International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 9, September 2014

# A Novel data Protection System for Data Concealment using Reserving Room Approach

**T. Ramasubbaiah, A. Surendra Reddy, Ande Siva Sai Kumar**

***Abstract*— This paper presents the enhancement of data protection system for secret communication through common network based on reversible data concealment in encrypted images with reserve room approach. This idea will be implemented for true color image (RGB image) and reserve room approach under multi scale decomposition. The Blue plane will be chosen for hiding the secret text data. Reserving room approach is used to reserve space for embedding a privacy text messages. Chaos encryption is used to scramble an image except reserved space to make protection of image details during transmission. After encryption, the data hider will conceal the encrypted secret data into the reserved coefficients using Adaptive LSB replacement algorithm. 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.**

***Index Terms*—Adaptive LSB algorithm, Chaos encryption, Reserve room approach, RGB image, Reversible data concealment.**

## I. INTRODUCTION

Nowadays most of the internet users need to store send or receive data. The common way to do this is to transform the data into some unknown form. The resulting data can be understood only by those who know how to return it to its original form. This way of protecting information is known as encryption. Steganography [1] is the art of hiding information in ways that prevent the detection of hidden messages. Steganography is a Greek word which literally means "covered writing". The word steganography consists of two words Steganos and graphein, where Steganos means "hidden" or "covered" and graphein means "to write" [2]. The basic idea of steganography is to transmit the secret data securely so that the third party cannot understand the transmission of secret data.

Some of the basic key words in steganography are

- Secret Data: The information which is to be concealed or hidden.
- Carrier object: The media where payload has to be hidden.
- Stego object: The medium in which the information is hidden.
- Steganalysis: The process of detecting hidden information inside of a file.
- Stego medium: combination of Payload file and Carrier file.

### A. Types of Steganography

There are basically three types of steganography protocols used [3]. They are

- Pure steganography
- Secret key steganography
- Public key steganography

Pure steganography: In pure steganography system there is no need of exchanging the stego-key between the sender and receiver. This method of steganography is less secured.

Secret key steganography: In secret key steganography th secret key (stego-key) needs to be exchanged between the sender and receiver prior to communication. The major advantage of secret key steganography is that the parties who know the secret key can extract the secret message.

Public key steganography: The Public Key Steganography uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. The sender uses the public key during the encoding process and the private key, which has a relationship with the public key, can decipher the secret message. Public key steganography provides multiple levels of security.

### B. Steganography verses cryptography

Both steganography and cryptography are closely related. Cryptography converts the secret message into an unknown format which is not understandable. Whereas on the other hand steganography hides the secret message in another media so that there is no knowledge of secret message.

## II. RELATED WORK

### A. Reversible Data Concealment

Reversible Data Hiding (RDH) [4] is a technique, in which the original cover image can be losslessly recovered after the embedded message is extracted. This technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed [5].

### B. Reserve Room Approach

This technique is used to reserve the space for hiding data with minimum distortion. LWT[6] decomposes the image into different subband images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of subbands. Lifting scheme is a technique to convert DWT[7] coefficients to Integer coefficients[8] without losing



ISSN: 2278 – 909X 

information. LL subbands contains the significant part of the spatial domain image. High-frequency subband contains the edge information of input image. These coefficients are selected as reserved space foe hiding the text data. The secret text data is embedded into the wavelet coefficients of high frequency subbands because it is non sensitive to human visual system.

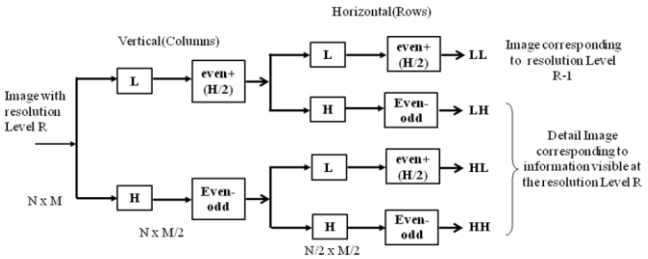


Figure1. Block diagram of Lifting Wavelet Transform

*C. Chaos Encryption*

This method is one of the advanced encryption standard to encrypt the image for secure transmission.

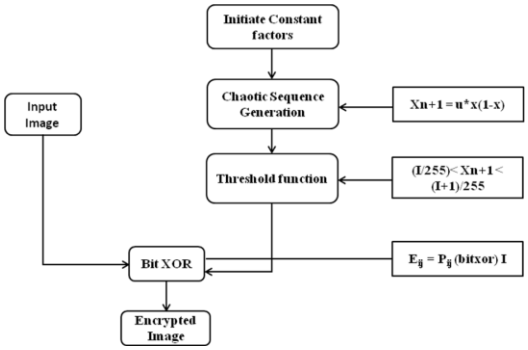


Figure2. Image encryption flow

It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by BIT-XOR 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.

*D.Adaptive LSB Algorithm*

LSB [9] is the most popular Steganography technique. Many carrier messages can be used in the recent technologies, such as Image, text video and many others. LSB uses the image as carrier message because the image file is the most popular for this purpose because it easy to send during the communication between the sender and receiver. It uses the RGB color image as carrier message. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. It hides the secret message in the RGB image based on it its binary coding. 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 an 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible.

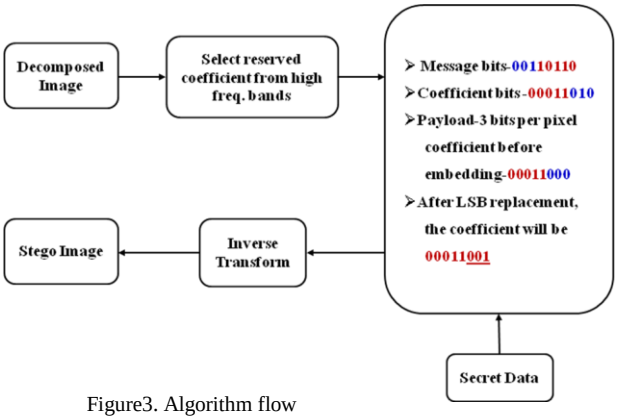


Figure3. Algorithm flow

## III. DATA EMBEDDING PROCESS

The embedding process is as shown in figure4.

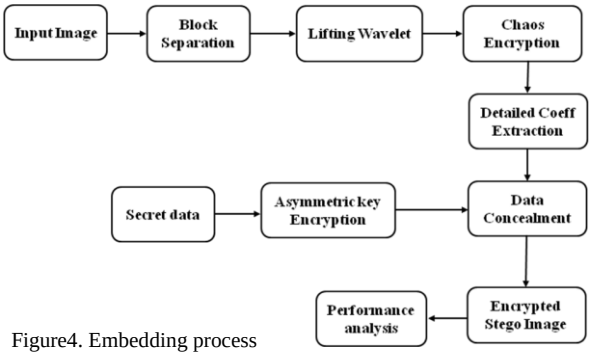


Figure4. Embedding process

In embedding process first we have to select the cover image. After image selection we have to separate the R, G and B plane separately and we have to select the B plane for data concealment. By applying lifting wavelet transform to the B plane image we have to reserve space for embedding the secret data. Except the reserved space in cover image (B plane image) we scramble the remaining space of the image by using chaos encryption. The secret data is also converted into an unknown format using asymmetric key encryption. The encrypted secret data is hidden in reserved space of the encrypted image using adaptive LSB algorithm. The final result of the embedding process is the encrypted stego image which contains the encrypted secret data.

## IV. DATA EXTRACTION PROCESS

The extraction process is as shown in figure5.

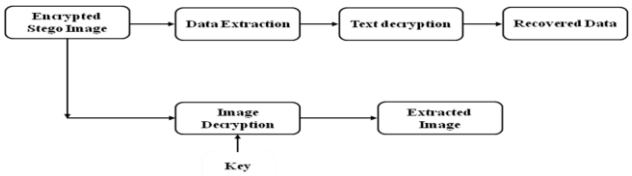


Figure5. Extracting process

The input in the extraction process is the encrypted stego image. An image and secret hidden text messages are extracted from stego encrypted image. The secret data can be

extracted from the embedded image with help of key matrix. The lifting wavelet transformation will be performed to stego image to find reserved space to select coefficients which are used at embedding side. Finally, Extracted secret text data is in the form of cipher text and then convert into plain text (original text) using chaos decryption process.

## V. RESULTS

*a). Cover image selection:*

The cover image can be selected as shown in figure6 which can be of any dimensions.


Figure6. Cover image selection

*b). Cover image and B plane image:*

The cover image and its B plane image are as shown in figure7.

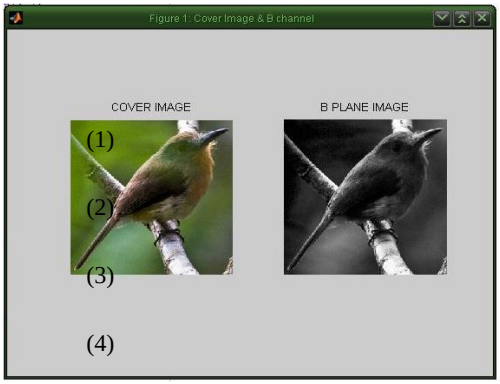


Figure7. Cover image and B plane image

*c). Secret data selection:*

The text file that contains the secret data is selected as shown in figure8.


Figure8. Secret data selection

*d). Transformed image:*

The transformed image of the cover image (B plane image) is as shown in figure9.

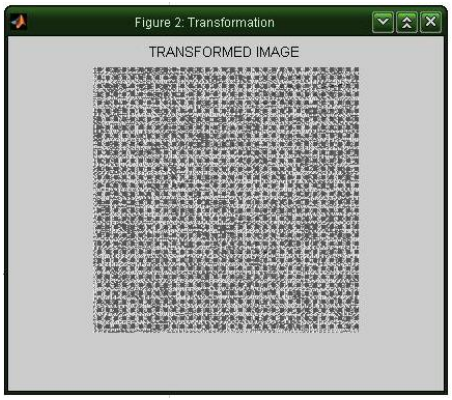


Figure9. Transformed image

*e). Encrypted stego image:*

The encrypted stego image which contains the secret data is as shown in figure10.

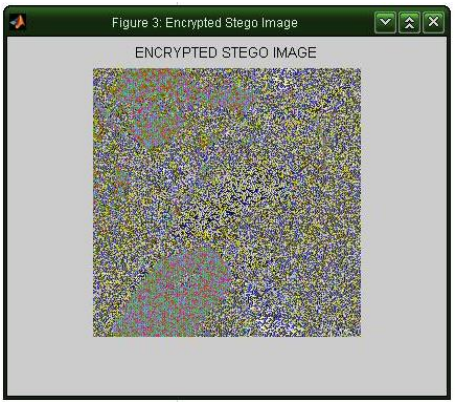


Figure10. Encrypted stego image

*f). Recovered image:*

The recovered cover image after extraction process is as shown in figure11.


Figure11. Recovered image

*g). Parameter analysis:*



ISSN: 2278 – 909X 

The different parameters that justify the proposed system and the final results of the proposed system are as shown in figure12.

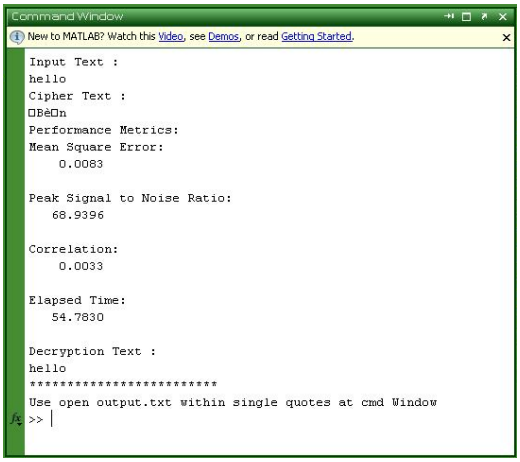


Figure12. Parameter analysis

## VI. CONCLUSION

This paper presented that protection of image quality and hidden data during transmission based on approach of reserve room technique and chaotic crypto system with LSB based data concealment. Here, lifting wavelet transform was used to reserve space for concealing data effectively and chaos encryption was used as to protect image contents. This system was generated the stego image with less error under maximum data hiding capacity. Finally, the performance of system was evaluated with quality metrics such as error and SNR factor. It was better compatible approach and flexibility with better efficiency rather than prior methods.

## REFERENCES

[1] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010.

[2] Fahim Irfan Alam, Fateha Khanam Bappee, Farid Uddin Ahmed Khondker, "An Investigation into Encrypted Message Hiding Through Images Using LSB", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 2 Feb 2011.

[3] Jammi Ashok, Y.Raju, S.Munishankaraiah, K.Srinivas, "Steganography: An Overview", International Journal of Engineering Science and Technology, Vol. 2(10), 2010, 5985-5992.

[4] 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.

[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[6] 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.

[7] 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

[8] R.EI Safy, H. H. Zayed, A. EI Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", 978-4-4244-3778-8/09, 2009IEEE.

[9] Fahim Irfan Alam, Fateha Khanam Bappee, Farid Uddin Ahmed Khondker, "An Investigation into Encrypted Message Hiding Through Images Using LSB", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 2 Feb 2011.