www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7744-7747

DWT Domain Data Encryption with Asymmetric key Cryptography

Miss. Snehal C.Dinde[1], Dr.Mrs.Shubhangi B.Patil[2]

[1]Student,Department of Electronics & Telecommunicaton
Dr.JJ.Magdum College of Engineering,Jaysingpur,India
E-mail: dindesc@gmail.com

[2]Professor,Department of Electronics & Telecommunicaton
Dr.JJ.Magdum College of Engineering,Jaysingpur,India
E-mail: sbp_jjm2004@yahoo.co.in

Abstract: ***This paper discuses the attempt done to provide secret communication technique by hiding confidential data in image. Here steganography along with cryptography is used to strengthen the security. Steganography hides existence of data while cryptography protects the information by transforming it into an encrypted form. Asymmetric key cryptography technique – RSA is used to encrypt the secret data and then Haar- DWT transformation algorithm is used to embed the secret data which is in encrypted form. Experimental result shows image quality parameters like PSNR and Mean Absolute Error.***

Keywords: Cryptography,Discrete Wavelet Transform, RSA, Steganography

1. Introduction

Now a days Internet has become a basic medium for communication and there is strong need of security against malicious and unintentional attacks. So in order to protect confidentiality and integrity of data against attackers many techniques like steganography and cryptography are used. Steganography hides the data into cover media where cryptography encrypts the data by transforming it into a secrete format which is readable to authorized person. This paper uses Asymmetric key cryptography approach for security of secret data. Encrypted secret data is hided into an image using DWT steganography. DWT (Discrete Wavelet Transform) steganography technique reconstructs detail coefficients of an image for embedding the encrypted data. DWT technique maintains visual clearance.

2. RSA algorithm

RSA algorithm[2] is Asymmetric cryptography algorithm. This algorithm uses key pair, one for encryption and second for decryption of data. This algorithm used for authentication and encryption. The Step given below describes the operation of RSA.

- Select two random prime numbers ‘p’ and ‘q’ and calculate modulus, n= p × q
- Select third number ‘r’, which is prime to product (p-1) (q-1). The number ‘r’ is public exponent.
- Now, Calculate integer‘d’ from quotient (rd-1)/ [(p-1) (q-1)], where the number‘d’ is the private exponent.
- The public key is pair (e, n) and pair (d, n) is the secret private key.

Sender of the message will use public key for encryption. $C = M^r \bmod n$ here C is generated cipher text, M is message.
Receiver then decrypts the cipher text with the private key $M = C^d \bmod n$

3. Steganography

Steganography is process of hiding secret information into cover media. Cover media can be an image, Audio, Video, text etc. The Steganography[12] is a protective technique of communication where the true information is not visible to observer.

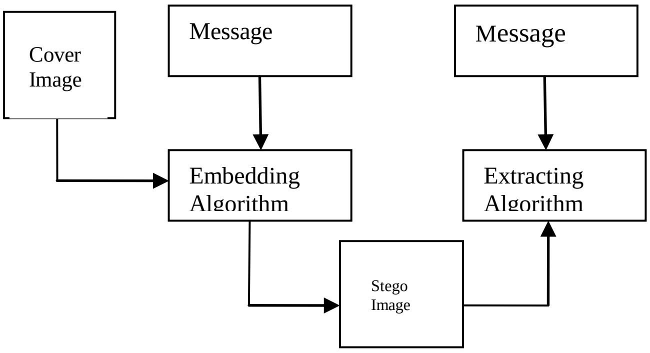


Figure. 1. Image Steganography

Some steganographic Techniques are:
- Substitution Technique in Spatial Domain.
- Transform Domain Technique.

- Spread spectrum Technique.
- Distortion technique.
- Statistical Technique

3.1 Transform Domain Technique

Proposed paper uses this technique. This technique [5] uses transform coefficient to hide the data. By modifying transform coefficient, secret data is to be embedded. This is widely used because of its independency over image formats. This technique is more robust to different types of attacks.

Some methods of transform domain Techniques are DCT and DWT

- Discrete Cosine Transform (DCT)

This method helps to separate the image into spectral sub bands[5] with respect to images visual quality. It transforms signal or image from spatial domain to frequency domain. This method divides image into 8*8 pixel blocks transformation applied on each block. The least coefficient bits of these coefficients are modified to embed secret data.

- Discrete wavelet Transform (DWT)

Discrete wavelet transform[8] is based on sub band coding which gives fast computation of wavelet transform. It is easy to implement and reduces the computation time and resources as required. This method stores secret data in least important coefficient of 4*4 Haar transformed blocks. Proposed system is based on this method

- Haar DWT Transform

Proposed paper uses Haar wavelet Transform [4] which is simplest type of DWT. Haar wavelet is a sequence of rescaled "square-shaped" functions which together form a wavelet family or basis. Wavelet analysis is similar to Fourier analysis in that it allows a target function over an interval to be represented in terms of an orthonormal function[5] basis. By calculating the sums and differences of adjacent elements, Haar wavelet operates on the data. First it operates horizontally and then vertically in 2-D Haar . A 2-dimensional Haar-DWT [1] consists of two operations which are described as follows:

a) Scan the pixels from left to right in horizontal direction[4] and perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as shown in Figure 3

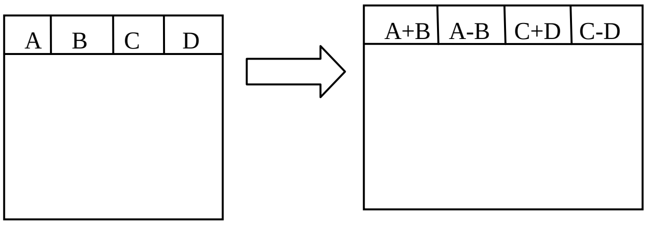


Figure2. The horizontal operation on the first row

Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

b) Scan the pixels from top to bottom in vertical direction[4]and perform the addition and subtraction operations on neighboring pixels. Then store the sum on the top and the difference on the bottom as shown below. Repeat this operation until all the columns are processed. Finally 4 sub-bands denoted as LL, HL, LH, and HH respectively are obtained. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

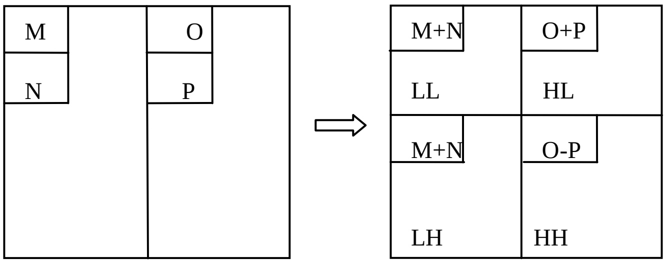
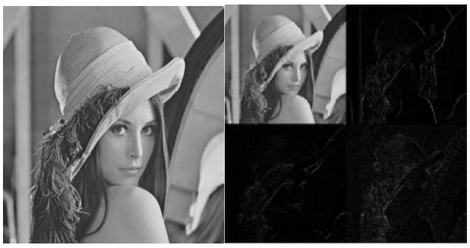


Fig.3 The Vertical operation

First order 2-D DWT applied on image “lena” illustrated in



(a) (b)

Figure 4 . (a) Original image-Lena (b) Result after the first-order 2-D Haar-DWT

4. **Proposed Method**

Proposed system uses grayscale image as cover image[1]. For embedding encrypted data grayscale image as a cover image provides high level of security. Proposed paper uses both cryptography as well as steganograpy. Embedding and encryption process done in following two stages:

4.1 Encryption using RSA Algorithm

In this stage data is encrypted using public key RSA algorithm. Using public encryption and private decryption keys it produces cipher text.

4.2 Data Embedding

For embedding data cipher text is converted into 8-bit binary code[1]. This binary code is embedded into cover image. Haars 2-Dimensional DWT uses for embedding data. It produces coarse and detailed coefficients. Coarse coefficient is nothing but approximation coefficient and detail coefficients are horizontal, vertical and diagonal coefficient. Approximation sub band looks like an original image. But approximation coefficients are not suitable for embedding because they carry the most information content of the whole cover image.

The process of embedding consists of comparing the secret message with detail coefficients. The coefficients suitable for first embedding are elected from detail areas (VL, DL, HL) and encrypted secret message. In the second embedding process it consists of comparing the modified coefficient (DWT detail area) with the other detail coefficients

In data embedding, firstly steganography is applied to cover image for embedding encrypted secret data. Then by applying detailed coefficient[1] to one of the area of cipher text we obtain the stego image. Secondly Steganography is applied again to embed that detail coefficient to another area of detail coefficient of the image. After embedding all secret data and performing inverse DWT (IDWT), the stego image is obtained. The Stego-image with the secret message embedded is then ready for transmission

At the receiver, the recovery of the original secret message is done in two steps:

4.3 Extraction Process

It requires two stages of decoding to recover the original secret data. The first stage of decoding is done to recover the first details coefficient[1] from the second details coefficient. The second stage decoding involves recovering the original secret data from the first details coefficient. The advantage of this method is that the original cover image does not have to be present on the receiver side for the successful reconstruction of the original data. Therefore, the risk of disclosure of secret communication is lower.

4.4 Decryption

At this stage decryption of cipher text is competed by using the private key by RSA algorithm.

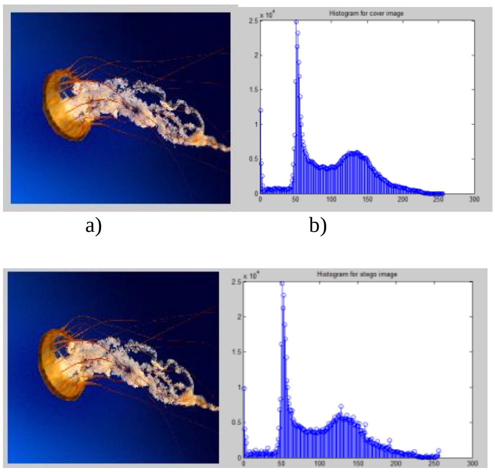
5. Experimental Results

Evaluated performance of proposed technique[15] using different images as cover image. The performance of algorithm is measured using different parameters given below: Proposed Technique is implemented in MATLAB. Five sample observations with their PSNR, Bpp, MAE and Histogram are shown below.

Image Name	Image Size (Kb)	Amount of cipher text embedded (Kb)	bpp (bits per pixel)	PSNR (dB)	Mean Absolut e Error
Jellyfish	757	22.3	0.24	48.0929	1.1405
Eye	768	22.3	0.23	45.3740	2.9450
Australia	900	11.4	010	45.7702	2.1619
Tiger	225	5.09	0.18	42.7042	4.4999
penguin	759	8.00	0.084	58.1005	0.1243

Table 1. Observed PSNR, MAE and Bpp values

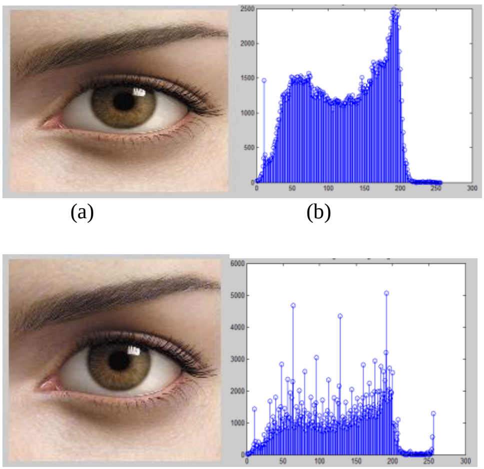
5.1 PSNR*:* The peak signal-to-noise ratio is computation done against two images. It is quality measurement parameter between the original and a compressed image. For better quality of the compressed or reconstructed image PSNR, is higher. For all the stego images values of PSNR and MAE are shown below



a) b)

(c) (d)

Figure. 5 (a) original Jellyfish image (b) is its histogram, (c) is the stego Jellyfish image with 22.3 kilo bytes embedded, and (d) is the histogram of stego Jellyfish image



(a) (b)

(c) (d)

Figure.6 (a) original Eye image (b) is its histogram, (c) is the stego Eye image with 22.3 kilo bytes embedded, and (d) is the histogram of stego Eye image

6. Conclusion

This paper employs steganography technique in DWT domain as related to images. This is an effective steganographic method for embedding secret messages into images without any vital changes has been proposed. This paper used both cryptography and steganography for security of data. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. These transformations provide sufficient secrecy. Embedding capacity of this method is much better than other existing methods.

7. References

[1] Nadiya P v and B Mohammed lmran , “Image Steganography in DWT Domain using Double-stegging with RSA Encryption” International Conference on Signal Processing, Image Processing and Pattern

Recognition [ICSIPR] 978-1-4673-4862-1/13/$31.00 ©2013 IEEE

[2] Mohit Kumar Goel and Dr. Neelu Jain, "A RSA- DWT Based Visual Cryptographic Steganogrphy Technique" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 2

[3] Chen, T.S., Chang C.C., and Hwang, M.S, "A virtual image cryptosystem based upon vector quantization". IEEE transactions on Image Processing 1998, 7,(10): 1485 – 1488

[4] Po-Yueh Chen and Hung-Ju Lin , "A DWT Based Approach for Image Steganography" International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[5] Darshana Mistry, Asim Banerjee, "Discrete wavelet transform using MATLAB" (IJCET),2013 Volume 4, Issue2

[6] Prabakaran Ganesan and R. Bhavani , " A High secure and robust image steganography using dual wavelet and blending model" Journal of Computer Science, 9 (3): 277-284, 2013

[7] Luo, W. F. Huang and J. Huang, " Edge adaptive image steganography based on LSB matching revisited" IEEE Trans. Inform. Forensics Securty, 5: 201-214. DOI:10.1109/TIFS.2010.2041812

[8] Parul Sehgal and Vijay Kumar Sharma, "Eliminating Cover Image Requirement in Discrete Wavelet Transform based Digital Image Steganography" International Journal of Computer Applications 2013 (0975 – 8887) Volume 68– No.3

[9] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography", IEEE International Symposium on Information Theory on 1976, Ronneby,Sweden.

[10] Vladimfr BANOCI, Gabriel BUGAR, Dusan LEVICKY, "A Novel Method of Image Steganography in DWT Domain", Technical University of Kosice, Slovak Republic.

[11] Ayman Ibaida and Ibrahim Khalil,"Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems", IEEE Transactions on Biomedical Engineering, Vol.60,12 December 2013.

[12] Gowtham Dhanarasi and DR.Malikarjun Prasad, "Image Steganography using Block Complexity Analysis", International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.07 July 2012

[13] Sushil Kumar and S.K.Muttoo,"A Comparative study of Image Steganography In Wavelet Domain", International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 2, February 2013

[14] Ching-Yu Yang, Chih-Hung Lin and Wu-Chih Hu, "Reversible Data Hiding for High-Quality Images Based

on Integer Wavelet Transform, Journal of Information Hiding and Multimedia Signal Processing" , Volume 3, Number2, April 2012

[15] Gandharba Swain and Saroj Kumar Lenka, "A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography ", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012 .