ISSN XXXX XXXX © 2016 IJESC

Research Article Volume 6 Issue No. 12

Secret Data Sharing Through Image by Using LWT and LSB Steganography Techniques

Vijayaraghavan.V[1], Harini .V[2]
Assistant Professor[1], PG Scholar[2]
Department of ECE
Adithya Institute of Technology, Coimbatore, Tamil Nadu, India

Abstract:
Security of information is very important in terms of communication and/or the secrecy of how to decode it. The enhancement of security system for secret data communication through encrypted data embedding in Color images is proposed. Initially the cover image is converted to any one plane process and encrypted by using Chaos encryption. Adaptive LSB replacement algorithm is used for hiding the secret message bits into the encrypted image. In the secret data extraction module, the secret data will be extracted by utilizing significant key for choosing the image pixels to extract the data. This technique is particularly helpful in applications such as medical and military imaging. The proposed methodology provides better performance in terms of MSE, Hiding capacity and peak signal to noise ratio. It is implemented in FPGA (Field Programmable Gate Array) and MSE, PSNR are computed. The design architecture when implemented on FPGA Spartan III offers high processing speed, which might give an impulse for the researchers to a very fast, programmable & cost effective hardware solution in the area of Secure Communication.

Index terms: Adaptive LSB replacement, Chaos encryption, Data hiding, FPGA, Lifting Wavelet Transform, PSNR.

I. INTRODUCTION

Stegnography is widely used in medical and military imagery for secret data communication. The system uses reserve room before encryption way to deal with defeat the issue of earlier methods such as vacating room after encryption and pixel difference expansion. In existing, pixel difference expansion based RDH is the spatial domain process to conceal secret text messages within a cover image. The data hiding includes histogram adjustment to reduce overflow and underflow error and adjacent pixels are subtracted to decide the distinctions image [1]. Then the variation will be either incremented or decremented based on message pixels. This application produces the spatial distortion leads to degrade an image quality and it is less compatible and difficult. That will overcome by the method of least significant bit replacement topology. In Vacating room after encryption stage, the encrypted messages are concealed into encrypted domain by replacement of some pixel value. This spatial domain technique distorts an image quality wherever the secret message bits were blocked by the thought of these issues [2]; the system proposes the reserve room approach with lifting wavelet transformation for saving an image quality and enhance the security of communication. The algorithm lifting wavelet decomposes an image into frequency sub bands which contains approximation and detailed elements it reserve the coefficients from detailed components which have shape, edges and region boundary point. It is insensible region for human visual system applications. Also with this approach, chaos system, transmission of adaptive least significant bit replacement will be used for image encryption and message embedding will be done recovery of data is the reverse process of the encryption and embedding to get lossless extracted image and messages in the particular picture. The simulated result shows performance of the used systems regarding measurements assessment, for example, mean square error signal, wave of peak signal to noise ratio and correlation coefficients.

II. PROPOSED METHOD

A) LIFTING WAVELET TRANSFORM

Lifting wavelet transform implementation is theoretical invertible. However, due to the finite register length of the computer system, inversion errors could happen and it would result in unsuccessful image reconstruction. In practical cases, the wavelet elements will be rounded to the nearest integer in the discrete transformation stage. This makes the lossless compression impossible. A developed algorithm called lifting wavelet transform which is based on the wavelet theory is developed and it needs significantly fewer arithmetic and memory compared to the convolution based discrete wavelet transform. The lifting-based DWT conspire separates the high-pass and low-pass wavelet filters into a sequence of many filters. These decomposed filters are then converted into a sequence of upper and lower triangular filters.

B) ADAPTIVE LSB REPLACEMENT:

In this approach variable number of LSBs would be used for embedding secret message bits according to the mentioned algorithm: For all components of each and every pixels of color image across smooth areas [4]. Every pixel value in this image is analyzed and the following checking process is employed for all the three bytes respectively If the value of the pixel say P, is in the range $240 \leq P \leq 255$, then we embed 4 bits of secret data into the 4 LSBs of the pixel value. It should be possible by detecting the first 3 Most Significant Bits. If they are all 1’s then the remaining 4 LSB’s can be used for embedding data. If the value of P is in the range 224 ≤ P ≤239, then we embed 3 bits of secret data into the 3 LSB’s of the pixel. If the value of P (First 2 MSB’s are all 1’s), is in the range 193 ≤ P ≤223 then we embed two bits of secret data into the two LSB’s of the pixel value other cases for the values in the range 0 ≤ P ≤192 we embed 1 bit of secret data in to 1 LSB of the pixel value. Same procedure is adapted for extracting the hidden secret data from the image.

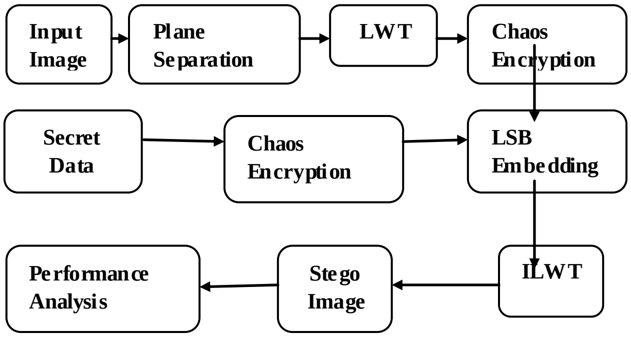

Figure. 1. Block Diagram for Secret Data Hiding Process

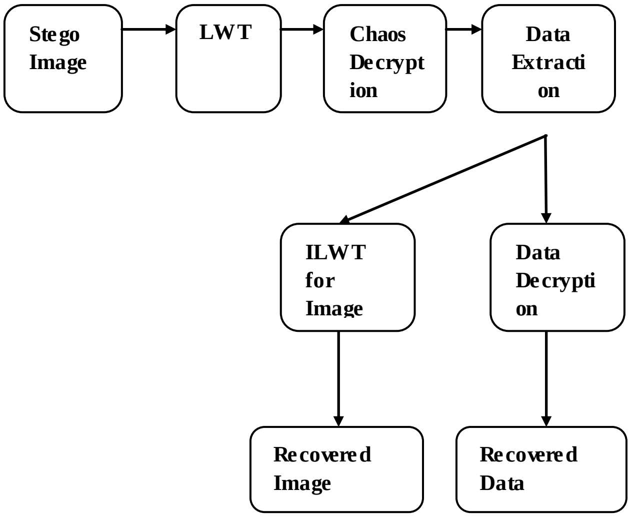

Figure. 2. Block Diagram for Secret Data Extraction Process

It is clearly observed that the adaptive LSB reflect the texture information of the cover image to some pointy. Reference on wide analyses, we find that uncompressed natural images usually contain some flat regions and adaptive LSB in those regions have the same values. In the event that we embed the secret message into these regions, the adaptive LSB of stego images would turn out to be increasingly irregular, which may lead to visual and statistical differences between cover and stego images in the adaptive LSB plane Compared with smooth portion, the adaptive LSB of pixels located in edge part typically display more arbitrary attributes, and they are almost similar to the distribution of the secret message bits. Hence, little measure of noticeable ancient artifacts and visual artifacts would be left in the edge part after data hiding. Besides, the edge data is profoundly needy on image portion, it generate detection even more tough So that only the proposed technique will at first embed the secret bits into edge regions as far as possible while holding other smooth regions as they are.

C) CHAOS ENCRYPTION

The use of chaotic cryptography for image encryption is the nature of chaos has initiated a lot of interests in different engineering applications, where cryptography must be one of the most potential technologies [4]. Chaotic maps have been connected to cryptography in a few distinctive ways. Chaotic sequences have several good properties; in underlying conditions and their fault-like properties using the chaos to cryptography was a great contribution to enhance the security of information because of the sufficient properties of chaotic encryption [5]. All three chaotic dynamic systems namely Lorenz, Chen and LU one is selected by the system elements where it is obtained from the key and it is applied to the 0's and 1's color image encryption because of higher privacy of high-dimension chaotic encryption system. Next of the encryption procedure is to scramble the rearranged image by changing its pixel values based on one of the three high-dimensional chaotic systems. This is referred to as the diffusion stage. The first conditions and the control elements used to generate the chaos encryption sequence in both the stages serve as the secret key in the two stages. The resulting image is the encrypted image. Separate key is used for permutation and diffusion stages of the chaos encryption process to improve security of the algorithm.

D) CHAOS DECRYPTION

The decryption system is illustrated in the Figure 2. The first stage in the decryption process is the diffused image decryption point at first encryption stage, the value of pixels diffusion was carried out with any one of the three chaotic decryption systems. To retrieve the original pixel values, again any one of the chaotic system is employed in the first stage of decryption in step one of chaos decryption process uses the three dimensional sequence generated by any one of the chaotic decryption system. The initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first step. The pixel position permutation was carried out with any one of the chaotic system. The initial conditions and control parameters for generating the chaos-sequence were used as the confusion element. So in the chaos decryption stage, the exact chaotic decryption systems with same confusion key are used to get the original position of the picture.

III. SIMULATION RESULTS

The performance of proposed methodology will be evaluated with the natural images. Secret image will be hided securely in the cover image and recovered back. Here the metrics such SSIM and PSNR were measured. The performance of the technique will be evaluated as following,

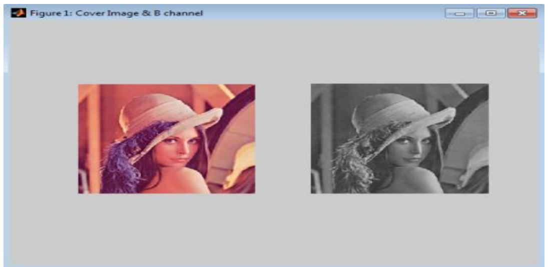

Figure. 3. Input and B Plane Image

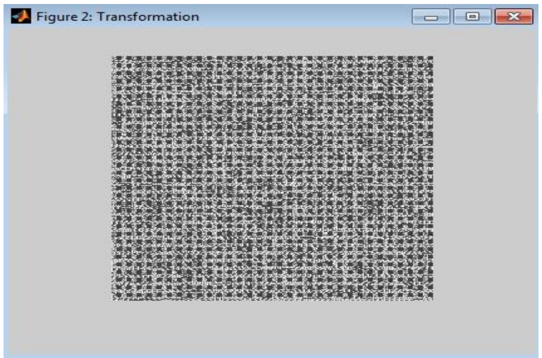

Figure. 4. LWT Image

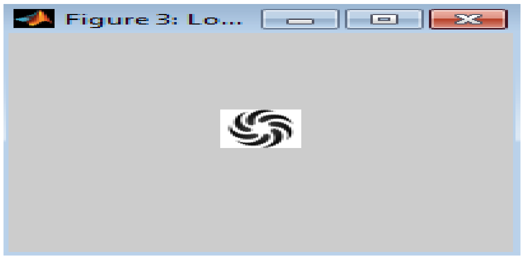

Figure. 5. Secret Image

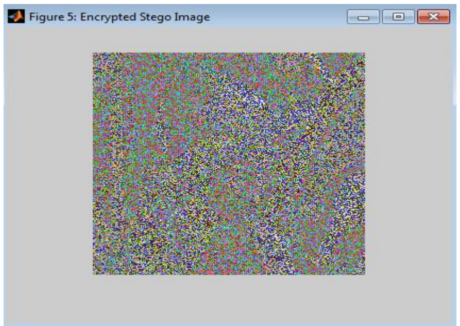

Figure. 6. Encrypted Stego Image

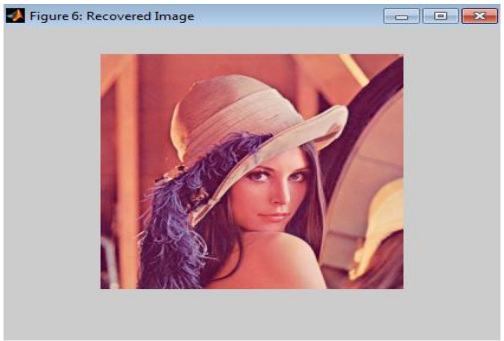

Figure. 7. Recovered Cover Image

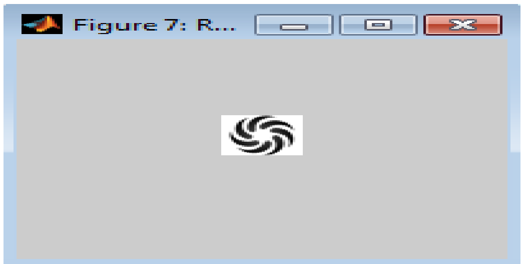

Figure. 8. Recovered Secret Image

TABLE .1: PSNR AND SSIM INDEX

		PSNR	SSIM
PROPOSED METHOD	BALL	65.8190	1.0000
	LENA	70.8056	1.0000
	BABOON	62.0746	0.9997

IV. CONCLUSION

Data hiding using steganography has two primary objectives firstly that steganography should provide the maximum possible payload, and the second, embedded data must be imperceptible to the observer. It was found that the proposed method gives high payload in the cover image with very little error. This is of course on the expense of increasing PSNR and reducing the MSE. The Optimum Pixel adjustment process was used for reduction of error between the input image and embedded image. Future work is to implement this process in FPGA kit.

V. REFERENCES

[1] S. Bhattacharyya,. "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier." Journal of global research in computer science 2, no. 4, 2011.

[2] N. Raftari and A.-M. E. Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT," in 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2012, pp. 295–300.

[3] S. Saejung, A. Boondee, J. Preechasuk, and C. Chantrapornchai, "On the comparison of digital image steganography algorithm based on DCT and wavelet," in Computer Science and Engineering Conference (ICSEC), 2013 International, 2013, pp. 328–333.

[4] N. Sathisha, G. N. Madhusudan, S. Bharathesh, K. B. Suresh, K. B. Raja and K. R. Venugopal, "Chaos based Spatial Domain Steganography using MSB", International Conference on Industrial and Information Systems(ICIIS), pp. 177-182, 2010.

[5] M. Tayel, H. Shawky and A. E. S. Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data," 14th International Conference on Advanced Communication Technology, pp. 208 – 212, 2012.