**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 2, February 2014, pg.794 – 803***

**RESEARCH ARTICLE**

# A Wavelet Transform Based Secure Data Transfer Using Blowfish Algorithm

**Rashmi.J[1], Bharathi.G[2]**

[1]PG Scholar, Department of Electronics and Communication, SRM University, Chennai

[2]Assistant Professor, Department of Electronics and Communication, SAMS College of Engineering, Chennai

rash89ashok@gmail.com [1], bharathi.aume@gmail.com [2]

***Abstract-- The modern era has seen ample number of cryptographic and stenographic techniques to transmit and receive data in a secure and confidential manner. In our paper we use 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 transform 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 technique is used to obtain the plain text. The experimental results of this technique is unanimous and it's found to be less suspicious.***

***Keywords: Blowfish, Cryptography, F-function, multi-resolution, security, steganography, wavelet***

## I. INTRODUCTION

Steganography and Cryptography are two important and famous techniques which are used to encoding and hiding of data. More specifically, Steganography is a technique which hides the existence of the message itself. Thus a Steganographic system hides the content inside any multimedia content and this process of hiding the text inside an image or an audio file or a video file is referred as "Embedding process". On the other hand, cryptography protects information by transforming it into an unreadable format [16]. The original text is transformed into a scramble equivalent text called cipher text and this process is called as "Encryption". This is achieved via an Encryption Algorithm. Only those who possess a secret key can decrypt the cipher text into plaintext. The wavelet transform (WT) [3], which is characterized by a dilation and translation factors to overcome a Fourier transform. Many types of wavelet, such as Haar wavelet, Daubechies wavelet [4], the morelet wavelet and maxican-hat wavelet exists, among which Haar Wavelet is most simple and easiest wavelet of its kind. Let us consider two samples (say *a* and*b)*. A simple arithmetic transform is done which transforms a and*b* into their average s and difference d respectively.

$$s = (a+b)/2$$
$$d = b - a \qquad (1)$$

The main goal to be achieved is to minimize the size (i.e., in bits) needed for *d*, and this can be achieved easily if and only if *a* and*b* are highly correlated. This calculation for inverse transform can be carried out as follows to regain *a* and*b*:

$$a = s - d/2$$
$$b = s + d/2 \qquad (2)$$

Conceptually, Haar wavelet is very simple because it is constructed from a square wave [15]. Moreover, Haar wavelet computation is fast since it only contains only two coefficients and it does not need a temporary array for multi-level transformation [18]. Thus, each pixel in an image that will go through the wavelet transform computation will be used only once and there will be no pixel overlapping. Then a simple two point length averaging and differencing basis can be written as

$$a(n) = \begin{cases} 1/2, n = k, k+1 \\ 0, elsewhere \end{cases} \qquad (3)$$

$$d(n) = \begin{cases} 1/2, & n = k \\ -1/2, & n = k+1 \\ 0, & elsewhere \end{cases} \qquad (4)$$

Where a (n) denote approximation and d (n) details of a decomposed image.

The rest of the paper is organized as follows: Section 2 gives us the literature review of the techniques used in our proposed system. Section 3 provides an insight to the proposed system. The simulation and snapshots of our experiment is given in Section 4. Section 5 is a brief security analysis of the approach used in the experiment. Section 6 gives the conclusion to the approach defined in this paper.

## II. RELATED WORKS

Lot of research has been done in this area in the recent past and various techniques of cryptography and steganography have been suggested. In [8] a new approach for enhancing data security by combining the two basic types of ciphers, namely stream ciphers and block ciphers was proposed. Further this approach was modified and instead of using both the ciphers on the plain text, one was used on the key and the other on the plain text [9].

A hybrid system was proposed by integrating cryptography and steganography along with compression in order to improve the overall security of a system [10]. In [12] usage of multilevel cryptographic schemes was introduced which helped in enhancing the security of a cryptographic system.In order to decrease the execution time of blowfish algorithm, a system with a modified F-function was suggested [17].

Our aim in this paper is to reduce the size of the Steg image without the loss of any information. For the same purpose, we have used wavelet transform.

### *A The Haar Wavelet Properties*

1. Orthogonality: The original image is divided into low and a high frequency parts and this can be enabled by using filters.

2. Compact Support: The magnitude response of the filter should be exactly zero outside the frequency range covered by the transform. If this property is satisfied, the transform is energy invariant.

3. Perfect Reconstruction**:** If the input image is transformed and inversely transformed using a set of weighted basis functions and the reproduced sample values are identical to those of the input image, the transform is said to have the perfect reconstruction property. If, in addition no information redundancy is present in the sampled image, the wavelet transform is, as stated above, ortho normal.

4. Best performance in terms of computation time.

The above properties motivate us to use this transform in our proposed work.

### *B Cryptography*

Cryptography is the study and practice of protecting information by data encoding and transformation techniques [16]. There are two types of cryptographic schemes available on the basis of key namely *symmetric key Cryptography* and *Asymmetric or Public Key Cryptography*. We can also classify symmetric key cryptography into two types on the basis of their operations as *Stream and. Block Ciphers*. We have chosen block cipher for our cryptographic operation since it is the main tool for implementing private key encryption in practice.

*C Steganography*

This is a type of security technique which is of the form "security through hiding". Steganography is the art of hiding data through carriers which are comparatively larger in size than the original message and is an effort to conceal the existence of data Domenico, et.al, [1].

In this method the data which is to be sent is concealed in any multimedia file like image, video or an audio file. There are many famous steganographic techniques exist worldwide. The most frequently used techniques are, LSB Insertion, Fingerprinting and Watermarking, Transform Based Steganography, Public key Steganography. We have taken LSB Insertion method in which the data is hidden inside the Least Significant Bits of the image. On the basis of hiding the text inside the multimedia contents, we can classify the Steganography into Image Steganography, Audio Steganography and Video Steganography. We are going to deal with Image Steganography and hence hereafter if we refer Steganography it actually refers to image Steganography.

*D Wavelet Based Steganography*

Po-Yueh, et.al, [2] proposed a new steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality.

Some basic mathematical operations are performed on the secret messages before embedding. These operations and a well-designed mapping Table keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security.

Mythreyi, et al, [11] proposed a scheme for steganography namely Gabor Transform Based Image Steganography (GTIS). In this scheme, image steganography is achieved using Gabor compression. In normal methods of steganography, the secret message is distributed in all pixels whereas in this scheme the distribution of secrete message is more in high complex areas and less in low complex areas.

Moreover for embedding the secret message over the image, pixel positions are obtained by pseudo random number generator. Wavelets are extended to the domain Steganography which hides the message. Here at the end of embedding process, messages are transformed into DHWT wavelet coefficients which are simply decomposed signals and images. Recomposing or reconstruction is done by undergoing inverse DHWT which exactly reconstructs stego-image without any loss.

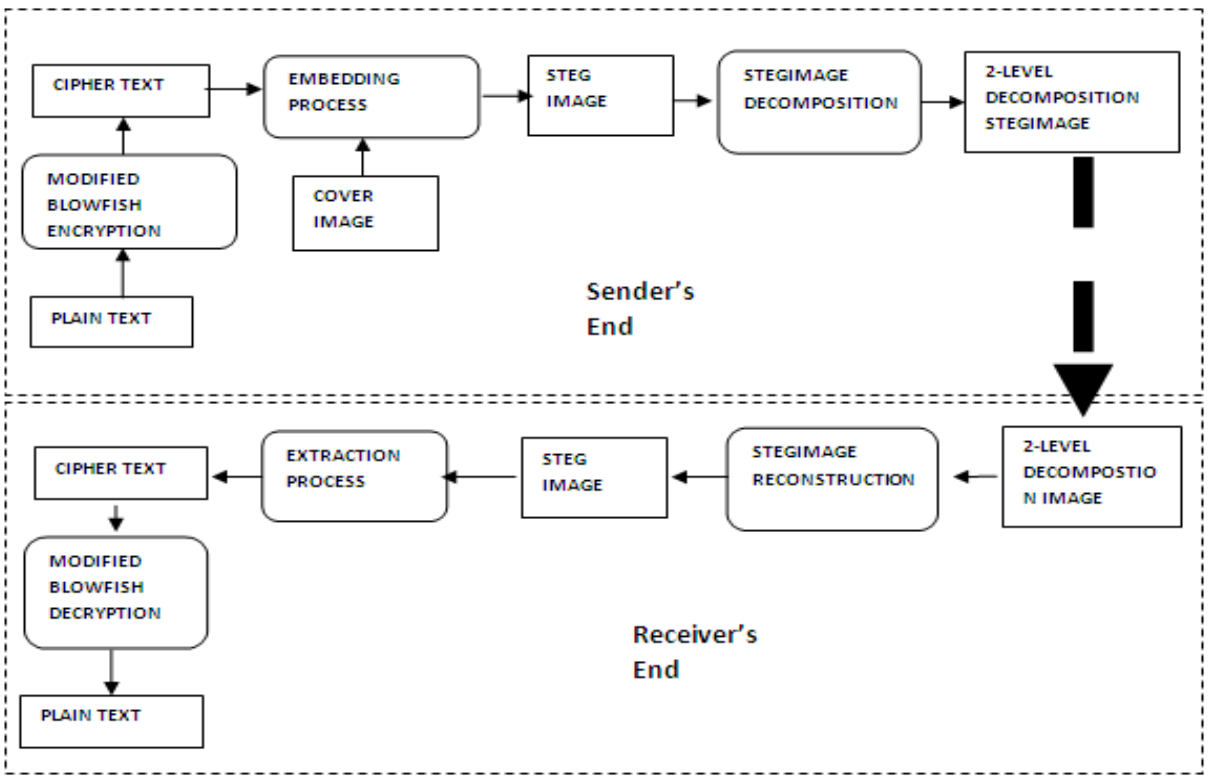



*Figure 1 WCSM (Wavelet Crypto-Stegno Model)*

## III. THE PROPOSED SYSTEM

In the Proposed system, we have effectively combined Cryptography, Steganography and Discrete Wavelet Transform in deriving a new hybrid model for transmitting the message in a highly secured manner. We made this attempt in order to make the system theoretically and practically unbreakable. The steps involved in our approach are as follows:

1. Getting Plaintext which is to be sent to the recipient from the user.

2. Transformation of plaintext in to cipher text by undergoing an encryption process using the modified cryptographic algorithm.

3. Embedding the cipher text inside any cover image using a Steganographic algorithm.

4. Furthermore the obtained Steg image is decomposed into approximation and details using 2D Discrete HaarWavelet(DHWT)

5. Thus the reduced approximation image is communicated through any communication channel to the receiver.

The inverse of these steps will be taken place in the receiver side which are as follows:

6. The Received image is reconstructed using 2D Inverse Discrete Haar Wavelet Transform.(IHWT)

7. Extraction Process will be carried out which separates the embedded message from the Steg image.

8. Thus obtained message will be in the scrambled form, so decryption is performed.

9. Finally, the receiver can able to read the actual secret message sent at the sender's end.

The block diagram of our proposed approach is shown in Figure 1.

*A Cryptographic Approach*

In this work, the Blowfish encryption algorithm is chosen for Encryption since,

- It is a symmetric block cipher which can take a variable-length key, from 32 (4 Bytes) bits to 448 bits (56 Bytes);
- It is fast, strong and free and hence an alternative to existing encryption algorithms [13];
- It is suitable and efficient for hardware implementation;
- It uses only simple operators which include addition, table lookup and XOR. The table includes four S-boxes (256~32bits) and a P-array (lXx32bits).

(1) Blowfish Algorithm

Blowfish, a symmetric block cipher uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size of blowfish algorithm is 64 bits, and the size of the key may be of any length but having a maximum range till 448 bits. The power 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 uses a Fiestal cipher which is a general method of transforming a function into another function by using the concept of permutation. The working of blowfish cipher can be illustrated 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 thus obtained result is fed in to a function called F-function. Inside the F-function substitution operations are carried out which in turn converts 32 bit blocks in to another 32 bit blocks.

Thus resulted 32bit entries are XORed with the Right half and the result obtained is swapped as the left half for the next round. So, After the successful completion of each round Right half becomes the new left half or vice versa and Fiestal structure is followed up to 16 rounds. The resultant left and right halves are not swapped but XORed with the seventeenth and eighteenth P-arrays.

(2) Modified F-function

Function F plays an important role in the algorithm, and we decided to modify function F. Original function F is defined as follows [14].

$$F(X) = ((S1 + S2 \bmod 232) \text{ XOR } S3) + S4 \bmod 232$$

Instead, we modified the F-function by replacing 2 addition operations as XOR Operations and one circular shift operation. Thus the modified F-function is written as,

$$F(X) = CS ((S1 \text{ XOR } S2 \bmod 232) + (S3 \text{ XOR } S4 \bmod 232))$$

This modification leads to the parallel execution of two XOR operations. In the case of original F-function which executes in sequential order and it requires 32 Addition operations and 16 XOR operations. But in the case of our modified F-function it requires the same 48 gate operations (32-XOR, 16-addition) but time taken to execute these 48 operations will be reduced because of parallelism. We executed 32 XOR operations in parallel order using threads and hence time taken to complete 16 gate operations will be equal to the time taken to complete 32 XOR operations since we are running it in parallel environment [8]. 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 2.

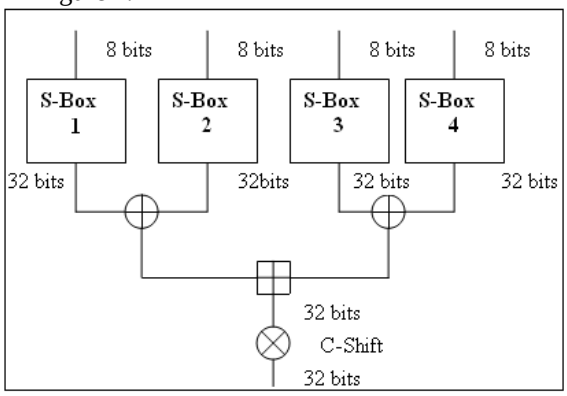



*Figure 2 Modified F-function*

*B Steganographic Approach*

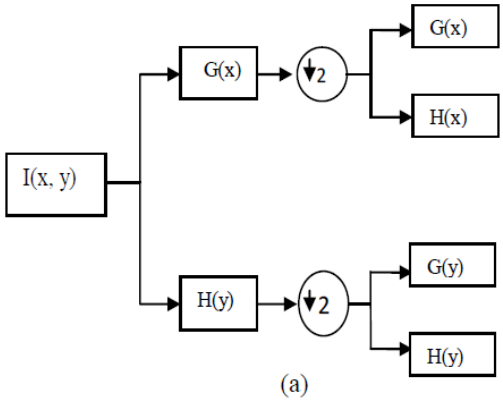
In the case of Steganographic algorithm we chooses LSB Hiding algorithm which hides the very presence of the text inside an image. Least Significant Bit (LSB) insertion is a simple approach to hide information in any multimedia cover file: it overwrites the LSB of a pixel with an M's bit. We can able to hide 3 bits per pixel in a 24-bit cover image. Hence the resulting Stegimage will make no difference to the cover image to human eyes [6].

*C The Discrete Haar Transform*

A stegimage that undergoes Haar wavelet transform will be divided into four frequency bands (LL, LH, HL, HH) at each of the transform level [8]. The first band represents the input stegimage filtered with a Low Pass Filter(LPF) which compresses the image into half of its original dimension (i.e., an image of X x Y is decomposed into X/2 x Y/2. This band is also called 'approximation' (LL), which contains more energy of Stegimage. The other three bands are called 'details' (LH, HL, and HH) where High Pass Filter (HPF) is applied. These bands contain directional characteristics. Specifically, the second band contains vertical characteristics, the third band shows characteristics in the horizontal direction and the last band represents diagonal characteristics of the input image. Since image is of two-dimension, performing wavelet transform is done twice in each of its level. First, it is done at row wise and then at column wise.

The low pass filter is denoted by G(x) while the high pass filter is denoted by H(x). At each level, the high pass filter produces detail information; while the low pass filter associated with scaling function produces coarse approximations [19]. After successfully decomposing the stego-image, we sent 'approximation' (2-level LL band) of stego-image to the receiver side. Then receiver uses Inverse Haar Wavelet Transform (IHWT) to reconstruct the original size of stego-image with help of 'details' bands.



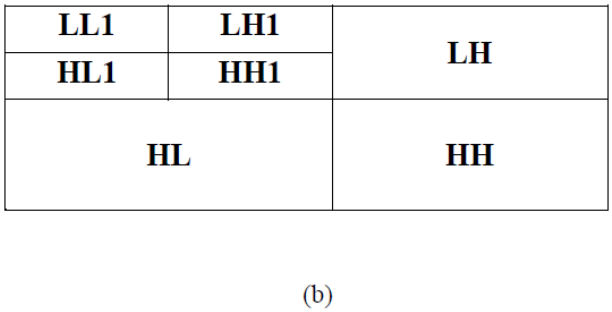




*Figure 3The 2-level wavelet decomposition. (a) Block diagram for a 4-band wavelet decomposition (b configuration of 2-level wavelet decomposition*

*D Significance of the Hybrid Model*

We integrated three different techniques which determine the security of the data. They are,

- Enciphering & Deciphering phase with the Cryptography;
- Embedding & Extraction of data with the Steganography;
- Image Decomposition and reconstruction using 2D DHWT and IDWT respectively.

1. While F-function is executed, time taken to perform 32 logical operations in sequential order is considerably reduced to time taken to perform 16 logical operations due to parallelism [7].

2. it's quite hard for the eavesdroppers to realize that the F-function is modified and hence probability of attack is less on comparing with the original Blowfish algorithm.

3. If in case Steganalysis is performed and hence the LSB algorithm is breaked, there is yet another a struggle for intruders to cryptanalysis the cipher text which is considered to be very hard as far as the strength of Blowfish algorithm is concerned.

4. Intruder may not have chance for guessing the presence of any message since the image is of very small in size.

5. Because of its size it is easy to transmit the image even with minimum available bandwidth.

6. The uniqueness in this approach is, for reconstructing the image the receiver needs a key that is the image details components.

7. Even the intruder reconstruct from decomposed image but they don't know levels of reconstructions. Since reconstruction depends on level of detail components.

## IV. SIMULATION

We simulate the hybrid model using Java Development Kit, because of its better GUI features, robustness and platform independent features.

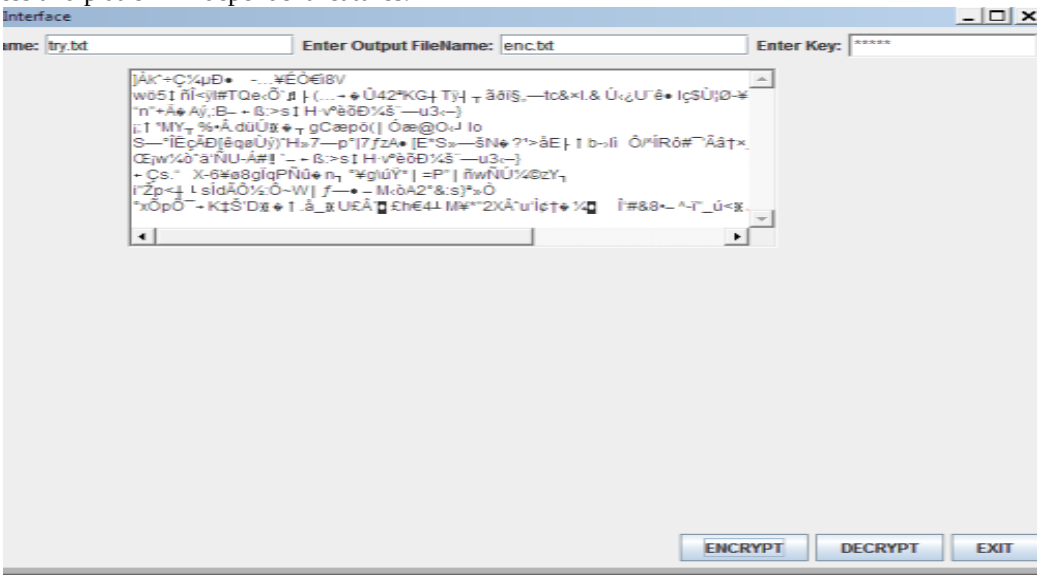



*Figure 4 Encryption process*

Figure 4 is a snapshot of the encryption process. This encrypted text is embedded in an image of size 256x256 which is shown in Figure 5. After this we reduce the image into 128x128 which is shown in Figure 6.


*Figure 5Stego-image with size 256x256*

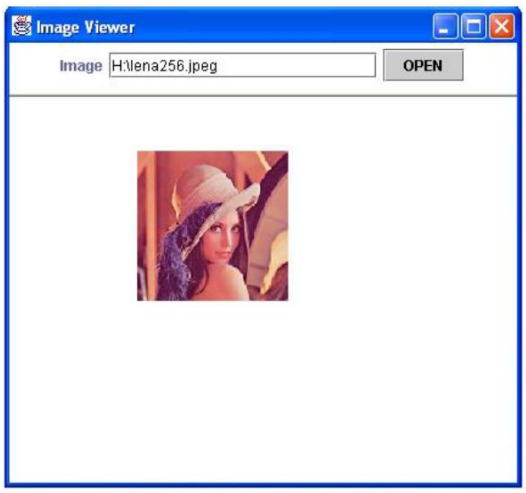



*Figure 6 Reduced Stego-image with size 128x128*


*Figure 7 Reconstructed original Image with size 256X256*

From the 128x128 image we reconstruct the original image and obtain an image of size 256x256 which is shown in Figure 7. After this the cipher text is extracted from the image and then the decryption process takes place which gives us our original plain text. This decryption process is illustrated in Figure 8.

## V. SECURITY ANALYSIS

Since our proposed system brings modifications only to the order of execution in the blowfish algorithm and no changes are made to the actual functionalities (i.e., we did not add or remove any operations, rather we have changed only the order of execution of existing XOR and Adders) so performing cryptanalysis is not necessary. Since this approach uses a combination of modified cryptographic and steganographic approach it enhances the overall security of the system and hence is difficult for an intruder to gain access to the plain text.

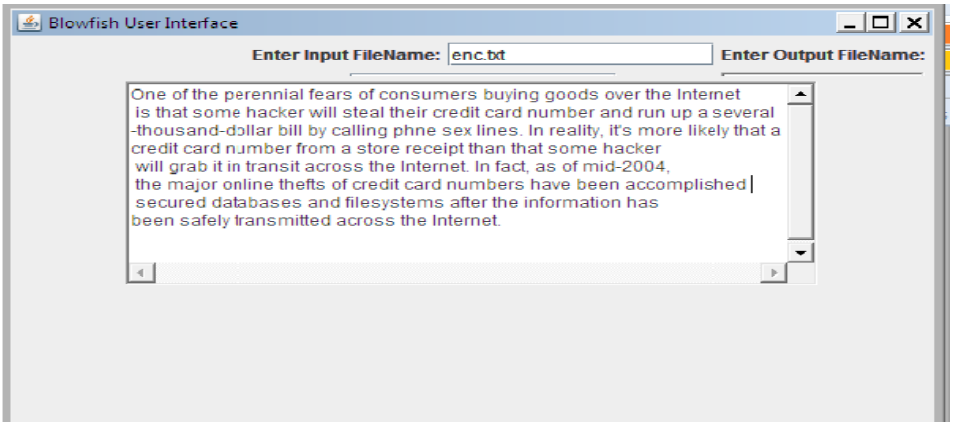



*Figure 8 Decryption process*

## VI. CONCLUSION

In this paper we have presented a novel method enhancing security using modified Cryptography and Steganography. We have proven that this hybrid approach is both an effective steganographic method as well as a theoretically unbreakable cryptographic one since the F-function is modified and hence hard to guess. The highlight of this approach is the image can be perfectly reconstructed and the message can be retrieved without any loss since we have used 2D DHWT. In Future this work can be extended for video data.

## REFERENCES

[1] D. Bloisi and L. Iocchi., "Image based Steganography and cryptography," *International Conference on computer vision Theory*, vol. 1, pp. 127-134, 2007.

[2] P. Chen and H. Lin, "A DWT Based Approach for Image Steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275-290, 2006.

[3] I. Daubechies, *Ten Lectures on Wavelets, Philadelphia*, PA: SIAM, 1992.

[4] I. Daubechies, "The wavelet Transform, time-frequency localization and signal analysis," *IEEE Transactions on Information Theory*, vol. 36, pp. 961- 1005, Sept. 1990.

[5] L. Driskell, "Wavelet-based Steganography," *Crypto-logia*, vol. 28, no. 2, pp.157-174, 2004.

[6] N. F. Johnson, Z. Duric, and S. Jajodi, *Information hiding: Steganography and watermarking: attacks and countermeasures*, 3rd ed., Kluwer Academic Publishers, 2003.

[7] G. N. Kishnamurthy, V. Ramaswamy, and G. H. Leela, "Performance enhancement of blowfish algorithm by modifying its function," in *Proceedings of International Conference on Computers, Information,*

*System Sciences and Engineering*, pp. 240-244, 2006, University of Bridgeport, Bridgeport, CT, USA.

[8] 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.

[9] G. Manikandan, R. Manikandan, P. Rajendiran, G. Krishnan, and G. SundarGanesh, "An integrated block and stream cipher approach for key enhancement," *Journal of Theoretical and applied information Technology*, vol. 28, no. 2, pp. 83-87, 2011.

[10] G. Manikandan, M. Kamarasan, P. Rajendiran, and R. Manikandan, "A hybrid approach for security enhancement by modified crypto-stegno scheme," *European Journal of Scientific Research*, vol. 60, no. 2, pp. 224-230, 2011.

[11] S. Mythreyi and V. Vaidehi, "Gabor transform based image steganography," *IETE journal of research*, vol. 53, no. 2, pp. 103-112, 2007.

[12] N. Sairam, G. Manikandan, and G. Krishnan, "A
novel approach for data security enhancement using multi level encryption scheme," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 1, pp. 469-473, 2011.

[13] B. Schneier, "description of a new variable-length key, 64-bit block cipher (blowfish)," in *Proceedings of Fast Software Encryption, Cambridge Security Workshop*, pp. 191-204), Springer-Verlag, 1994.

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

[15] C. Shremmer, "Decomposition strategies for wavelet-based image coding," *International Symposium on Signal Processing and its Applications*, vol. 2, pp. 529-532, 2001.

[16] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 2nd ed., Prentice Hall,1999.

[17] V. Vaidhiyanathan, G. Manikandan, and G. Krishnan, " A novel approach to the performance and security enhancement using blowfish algorithm," *International Journal of Advanced Research in Computer Science*, vol. 1, no. 4, pp. 451-454, 2010.

[18] M. Vetterli, *Wavelets and Subband Coding*, 1st ed., Prentice Hall, 1995.

[19] S. G. Wallat, "A theory for multiresolution signal decomposition:the wavelet representation," *IEEE Transaction on Pattern Analysis and Machine Intelligence*., vol. 11, no. 7, pp. 674-693, 1989.

## ABOUT THE AUTHORS

**Rashmi. J** was born on 1989 in Chennai. She received her master's in Communication systems from SRM University, Chennai in 2013. She received her bachelor's in Electronics and Communication from SMK Fomra Institute of Technology in 2011. Her area of interest includes network security, wireless networks, communication systems and Adhoc networks. Her subject of interests include cryptography & network security, signals & systems, Digital signal Processing and Wireless networks.

**Bharathi. G** was born on 1989 in Chennai. She is currently an Assistant Professor in Department of Electronics and Communication in SAMS College of Engineering, Chennai. She received her master's in VLSI design from Anna University Chennai in 2013. She received her bachelor's in Electronics and Communication from ShakthiMariamman Engineering College in 2007. Her area of interest includes Network security, digital electronics, VLSI degign, Digital signal processing and wireless sensor networks. Her subject of interests include cryptography & network security, Adhoc networks, WSN and Communication theory.