Image &Text Security Enhancement using DT-DWT with High Boost Filter : A Review

Ankita Jain ,Y. Pandey

SIRT Bhopal

Abstract - The transmission of image or data is done over the network and the attackers trap most of the data when it is moving in the network from source to destination. So, the security of the image data is the major issues. The image can be secure using steganography, cryptography, wavelet transform and some other security measures. The steganography is the art of hiding the message like image or text. A lot of work has been one by different researchers for the image security. In this paper presents the literature study of the various techniques proposed and implemented.

Keywords : Cryptography, Image data, Steganography, Wavelet transforms.

1. INTRODUCTION

As the development of Internet technologies escalations, the broadcast of digital media is now daysappropriate over the networks. But secret information broadcasting over the network suffers from strict security overhead. So, defensive of secret information for the period of transmission becomes a noteworthymatter. Though cryptography changes the message so that it cannot be understood but this can createscurio level of a hacker. It would be rather more appropriate if the secret message wereexpertly embedded in another media so that no one can guess if anything is hidden there or not.The truncation from stenography is a branch for hiding the information by flagging the confidential information inside other random information. The word steganography in Greekmeans, "covered writing" whilst Greek word stego indicates covered and graphie means writing. The keyobjective of steganography is to hide a reliable messageinside harmless disguise media in such a way that the secretmessage is not noticeable to the spectator. Thus the stenographyimage should not differ much from original cover image.In the era of development steganography is mostly used oncomputers with digital data being the carriers and networksbeing the high-speed delivery frequencies.The other type of hiding approach is the transform domain technique that appeared to overcome the robustness and imperceptibility problems found in the LSB changeovermethods.There are many alter that can be used in data hiding, the most widely used transforms are;the discrete cosine transmute (DCT) which is used in the common image density format JPEG and MPEG, the distinct wavelet transform (DWT) and the discrete Fourier transform (DFT). Mostcurrent researches are directed to the use of DWT since it is used in the new image compression format JPEG2000 and MPEG4.Inthe stealthy message is embedded into the high frequency coefficients of the wavelet transform while parting the low frequency coefficients sub-band infrangible.While in an adaptive hiding capacity function is employed to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients.The benefits of transform domain procedures over spatial domain techniques are their high ability to stand noises and some signal processing procedure but on the other hand they are computationally complicated and hence slower. In all suggested techniques for steganography whether spatial or transform the key problem is how to upturn the size of the stealthy messages without causing evidentalterations in the cover object.Some of these methods try to achieve the high whacking capacity of the cover according to its indigenous characteristics.

In Section II we ill discuss related work for decreasing the energy depletion. The Section III discusses about the different routing procedures. Section IV describes the proposed methodology and the last section concludes the paper.

2. RELATED WORK

Numerousprocedures has been proposed and implemented to boost the security of image data. In this section literature of the previous work done is described below:

Rashmi. J and Bharathi. G proposed a multi resolution wavelet domain by collaborating the concepts of steganography and cryptography. Initially we use a modified blowfish algorithm and will embed the encrypted message into an image. At the later part of the technique discrete wavelet alter is used so that the stagnated image is transformed into approximation and detailed image. The final reduced image is subjected into the receiver and the vice versa of the performance is used to obtain the plain text. The experimental results of this technique are unanimous and it’s found to be less suspicious.

Sara Nazari, Amir-MasoudEftekhari and Mohammad ShahramMoin proposed a novel steganography algorithm based on Morphology associative memory. Regularly,

steganalysis methods are formed to discover steganography algorithms using Discrete Cosine Transform and Discrete Wavelet Transform (DWT). This suppression images are mapped to morphological depiction by using morphology transform encompassing morphological coefficients and every bit of secret message is introduced in the least significant bit of morphological coefficients. To approximation stego significance, they bring to a close the feature of the cover image after embed by compare with other image transformed steganography algorithms similarly discrete cosine and wavelet transforms. The merit of stego has significantly enhanced in evaluation with the state-of-art methods. In the other conducting tests, they analysis the durability of their proposed method by using Wavelet and Block-based steganalysis methods. The result illustrates a high level of robustness of our algorithm esteem to other steganography algorithms.

N. Akhtar, P. Johri, S Khan implemented a steganography for images, with an augmentation in both security and image quality. The one that is implement now is a variation of plain LSB (Least Significant Bit) algorithm. Using bit-inversion technique enhances the stego image quality. In this method, certain least significant bits of cover image are reversed afterward LSB steganography that co-occur with a few pattern of other bits and that decreases the number of modified LSBs. Accordingly, less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stego image. By accumulate the bit patterns for which LSBs are inverted, message image can be achieve appropriately.

M. K Ramaiya; N. Hemrajani proposed work presents an elite technique for Image steganography which is based on the Data Encryption Standard (DES) through the power of S- Box mapping & private key. Embedding function using two sole S boxes passes the preprocessing of confidential image. The preprocessing provides echelon of security, as extraction is not likely without the acquaintance of mapping policy and private key of the function..In addition the proposed perception is accomplished of not just scrambling information but it also alters the strength of the pixels that contributes to the security of the encryption.

B. Geethavani E. V. Prasad proposed a Highly Secure steganography algorithm. This growth restrains three stages. In the key phase, the text is encrypted by using a conventional encryption method i.e. Caeser method. In the following stage using the chaotic neural network once more encrypts the cipher text and in the third stage the ensuing encrypted text is ingrained within the image using DWT. High security can be accomplished by encrypting the text using Chaotic Neural Network. The binary structure of the encrypted text created by chaotic neural network is changeable making it highly secure. The Proposed algorithm is tested alongside miscellaneous gray scale images considering PSNR, MSE and SSIM for approximation. It is observed that the security is improved with reasonable PSNR compared to other methods.

M. Vijay, V. Vignesh Kumar proposed an Integer Wavelet Transform is consummate on a gray level cover image and in turn embed the message bit stream into the LSB's of the integer wavelet coefficients of a the image. The main principle of the proposed work is to focus on improving embedding capacity and brings down the distortion-taking place to the stego image. The refinement of the algorithm plays an vital role for accomplishing higher embedding capacity and low distortion rate. The experimental results prove that the assessment metric such as PSNR is improved in a high mode. The experimental results show that the algorithm has a high capacity and a fine invisibility.

Seyyed Amin Seyyedi and Nick Ivanovpresented high volume payload and secure steganography technique based on integer wavelet transform. The cover image is partition into 8×8 non-overlapping blocks, and then each transformed block partitioned into two subsets and secret message is embedded in appropriate subset. To achieve higher security, Haar wavelet transform is functional to the secret message before embedding it. Experimental results indicate low degrading of the original image by hidden secret message of rather high volume.

AbhishekTripathy, Dinesh Kumar projected a secured steganography process using genetic algorithm to defend adjoining to the RS attack in color images. The proposed steganography method establish message in integer wavelet transform coefficients by using a mapping function. This mapping function based on GA in an 8x8 block on the input cover color image. Subsequent to embed the message optimum pixel modification process is functional. By applying the OPAP the fault distinction amongst the cover image and stego image is minimized. Frequency domain method is used to improve the robustness of proposed method. Usage of IWT prevents the floating-point precision evils of the wavelet filter. Genetic algorithm (GA) is used to enhance the trouncing capacity of image and preserves the quality of image. The investigational outcome show that the proposed steganography method is more secured united with RS attack as compared to existing methods. The result exhibit that peak signal to noise ratio and image consumption is 49.65 db and 100% correspondingly.

3. OVERVIEW OF IMAGE SECURITY TECHNIQUES/ ALGORITHM

This section explains the some of the techniques of image security below:

The chief terminologies used in the Steganography systems are: the cover Image, secret message, secret key and embedding algorithm. The cover note is the carter of the message such as image, video, audio, text, or some other digital media. The secret message is the information that desires to be hidden in the cover image. The secret key is usually used to embed the note depending on the trouncing algorithms. The embedding algorithm is the way or the idea that regularly use to embed the secret information in the cover message.

3.1 Integer Wavelet Transform

Integer to integer wavelet transforms maps an integer dataset into a supplementary integer dataset. This transform is entirely invertible and capitulate precisely the original dataset. A one dimensional discrete wavelet transform is a repeated filter bank algorithm. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are further. In two dimensions, we first pertain one step of the one-dimensional transform to all rows. Then, was peat the same for all columns? In the next step, we ensue with the coefficients that result from a convolution in both directions.

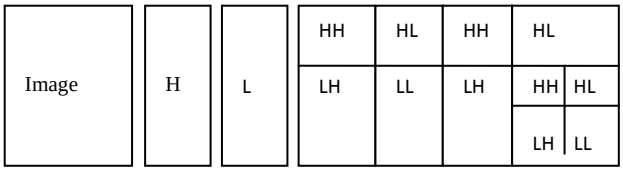

Figure 3.1 Integer Wavelet Transform

3.2 Block-DCT and Huffman Encoding

Unofficial user can easily extort hiding the confidential message/image in the distinct domain. They projected a frequency domain steganography scheme for hiding an big volume of data with high security, a good invisibility and no forfeiture of secret message. The basic indication to hide information in the frequency domain is to modify the sum of all of the DCT coefficients of cover image. The 2-D DCT convert the image blocks from spatial domain to frequency domain.

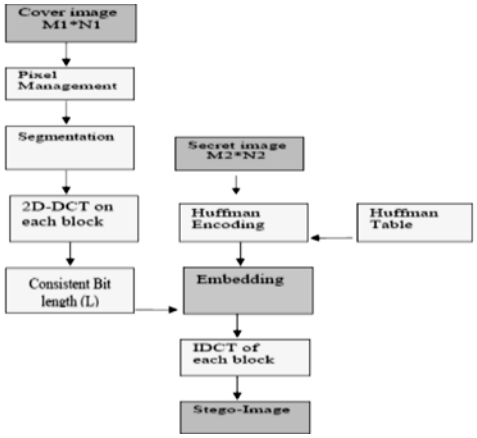

Figure 3.2 Block Diagram of Embedding Technique

The schematic/ block diagram of the whole process is given in figure (a) and (b)

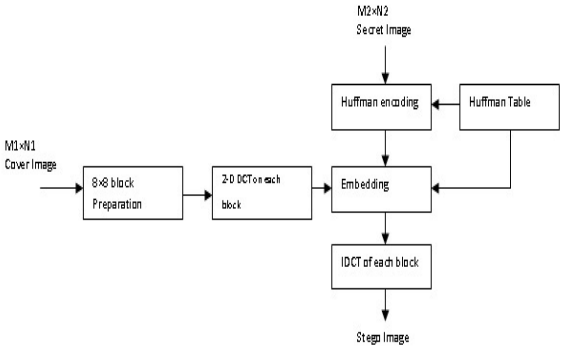

Figure 3. 2 (a) Insertion of a Secret image into a Cover image[13]

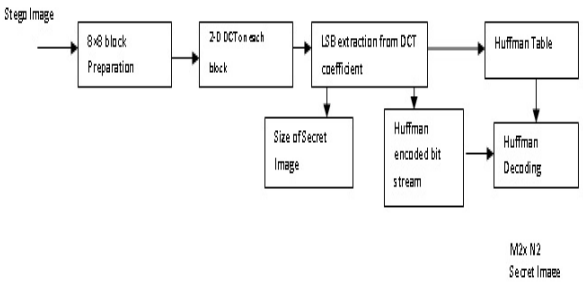

Figure3.2 (b) Removal of Secret Image [13]

Advantages

- Improvement in security & image quality
- A good invisibility
- Less distortion after embedding process
- Expected to be practical
- Provides three layers of security

Disadvantages

- Robustness is not achieved

- Can be distorted by unintended users

3.3 Genetic Algorithm

GA is a method that mimics the genetic evolution as its model to elucidate problems. The specified problem is measured as input and the solutions are coded deliberate to a pattern. The fitness function evaluate each candidate solution most of which are chosen randomly. Advancement begins from a entirely random set of entities and is recurring in subsequent generations. The most appropriate and not the bests are picked out in every creation. Our GA aim to improve the image quality. Pick signal to sound ratio (PSNR) can be a suitable valuation test. Therefore the definition of fitness function will be:

3	10	4	8	12	7

Figure 3.3. A basic chromosome with 16 genes

$$PSNR = 10Log_{10}\frac{M\times N\times 225^2}{\sum_{ij}(y_{ij}-x_{ij})^2} \qquad (1)$$

Where M and N are the image size and, x and y is the image intensity values before and after embedding equally. A solution to the problematic is translated into a list of parameters recognized as chromosomes. These chromosomes are habitually displayed as modest strings of data. At the initial step, quite a few characteristics are generated for the predecessor generation haphazardly and the pertinent proportionality value is measured by the fitness function. A chromosome is encoded as an array of 16 genes contains permutations 1 to 16 that point to pixel numbers in each wedge. All chromosome produce a mapping function as shown in “Figure 3.3”. The subsequent step associates with the base of the second generation of the culture that is based on selection processes via genetic operators in accordance with the earlier set characteristics. A duo of parents is designated for each individual. Selections are devised so that to find the mainly apt component. In this way, even the weakest components appreciate their own chance of mortal designated and local solutions are bypass. This paper employs Tournament method. The contents of the two chromosomes that enter the generation process are interact to produce two newborn chromosomes. In this methodology two of the bests are diverse to give an admirable one. In addition, during each process, it is likely for a series of chromosomes to undertake mutations and breed a following generation of unlike characteristics.

3.4 Discrete Wavelet Transforms

The simplest of DWT is Haar - DWT where averaging the two pixel values generates the low frequency wavelet coefficients and captivating half of the difference of the same two pixels generates high frequency coefficients. For 2D-images, applying DWT will result in the partition of four different band. LL is the lower resolution approximation of the image. HL is the horizontal, LH is the vertical, HH is the diagonal component. These bands are shown in Figure 3.4.

With the DWT, the significant part (smooth parts) of the spatial domain image exist in the estimate band that consists of low frequency wavelet coefficients and the edge and texture details generally exist in high frequency sub bands, such as HH, HL, and LH. The secret data are embedded to the High Frequency components, as it is difficult for the human eye to detect the existence of secret data.

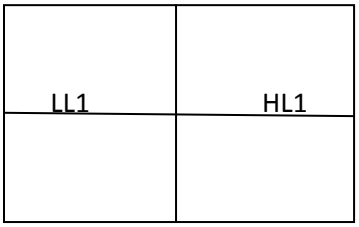

Figure 3.4. Components of 1 level 2 dimensional Discrete Wavelet Transform

3.5 Rounding Method

Rounding method is a way for embedding secret message bits in cover image. The pixel value is modifying into the adjacent integer with the last LSB bits equal to the enter bits. For example, assume that capacity of the current pixel is found to be 3 bits. Then, the current pixel is equal to 160 or (10100000)2 and the input bits are equal to (101)2. According to the rule described above, the value of pixel is changed into 157 or (10011101)2. The mathematical figure of rounding method is.

$$y = x + A \times B(A \le B) - B(B < A) \qquad (2)$$

$$A = mod(m - x, 2^c) \qquad (3)$$

$$B = mod(x - m, 2^c) \qquad (4)$$

where y, x, m, and c denote the output value, input value, secret message and capacity respectively.

3.6 Least Significant bit

LSB method is efficient in spatial domain. The method renovates image into sheltered gray scale image. This image will be performing as reference image to hide the text. Using this grey scale reference image any text can be hidden. The solo character of a text can be representing by 8-bit. If the reference image and the data file are transmitted through network independently, they can

achieve the consequence of Steganography. Currently the image is not at all distorted because said image is only used for referencing. Every enormous amount of text material can be concealed using a also trivial image. Decipher the text is not capable intercepting the image or data file independently. Therefore, it is more secure. In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". Therefore, this property is used to hide the data in the image. Here we have measured last two bits as LSB bits as they will affect the pixel value only by "3". This facilitates in storing extra data. The Least Significant Bit (LSB) steganography is one such method in which least significant bit of the image is substitute with data bit. Since this method is susceptible to stegano-analysis so as to make it additional secure they encrypt the raw data before embed it in the image. Nevertheless the encryption procedure increases the time density, but at the same time provides higher security also. This approach is very effortless.

In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains - for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today. From one of our reference paper we found that in LSB steganography, to conceal the message the least significant bits of the cover media's digital data are used. The useful feature of the LSB steganography techniques is LSB replacement that makes LSB steganography as simple. To reflect the message it needs to be hidden, LSB replacement steganography flips the last bit of each of the data values. Consider an 8-bit gray scale bitmap image where each pixel is stored as a byte and it also representing in a gray scale value.

3.7 Blowfish Algorithm

Blowfish is a symmetric block ciphers which usage a festal network of 16 rounds of iterative encryption and decryption functional design. The block size of blowfish algorithm is 64 bits and the size of the key possibly will be of several lengths but having a extreme range cultivate 448 bits. The influence of the Blowfish algorithm relies on its sub-key generation and its encryption. Blowfish cipher uses 18 P-boxes and four Substitution boxes each of 32-bit size. It utilizes a Fiestal cipher that is a universal method of transforming a function into alternative function by using the outset of permutation. The functioning of blowfish cipher can be exhibits as follows. It splits the 64-bit block into two equal blocks having 32-bit size each. Left block is XORed with first sub array P1 and consequently obtained result is fed into a role called F-function. Inside the F-function replacement operations are conceded out which in turn converts 32 bit blocks in to another 32 bit blocks. Consequently resulted 32bit entries are XORed with the Right half and the result obtained is swapped as the left half for the next round. Therefore subsequent to the successful success of each round Right half becomes the fresh left half or vice versa and Fiestal configuration is followed up to 16 rounds. The consequential left and right halves are not exchanged but XORed with the seventeenth and eighteenth P-arrays. Modified F-function plays a momentous role in the algorithm and they decided to transform function F. main function F is defined as follows

$$F(x) = ((S1 + S2 mod 232) XOR\ S3 + S4 mod 232 (5)$$

Instead, we customized the F-function by replacing 2 addition operations as XOR Operations and one circular shift operation. Thus the modified F-function is written as, F(X) =CS ((S1 XOR S2 mod 232) + (S3 XOR S4 mod 232)). This amendment leads to the parallel implementation of two XOR operations. In the case of original F-function that executes in sequential order and it requires 32 Addition operations and 16 XOR operations. However, in the case of our modified F-function it requires the same 48 gate operations (32-XOR, 16-addition) but time taken to implement these 48 operations will be reduced because of parallelism. We executed 32 XOR operations in parallel order via threads and henceforth time taken to complete 16 gate operations will be equal to the time taken to complete 32 XOR operations since they are running it in parallel situation. After that we are performing 32 bit circular shift operation which further enhances the security of the system. The block diagram of the modified F-function is shown in Figure 3.7

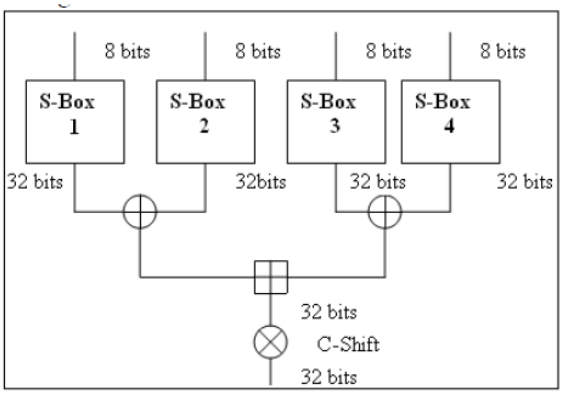

Figure 3.7 Modified F-function of 32- bit

4. CONCLUSION

The security of image data is develop into very necessary these days because most of the transmission is done via Internet. So many of techniques has been projected or implemented to enhance the security of image such as steganography, cryptography etc. In this thesis presents the literature study of different method for securing image data and steganography with wavelet and security algorithms in which some of the method is improved for execution time and some introduces the inaccuracy between the stego image and cover image. In future work, develop such process that can reduce the execution time and can reduce the error efficiently

5. REFERNCES

[1]. Komal Hirachandani, Gaurav Soni, Rajesh Nigam "New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric Encryption", International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6253-6260, ISSN: 0975-9646.

[2]. A. Antony Judice, Dhivya Shamini. P, Divya Sree. D. J, Lekshmi Sree. H. A. "An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[3]. Rashmi. J, Bharathi. G, "A Wavelet Transform Based Secure Data Transfer Using Blowfish Algorithm", IJCSMC, Vol. 3, Issue. 2, February 2014, pg.794 – 803, ISSN 2320–088X.

[4]. Sara Nazari, Amir-Masoud Eftekhari, Mohammad ShahramMoin "Secure Information Transmission using Steganography and Morphological Associative Memory", International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, January 2013.

[5]. N. Akhtar, ; P. Johri, ; S Khan, "Enhancing the Security and Quality of LSB Based Image Steganography" 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013 , Page(s): 385 – 390

[6]. M.K Ramaiya. ; N.Hemrajani, A.KSaxena, "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013 , Page(s): 1094 – 1099.

[7]. B. Geethavani E. V. Prasad "High Secure Image Steganography Based On Hopfield Chaotic Neural Network and Wavelet Transforms", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014

[8]. M.Vija , V.Vignesh Kumar "Image Steganography Method UsingInteger Wavelet Transform", 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14), Volume 3, Special Issue 3, March 2014 ISSN (Online) : 2319 – 8753.

[9]. Seyyed Amin Seyyedi and Nick Ivanov " High Payload and Secure Steganography method Based on Block Partitioning and Integer Wavelet Transform", International Journal of Security and Its Applications Vol.8, No.4 (2014), pp.183-194.

[10]. AbhishekTripathy, Dinesh Kumar, " Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014 ISSN: 2277 128X.

[11]. G.J.Simmons, "Thebprisoner's problem and the subliminal channel", in proceedings of Crypto'83,pp.51-67,1984

[12]. http://en.wikipedia.org/wiki/Steganography

[13]. Gonzalez, R.C. and Woods, R.E., Digital Image Processing using MATLAB, Pearson Education, India,2006.

[14]. S. Sarreshtedari, M. Ghobi and S. Ghaemmeghami, "High Capacity Image Steganography in Wavelet Domain", The 7th Annual IEEE Consumer Communications and Networking, (2010), pp. 1-5.

[15]. M. Pavani1, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods" International Journal Of Engineering And Computer Science ISSN:2319-7242

[16]. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, 1995

[17]. G. Manikandan, G. Krishnan, and N. Sairam, "A unified block and stream cipher based file encryption," Journal of Global Research in Computer Science, vol. 2, no. 7, pp. 53-57, 2011.