Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 3, Pages 291-294, April 2017

Reversible Data Hiding Using Reserved Room Approach with Chaos Encryption

Selva Priya.P[1], P.Suba Shini[2] and Kishore Kumar[3]

[1]*UG Scholar, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India.*
[2]*Assistant Professor, Department of Computer Science and Engineering, SRM University, Chennai, Tamilnadu, India.*
[3]*Senior Assistant Professor, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, Tamilnadu, India.*

Article Received: 15 April 2017 *Article Accepted: 25 April 2017* *Article Published: 30 April 2017*

ABSTRACT

The project proposes the enhancement of secret data communication through hiding encrypted data into the encrypted images. Thus, the images are separated into blocks and then lifting wavelets is used to detect detailed coefficient. Then, that part is encrypted using chaos encryption. After encrypting the image, the secret data is concealed in h detailed coefficient which is already reserved before encryption. This is enhanced with encryption information with asymmetric key method. By this, a new security called reversible data hiding is developed. Thus, the adaptive Least Significant Bit replacement is used for concealing the secret message bits into encrypted images. In extraction method, the relevant key is used to extract data from the encrypted pixels. By the decryption key the performance will be analyzed with respect to data and images recovery.

Keywords: Reversible data hiding, Chaos encryption, LSB replacement and RSA key encryption.

1. INTRODUCTION

It is widely be used in the military and medical field for secret data communication. To overcome the problems in prior method this method undergoes reserved room before encryption approach. In prior methods VRAE and pixel difference expansion were employed. In existing, to conceal the secret text within the cover image pixel difference expansion were used. In data hiding adjacent pixels are subtracted to determine the difference values and histogram adjustment to reduce underflow and overflow error. Based on message bits the difference can be decremented or incremented. Thus, this method will be more compatible and complex one and leads to spatial distortion which in turn image quality will be degraded.

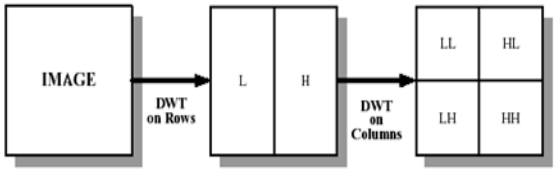
This can be overcome by the least significant bit replacement algorithm and lifting wavelet transformation can be used for preserving image quality. Decomposition of image into frequency subband will contains approximation and detailed coefficient. The reserving of coefficient from detailed coefficient will be based on Texture, edges and boundary regions.

For human visual system it is insensible. For image encryption and message embedding chaos crypto system and adaptive least significant bit replacement will be done. Thus, data recovery will be lossless. Thus, the result that is simulated will be in terms of metrics evaluation based on square error, peak signal to noise ratio and correlation coefficient.

2. METHODOLOGY

Lifting Wavelet Transform

The wavelet transformation had attained the widespread acceptance in processing of signals and particularly in images compression research. In many application DWT (discrete wavelets transform) had outperformed other coding schemes like DCT. Since, the image is need not to divide into non-overlapping blocks 2-D blocks, its function will have variable length, wavelet-coding schemes at higher compression ratios avoiding block artifacts. Because of their wavelets-coding schemes and inherent multi-resolution nature they are suitable for all applications where tolerable degradation and scalability are important. Now, JPEG committee has released, a new image coding standards, JPEG-2000 which is based on DWT.



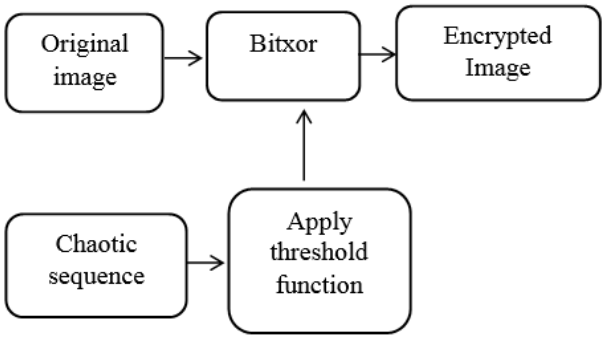
Forward transform

Step1: H and L by column wise processing H = (Co-Ce);L = (Ce+H/2)
Where, Ce and Co is the even column and odd column wise pixel values.
Step 2: Row wise processing to obtain HH, HL, LL and LH, Separate even and odd rows of L and H,
Namely, Heven- even row of H, Hodd – odd row of H, Lodd-odd row of L,
Leven – even row of L
LH = Lodd-Leven; LL = Leven + (*LH* / 2)
HH = Hodd – Heven; HL = Heven + (*HH*/2**)**
Reverse Lifting scheme
Reverse lifting scheme will form inverse integer wavelet transform. It is similar to perform forward lifting scheme.

3. IMAGE ENCRYPTION

This is the process of scrambling of original information into unknown form using asymmetric key or symmetric key standards were used. It will encryption the original pixels based on the encryption key value with respect to chaotic sequence and threshold function by bitxor operation.

© 2017 AJAST All rights reserved.



Chaotic sequence is generated from logistic map. This will prevent data hacking in unsecure channel during the transmission of secret images. The complex or real number spaces known as continuous spaces are defined as Chaotic system.

The chaotic sequence is given by, $C_{n+1}=U^{*}C_n*(1-C_n)$ and encrypted pixel form E=bitxor (P,C_{n+1}).

Fig.1.Cover Image

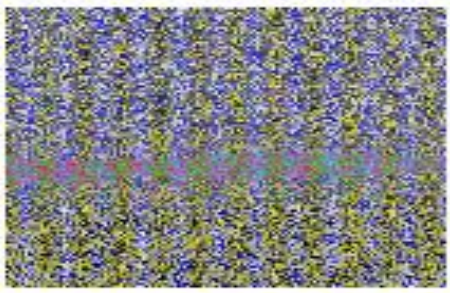


Fig.2. Encrypted Image

4. ASYMMETRIC KEY CRYPTOGRAPHY

The secured transmission of private information over the insecure channel are allowed by cryptography (example: packet-switched network). It means for secure storage of sensitive data on any computer.

RSA – Public Key Cryptography

Modulus N and public key are given to all users and private key(D)(secret key) provides Authentication/ Encryption Signing/ Decryption operation Verifying /Encryption operation data encryption Data encryption will be done by,

Cipher text = C.^E mod N

Where, C–Each Character of Input text message

N = p * q;

N=modulus parameter, p & q-two largest prime number from user given 8 bits. Data decryption will be done by,

Plain text = Cipher.^D mod N

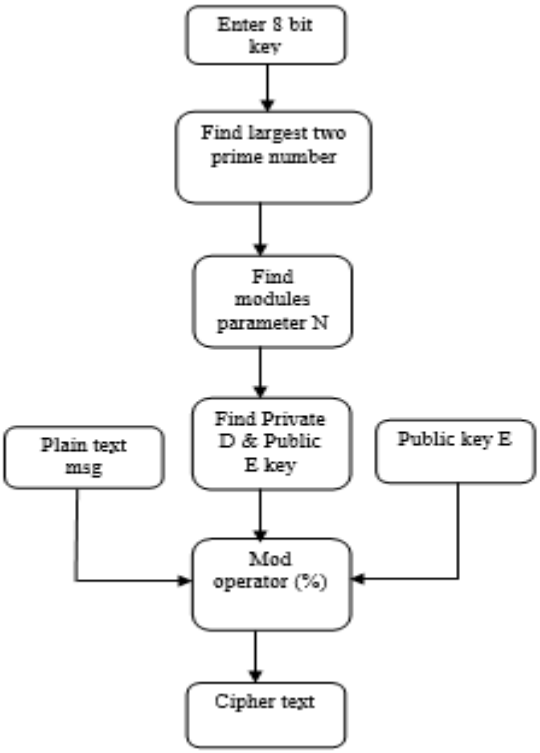


Fig.3. Encrypting the user given text.

5. DATA CONCEALMENT

The main objective of stegnography is to embed addition information over the digital contents which is undetectable to the listeners. We are investigating on its coding, embedding and detecting techniques. The LSB algorithm is based on inserting the bits of the hidden message into the least significant bits of the pixels. Since, there is an increasing practice of embedding data in digital multimedia sources are broadening, the groups of researchers including data hiding, steganography and digital watermarking. Off, these LSB substitution is widely used. Each pixel in gray-level image will consist of 8-bit. Thus, one pixel can display 2^8=256 variations. The 8-bit number, weighting configuration is illustrated. The concept of LSB is to embed the confidential data along the right most bit (bits with the smallest weighting). So, that original pixel value is not affected by embedding procedure. The mathematical representation for LSB method is: x represents that of the cover-original image, m and i are decimal values of the i^{th} block in confidential data. The LSB that are substituted is denoted by K. While extraction, process is done K-rightmost bits are copied directly.

Simple permutation of the extracted i , m gives us the original confidential data. This will be straight forward and easy. The image quality will be decrease a lot when capacity is greatly increased and hence suspected stego-image will results. By simply extracting the K-rightmost bit the confidential data might be easily stolen. The secret message will consist of K bits and 8bit gray scale matrix of m x n pixels. Thus, the first bits of message is embedded on LSB of

© 2017 AJAST All rights reserved.

first pixel and the second bit of message is embedded on second pixel and so on. The difference between the cover image and stego image are not visually perceptible. However, the image quality will be degrades with the increase in number of LSB. The error in between the input and output will be determined by mean square error and image quality is determine by the peak signal.

Process Flow

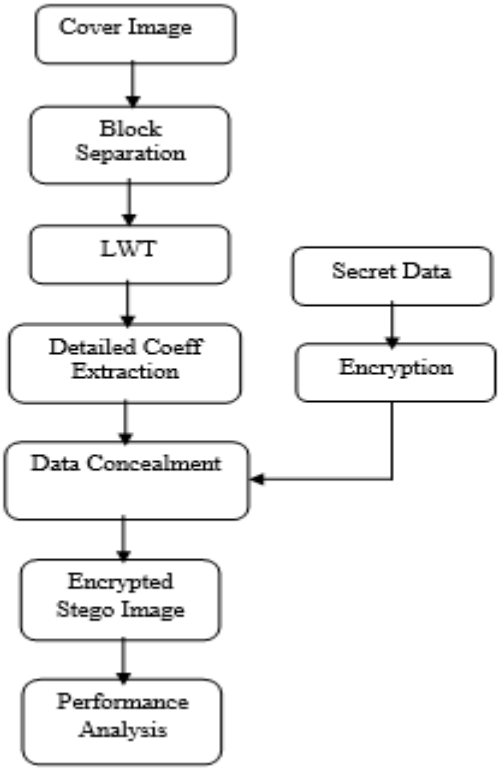


Fig.4. Embedding of Data in Image

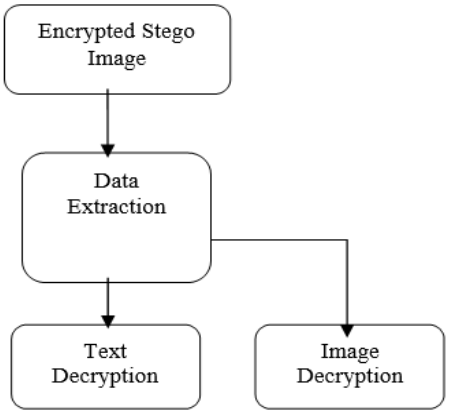


Fig.5. Extraction of Image and Text

Extraction Process

The information and embedded images are extracted by various decryption techniques like wavelet transform but in reverse process to get detailed coefficient and chaos decryption is done for decryption an image to recover transmission of data.

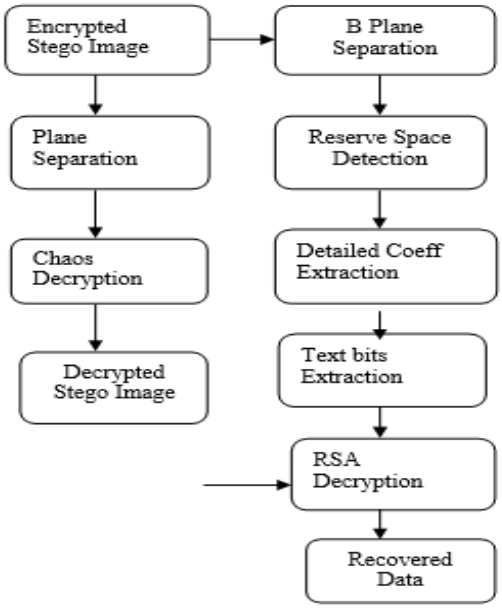


Fig.6. Image Decryption and Text Decryption.

Chaotic Decryption

The decryption key generated by the function can be attained by bitxor operation. The logistic map is used to attained the chaotic map. After getting the encrypted key value the next process is RSA decryption. By identifying the decryption key embedded text cab be extracted.

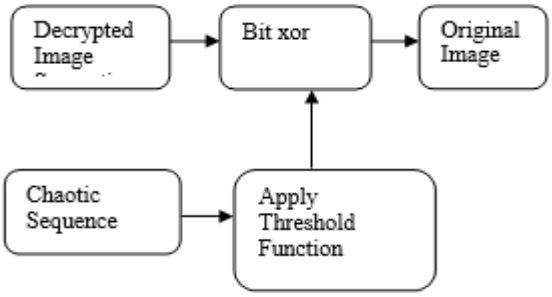
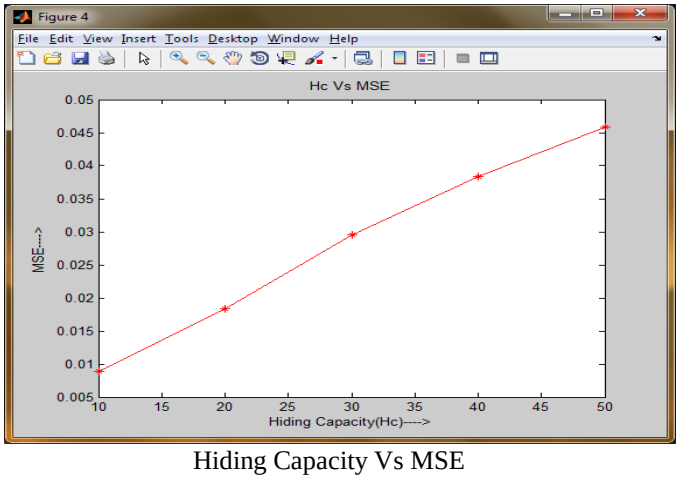


Fig.7. Chaotic Decryption

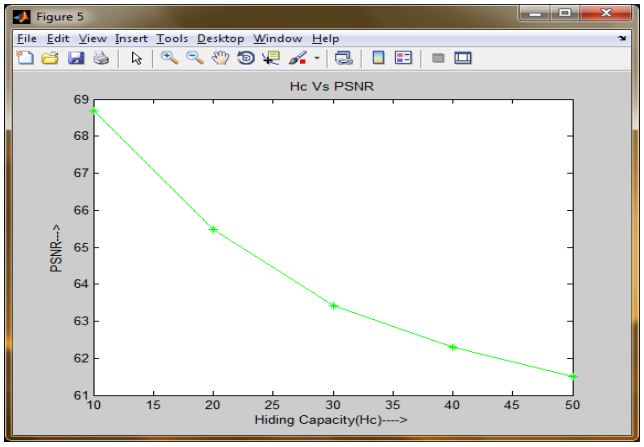
Performance Analysis

The performance of the technique will be evaluated as following,

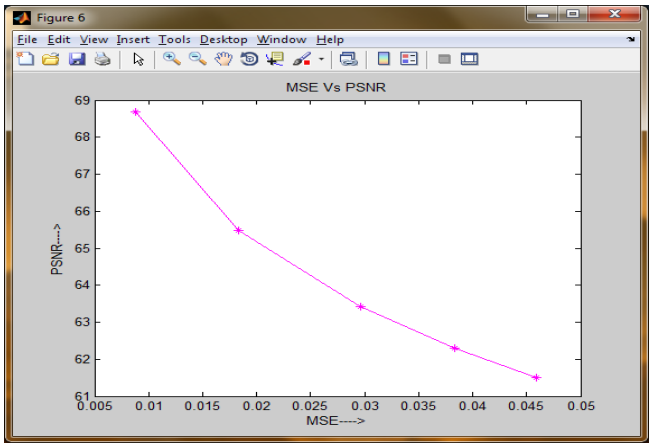


Hiding Capacity Vs MSE

© 2017 AJAST All rights reserved.



Hiding Capacity Vs PSNR



MSE vs PSNR

6. CONCLUSION

The project is mainly concerned with reserved room technique and chaotic crypto system along with LSB data concealment. By his image quality and hidden data is preserved. Space reservation is done for concealing data using lifting wavelet transform and chaos encryption to protect images. This system will produce the stego image with high capacity with less error. Finally the performance will be evaluated with SNR factor, and other quality metrics. It was better flexible and compatible approach with higher efficiency than the prior methods.

REFERENCES

[1] Keda Ma, Weiming Zhang, Xianfeng Zhao "Reversible Data Hiding in Encrypted images by Reserving Room Before Encryption", *IEEE Trans. Information Forensics and Security.* Vol 8 No.3 March 2013.

[2] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramachandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process*., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[4] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[5] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.

© 2017 AJAST All rights reserved.