# Image Steganography using DWT and Blowfish Algorithms 

${ }^{1}$ Mrs.Archana S. Vaidya, ${ }^{2}$ Pooja N. More., ${ }^{3}$ Rita K. Fegade., ${ }^{4}$ Madhuri A. Bhavsar., ${ }^{5}$ Pooja V. Raut.<br>${ }^{1}$ Asst. Prof. Department of Computer Engg.<br>GES's R. H. Sapat College of Engineering, Management Studies and Research, Nashik (M.S.), INDIA


#### Abstract

We propose a steganography technique which embeds the secret messages in frequency domain. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. A cryptography algorithm is used to convert the secret messages to an unreadable form before embedding. These algorithms keep the messages from stealing, destroying from unintended users on the internet and hence provide satisfactory security. Blowfish algorithm is used for encryption and decryption of text message using a secret-key block cipher. Blowfish is an evolutionary improvement over DES, 3DES, etc designed to increase security and to improve performance. This algorithm uses a variable key size up to 448 bits.


Keywords: Steganography, security, information hiding cryptography, wavelet transform.

## I. Introduction

Steganography and Cryptography are two popular ways of sending vital information in a secret way. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Cryptography scrambles a message so it cannot be understood and Steganography hides the message so it cannot be seen.

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

In our project we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security.

## II. Motivation And Background

Security system is a system that provides authentication. Security systems can be divided into two parts:

- Cryptography and
- Information hiding

Information hiding is also divided into parts Steganography and watermarking[1].There are various types of Steganography: Image, Video, Audio and Text. The most popular cover object is image to perform steganography. Image steganography is divided into spatial and transform domain. In spatial domain messages are embedded in the intensity of image pixel like in LSB. Whereas in transform domain, image is first transformed and them message is encoded like discrete cosine transform (DCT), discrete wavelet transform (DWT) and many others.

## III. Architecture

In our system we use cryptography and steganography together. We first enrypt the message to be sent using blowfish algorithm and then hide it in our image.Before hiding, the image is transformed using DWT algorithm. The message is extracted and using DWT and decrypted to get original message. Figure 1 illustrate the block diagram of system.


Figure 1: Block Diagram of System
Sender side:
1.Write text message.(original message).
2.Encrypt message using Blowfish algorithm.
3. Select cover image.
4.Use DWT algorithm for transforming the image and then hide the message into image to get the stego image.

Receiver side:
1.Receive the stego image.
2.Use DWT algorithm to extract message from image.
3. Decrypt message using Blowfish algorithm.
4.Get original message.

## IV. Blowfish Algorithm

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.

- It has as a scalable key, from 32 bits to at least 256 bits.
- Uses simple operations that are efficient on microprocessors. e.g. exclusive-or, addition, table lookup, modular- multiplication.[2] It does not use variable-length shifts or bit-wise permutations, or conditional jumps.
- Employs precomputable sub keys. On large-memory systems, these sub keys can be precomputed for faster operation. Not precomputing the sub keys will result in slower operation, but it should still be possible to encrypt data without any precomputations.
- Uses sub keys that are a one-way hash of the key. This allows the use of long passphrases for the key without compromising security.


Figure 2: Feistel structure of blowfish algorithm

- Uses a design that is simple to understand. This facilitates analysis and increase the confidence in the algorithm. In practice, this means that the algorithm will be a Feistel iterated block cipher as shown in fig 2.
- The Algorithm used for Decryption and Encryption is same.
- It uses same Feistel structure of blowfish algorithm but the only difference is Decryption algorithm takes Cipher text as input and converts it into original plain text.

The P-array and S-array values used by Blowfish are pre-computed based on the user's key. In effect, the user's key is transformed into the P-array and S-array. The key itself may be discarded after the transformation. The P-array and S-array need not be recomputed (as long as the key doesn't change), but must remain secret. Computation of the P and S arrays can be summarized as follows [2]:

- $P$ is an array of eighteen 32-bit integers.
- $S$ is a two-dimensional array of 32 -bit integer of dimension $4 \times 256$.
- Both arrays are initialized with constants, which happen to be the hexadecimal digits of $\pi$ (a pretty decent random number source).
- The key is divided up into 32-bit blocks and XORed with the initial elements of the P and S arrays. The results are written back into the array.
- A message of al 1 zeros is encrypted and the results of the encryption are written back to the P and S arrays. The $P$ and $S$ arrays are now ready for use.


## V. Discrete Wavelet Transform (DWT)

The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2.[3]The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. Human eyes are less sensitive to the high frequency signals.


Figure 3: Block Diagram of 1-D foward DWT
Our eyes will average fine details within the small area and record only the overall intensity of the area. The procedure of one dimensional (1-D) DWT is shown in figure 3.

In case of 2-D DWT, the input data is passed through set of both low pass and high pass filter in two directions, both rows and columns. The outputs are then down sampled by 2 in each direction as in case of 1D DWT. As shown in Figure 4, output is obtained in set of four coefficients LL, HL, LH and HH. The first alphabet represents the transform in row where as the second alphabet represents transform in column.

The alphabet L means low pass signal and H means high pass signal. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively.[3]


Figure 4: Block Diagram of 2-D foward DWT

The output of 1D DWT is illustrated in figure 5(a).


Figure 5(a): Illustration of 1D DWT
The output of 2D DWT is illustrated in figure 5(b).


Figure5 (b): Illustration of 2D DWT

## VI. Haar DWT

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT .A 2dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one.[3]
Detailed procedures of a 2-D Haar-DWT are described as follows:
Step 1: At first, scan the pixels from left to right in horizontal direction. Then perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 6. 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).


Figure 6: The horizontal operation on the first row.

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 7.


Figure 7: The vertical operation.

Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively [3]. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described above is called the 1D Haar-DWT. We perform 2D DWT by applying Haar DWT on the LL part. The figure 8 shows the 2D DWT.


First level


Second level

Figure 8: The 2D DWT.

## VII. Embedding Data

DWT algorithm divides our image into frequency components. The low frequency components are the approximation coefficients. They preserve the original image as it is. On the other hand the other frequency components or the detail coefficients store additional information about the image.[5] These coefficients can be used for embedding data. They can be replaced completely with message information or the LSB of the wavelet coefficients can be replaced by message signal.

## VIII. Conclusion

This work dealt with the techniques for steganography in dwt domain as related to image science. A new and efficient steganographic method for embedding secret messages into images without producing any major changes has been proposed. We use multilayer security by applying cryptography and steganography together. Blowfish algorithm is used for encryption. From the comparative study it has been seen this method is better compared to others in terms of various image similarity parameters. Embedding capacity of this method is much better than other exiting methods in transform domain. Beside this method is a robust method which can avoid various image attacks noise addition, compression.

## References

[1] "A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm" World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 239-246, 2011
[2] Image encryption and decryption using blowfish algorithm World Journal of Science and Technology 2012, 2(3):151-156 ISSN: 2231-2587
[3] A DWT Based Approach for Image Steganography International Journal of Applied Science and Engineering 2006. 4, 3:275-290
[4] Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907-3915A "New Method in image Steganography with Improved Image Quality".
[5] World Applied Sciences Journal 13 (3): 507-516, 2011 ISSN 1818-4952 " Improvement of Embedding Capacity and Quality of DWT-Based Audio Steganography Systems".

