International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.2., Issue.5, 2014

RESEARCH ARTICLE

ISSN: 2321-7758

STEGANOGRAPHIC METHOD WITH DWT AND ENCRYPTION

K. RAMYA KRISHNA[1], S. RANJITH KUMAR[2]

[1]M.Tech student, Department of ECE, GANAPATHY ENGINEERING COLLEGE, Warangal.

[2]Assistant Professor, Department of ECE, GANAPATHY ENGINEERING COLLEGE, Warangal

Article Received: 22/09/2014 | Article Revised on: 16/10/2014 | Article Accepted on:21/10/2014

K. RAMYA KRISHNA

ABSTRACT

This article proposes the effort prepared to offer secret communication method with hiding secret information in picture. at this point steganography along with cryptography is employed to reinforce the safety. Steganography covers subsistence of information while cryptography secures the data by converting it into an encrypted structure. RSA technique is applied to encrypt the furtive information and after that Haar DWT conversion algorithm is utilized to set in the furtive information which is in encrypted type. Experimental outcomes explain picture quality factors like PSNR and Mean Absolute Error.

Keywords: Cryptography, Discrete Wavelet Transform, RSA, Steganography

INTRODUCTION

At the present time Internet has turn into an essential medium for communiqué and here is sturdy necessitate of safety against malevolent and inadvertent assails. Therefore in order to keep privacy and reliability of information alongside invaders numerous methods similar to steganography & cryptography are employed. Steganography covers the information into hide medium where cryptography encrypts the information with converting it into a hide arrangement which is decipherable to approved person. This manuscript employs Asymmetric key cryptography method for safety of furtive information. Encrypted surreptitious information is covered into a representation by DWT steganography. Discrete Wavelet Transform steganography method rebuilds feature coefficients of a representation for entrenching the encrypted information.

II. RSA ALGORITHM

RSA algorithm is Asymmetric key cryptography method. This technique exploits key duo, one for encryption and another for decryption of information. This method exercised for verification and encryption. The given points illustrate the procedure of RSA.

- choose two arbitrary prime numbers ‘x’ and ‘y’ then compute modulus, n= x × y
- Choose third number ‘z’, which is prime to product (x-1) (y-1). The numeral ‘z’ is open exponent.
- Currently, determine integer‘d’ from quotient $(z^d-1)/ [(x-1) (y-1)]$, where the integer‘d’ is the secret exponent.

- The public key is duo (e, n) and duo (d, n) is the furtive private key. Transmitter of the data will utilize public key for encryption. $C = M^z \bmod n$ at this point C is produce cipher content, M is a message. Later recipient decrypts the secret message through the private key $M = C^d \bmod n$.

III. STEGANOGRAPHY

Steganography is the method of covering furtive data into secret medium. Secret media could be a picture, sound, Video, message, etc. The Steganography is a defensive method of communiqué where the exact data is not observable to viewer.

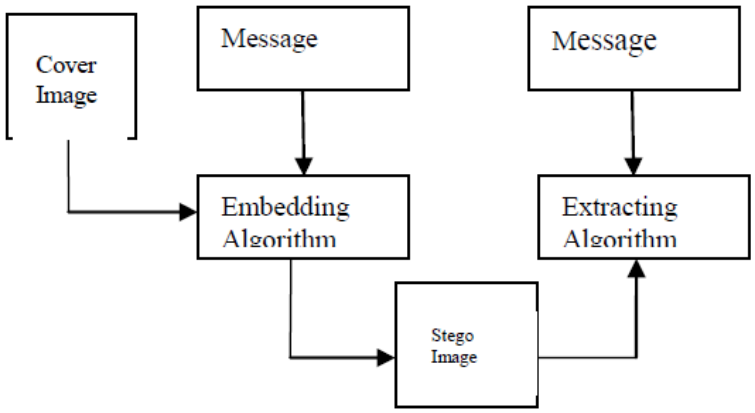

Figure 1. Image Steganography

Transform Domain Technique

Projected manuscript employs this method. This system employs convert coefficient to secrete the information. By amending transform coefficient, furtive information is to be entrenched. This is broadly utilized since its independency above picture designs. This procedure is more vigorous to several kinds of assails. Various schemes of transform domain Techniques are Discrete Cosine Transform and Discrete Wavelet Transform.

a. Discrete Cosine Transform (DCT)

This scheme aids to split the picture into spectral sub groups with respect to pictures visual feature. It converts signal or representation from spatial field to frequency field. This technique separates picture into 8*8 pixel blocks alteration functional on every block. The slightest coefficient bits of these elements are customized to entrench hidden information.

b. Discrete wavelet Transform (DWT)

Discrete wavelet transform is depends on sub group ciphering which provides quick calculation of wavelet transform. This is simple to apply and decreases the calculation time. This process hoards furtive information in smallest significant element of 4*4 Haar transformed blocks. projected scheme is depends on this technique.

c. Haar DWT Transform

Proposed manuscript employs Haar wavelet Transform which is easiest form of DWT. Haar wavelet is a series of rebalanced "square-shaped" functions which jointly forms a wavelet origin. Wavelet study is alike to Fourier study in that it allocates an objective task above a period to be embody in terms of an ortho standard function root. By scheming the additions and subtractions of neighboring fundamentals, Haar wavelet functions on the information. Earliest it works parallel and next perpendicularly in 2-D Haar. A 2-D Haar-DWT consists of two procedures which are depicted as follows:

i) Search the pixels starting left to right in horizontal path and execute the sum and difference process on adjacent pixels. Save the addition on the left and the subtraction on the right as exposed in Figure 2

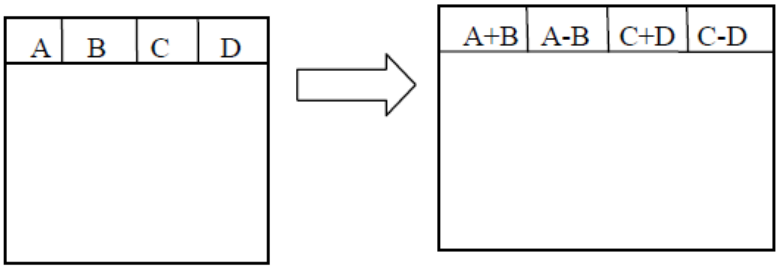

Figure2. The horizontal process on the primary row

Recur this process until each and every row is operated. The pixel summation signifies the short frequency division represented as character L whereas the pixel differentiation signifies the high frequency division of the unique representation (represented as character H).

ii) Inspect the pixels starting top to bottom in vertical path and execute the sum and difference processes on adjacent pixels. Then save the addition on the top & the subtraction on the bottom as exposed in fig 3. Replicate this process until each and every column is operated. At last 4 sub groups indicate as LL, HL, LH and HH correspondingly are attained. The LL sub-group is the short frequency part and thus seems incredibly alike to the original picture.

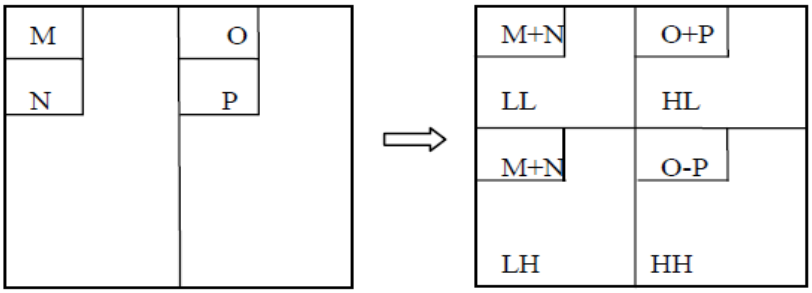

Figure 3. The vertical process on the primary column

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

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

IV. PROPOSED METHOD

Proposed scheme employs grayscale picture as conceal picture. For implanting encrypted information grayscale picture as an envelope picture gives a high stage of protection. Proposed manuscript employs mutual cryptography and steganograpy. Data implanting and encryption procedure completed in subsequent two steps:

4.1 Encryption using RSA Algorithm

In this step information is ciphered by public key RSA algorithm. Applying public encryption and private decryption keys it generates secret message text.

4.2 Data Embedding

For implanting information secret message is rehabilitated into 8 bit binary system. This binary system is rooted into hidden picture. Haar 2-D Discrete Wavelet Transform employs for implanting information. It generates coarse and exhaustive elements. Coarse element is also called as estimate element and exhaustive elements are horizontal, vertical and diagonal element. Estimate sub group seems like a unique picture. But estimate elements are not appropriate for implanting since they take the most data substance of the entire cover picture. The method of entrenching consists of evaluating the cipher text with detail elements. The elements appropriate for initial entrenching are chosen from detail parts (VL, DL and HL) and encrypted cipher text. In the subsequent entrenching procedure it consists of evaluating the customized element with the other detail elements.

4.3 Extraction progression

It needs two steps of deciphering to improve the original surreptitious information. The primary step of interpreting is completed to recuperate the initial details coefficient commencing the next details element. The subsequent step interpreting engages recuperating the original surreptitious information from the original details element. The benefit of this process is that the unusual cover picture doesn't have to be there on the recipient side for the victorious restoration of the original information. Consequently, the threat of revelation of secret communiqué is minor.

4.4 Decryption

At this process decryption of code message is contended by utilizing the private key with RSA algorithm.

V. EXPERIMENTAL RESULT

Verified recital of projected method employing various pictures as cover image . The Proposed method is executed in MATLAB. In data entrenching, initially steganography is functional to hide picture for embedding ciphered secret message. After that by pertaining detailed element to one of the region of nonentity text we attain the stego representation. Then Steganography is practical again to implant that detail element to a different region of detail element of the figure. After establishing all secret information and executing inverse DWT (IDWT), the stego representation is achieved. The stego representation by the secret communication embedded is next prepared for broadcast at the recipient.

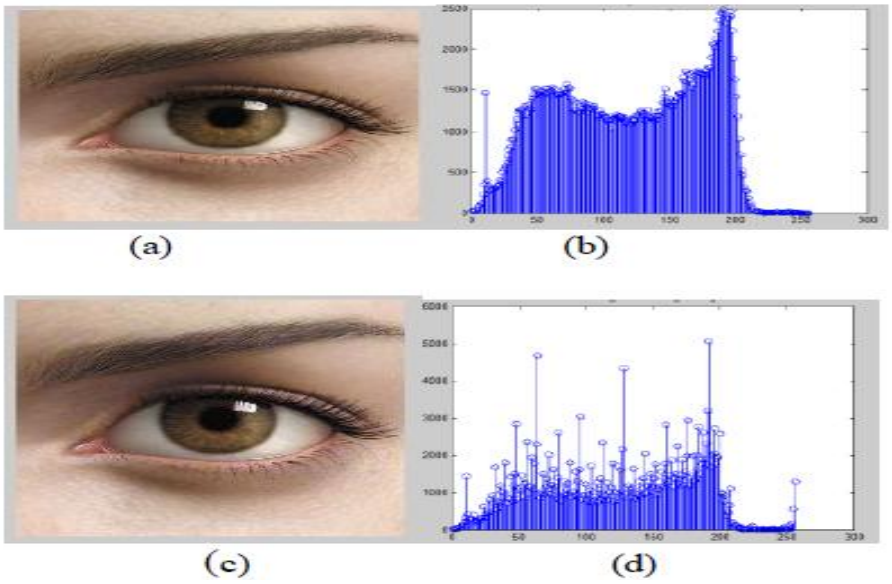

Figure.5 (a) original Eye picture (b) is its histogram, (c) is the stego Eye representation with 22.3 kilo bytes entrenched and (d) is the histogram of stego Eye representation

CONCLUSION

This manuscript uses steganography method in DWT area as associated to representations. This is an effectual steganographic technique for entrenching furtive texts into representations not including any imperative transforms has been described. This article employed mutual cryptography and steganography for protection of information. The entrenching procedure is concealed in the conversion of hidden picture. These conversions offer adequate privacy. Entrenching capability of this technique is greatly enhanced than other presented systems.

REFERENCES

[1] A Secure Skin Tone based Steganography Using Wavelet Transform Anjali A. Shejul, Umesh L. Kulkarni, International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011 1793-8201

[2] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, —Biometric inspired digital image Steganography, in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg.of Computer-Based Systems (ECBS„08), Belfast, 2008, pp. 159-168.

[3] A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum. International Journal of Modern Engineering Research (IJMER). Vol.1, Issue1, pp-157-161

[4] Schneier B.,"Applied Cryptography**,** Second Edition: Protocols, Algorithms andSource Code in C",John Wiley & Sons, Inc., USA, 1996

[5] Methodology of Spread-Spectrum Image Steganography,army research laboratory

[6] Object Oriented steganography Based On Biomertic And spread Spectrum. International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

[7] Nadiya P v and B Mohammed Imran , "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

[8] 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.