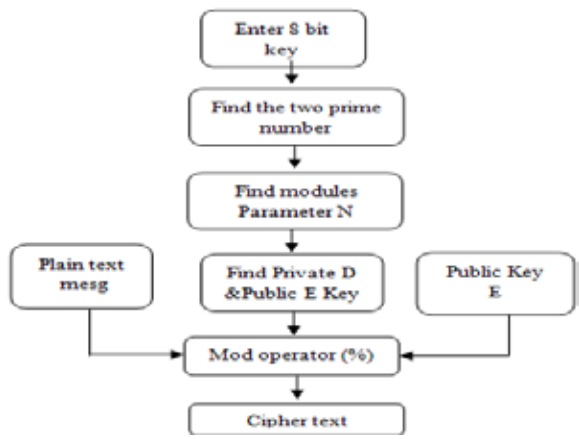


Fig 6: Text Encryption using 8-bit key

3. TEXT ENCRYPTION

Asymmetric key Cryptography

Cryptography allows secure transmission of private information over insecure channels (for example packet-switched networks). Cryptography also allows secure storage of sensitive data on any computer.

3.1 RSA – Public Key Cryptography

Public key (E) and Modulus *N* are known to all users. Private Key (D) (secret key) provides Authentication/Encryption Signing/Decryption operation Verifying/Encryption operation

3.1. a Data encryption will be done by,

Cipher_text= C. ^E mod N

N = p * q;

Where, C – Each Character of Input text message

N – Modulus parameter,

p & q – two largest prime number obtained from user given 8-bit key.

3.1.b Data decryption will be done by,

Plain_text = Cipher.^D mod N

4. DATA CONCEALMENT

Data concealment or hiding of data is done using LSB algorithm. Bits of the hidden message are inserted into the least significant bits of the pixels. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8 bits. One

Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

pixel can hence display 2^8=256 variations. The weighting configuration of an 8-bit number is illustrated. The basic concept of LSB substitution is to embed the confidential data at the right most bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB method is: x represents the i th pixel value of the stego-image, i x represents that of the original cover-image, and i m represents the decimal value of the i th block in confidential data. The number of LSBs to be substituted is denoted as k. The extraction process is to copy the k-rightmost bits directly. A simple permutation of the extracted i m gives us the original confidential data. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results. Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly.

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible. The quality of the image however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

5. PROCESS FLOW

Embedding:

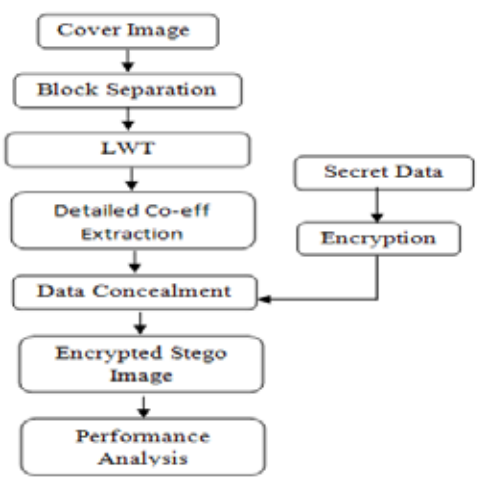
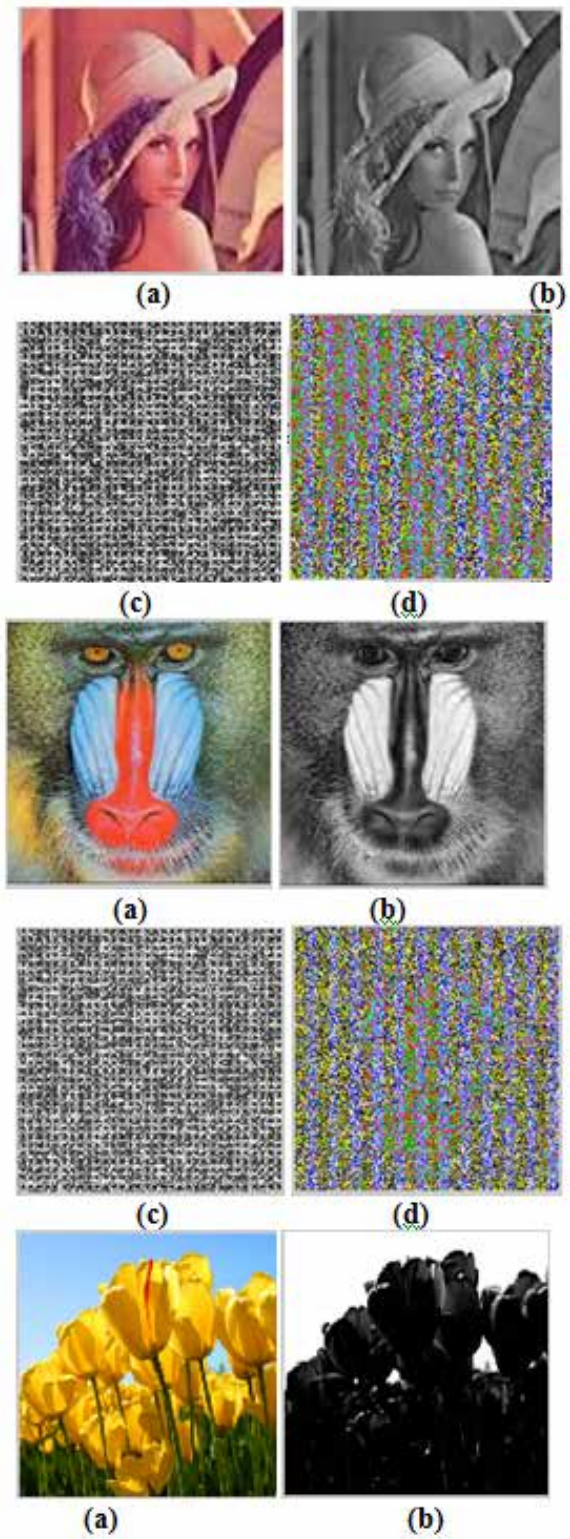


Fig 7 Process flow of Proposed work

RESULT AND PERFORMANCE

In this paper 4 Images were used to evaluate the performance of the proposed scheme



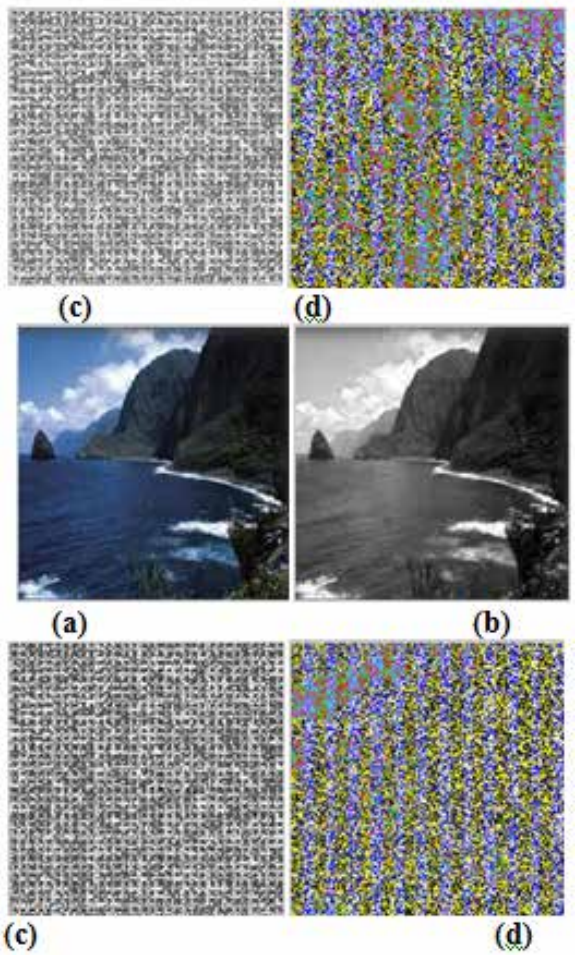


Fig 8:*(a)Cover/ Input image(b) B-plane or grey image(c)Transformed image (d)Encrypted stego image*

Fig : Output or Recovered images

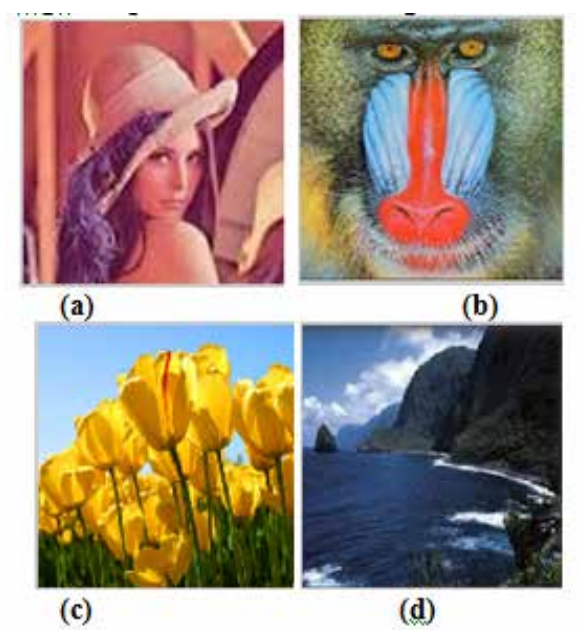


Fig 9: *(a), (b), (c) and (d) are the recovered images for the inputs of Fig7*

Fig 10: Example figure of Distorted Image



Fig11 : Concealed data output can be retrieved as

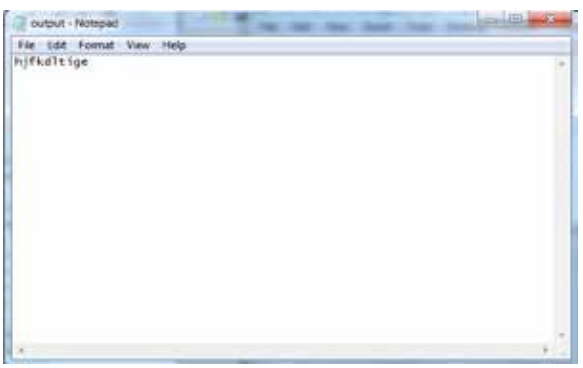
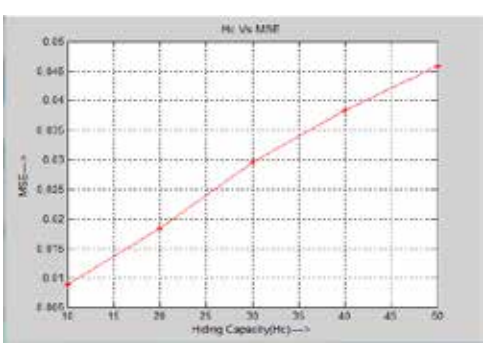


Fig 9: *concealed or hidden data*

The above concealed data can be retrieved in notepad. The hidden data was created and saved in a note pad as "message". The hidden data was extracted from the encrypted stego image and the output was seen in notepad saved as "output" The performance of the technique will be evaluated as following,

Fig: Performance analysis

Fig 10: *(a) Hiding capacity Vs MSE*



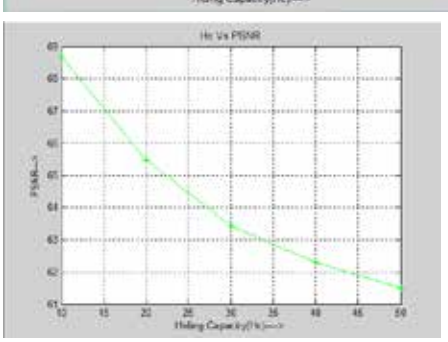


Fig 10:*(b)Hiding Capacity Vs PSNR*

Volume : 4 | Issue : 6 | June 2015 • ISSN No 2277 - 8179

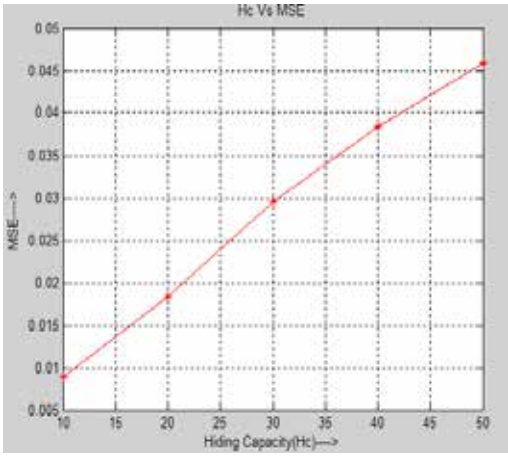


Fig 10: (c) MSE Vs PSNR

Table
Comparison of MSE, PSNR,Correlation time and Elapsed time.

Sr. No.	Cover/ Input image	MEAN	PSNR	Correlation Time	Elapsed Time
1	Lena. Tif	0.0025	74.1472	0.0029	7.7934
2	Baboon.tiff	0.0272	63.7021	2.8969e-004	7.4989
3	tulip.jpg	0.0015	76.3393	-0.0048	7.5241
4	4.jpg	5.3406e-004	80.0631	0.0012	7.8935

CONCLUSION

Our proposed work is RDH 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. For more robustness and security both Data and Image are Encrypted. Image is Enrypted using chaos encryption and Secret Data is encrypted using RSA asymmetric 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 doesn't yield a better result and there are some wavelets that degrades the original image. This is because for data hiding other wavelets can be used only if the original image is plane 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. Dabauchies wavelet is a family of wavelet where db1 is same as haar. The limitation in using Dabauchies and Coiflet is asymmetric that may cause artifacts at the border. Even Counterlet 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 coversion. The project presented protection of image quality that can be understand from PSNR and MSE . Hidden data during transmission is based on approach of reserve room technique by reserving space for concealing data effectively using lifting wavelet transform and chaotic crypto system to protect image content with LSB based data concealment.

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.

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 or not. 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.

REFERENCE

[1] "High Capacity Reversible Data Hiding with Adjacent-Pixel-Based Difference Expansion," in innovative computing, information and control (ICICIC) ,in 4th Int. Conf ,2009,pp.23-25 | [2] Chyuan-Huei Thomas Yang and Chun-Hao HsuA, " High Quality Reversible Data Hiding Method Using Interpolation Technique," in Fifth International Conference on Information Assurance and Security, 2009 | [3] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011. | [4] Xianting Zenga , Lingdi Ping and Zhuo Li , "Lossless Data Hiding Scheme Using Adjacent Pixel Difference Based on Scan Path," in Journal of multimedia, Vol. 4, No. 3, June 2009. | [5] Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Trans. on Electrical, Electronics and Computer Science, 2012. | [6] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," Signal Process., vol. 89, pp. 1129–1143, 2009. | [7] Kede Ma, Weiming Zhang, Xianfeng Zhao," Reversible data hiding in encrypted images by reserving room before encryption", IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, March 2013. | [8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003. | [9] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 826-832, April 2012. | [10] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76. | [11] J. Fridrich and M. Goljan, "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,Jan.2002,vol.4675,pp572–583 . | [12] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag. | [13] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012. | [14] "An Image Encryption Scheme Based on chaotic systems" IEEE Int. Conf on Machine learning and cybernetics, 2006. | [15]. J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U.S. Patent 5 646 997, 1997. | [16]. C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U.S. Patent 6 278 791, 2001. | [17]. B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO, Sept. 2000, pp. 533–536. | [18] Data Privacy and Security by David Salomon in Springer-Verlag ,New York (2003) | [19] Image Steganography Based on Wavelets Families by Sushil Kumar Azad and muttoo in journal of Computer Engineering and Information Technology () | [20]Stegnanography Based on contourlet Transform by Sushil kumar and S.K Muttoo in IJCSIS, Vol IX, No.VI,2011