ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure Data Transfer based on Wavelet Transform from Cryptographic and Steganographic Techniques

Mrs.M.Praveena[*1], Mr.V.Sivakumar[2]

[*1]M.C.A, M.Phil, Assistant Professor in Computer Science, Dr S N S Rajalakshmi College of Arts and Science, Coimbatore-6, India

[2] M.Phil Scholar in Computer Science, Dr S N S Rajalakshmi College of Arts and Science, Coimbatore-6, India

sivakanaku99@yahoo.in

Abstract

In today's world, there are a number of cryptographic and steganographic techniques used in order to have secured data transfer between a sender and a receiver. In this paper we present a new hybrid approach that integrates the merits of cryptography and Image steganography based on multi resolution wavelet domain. First, the original message is encrypted using modified blowfish algorithm and the resultant cipher text is embedded into a cover image. After that the Steg image is decomposed into approximation and detailed image using discrete wavelet transform. The resultant reduced image is transmitted to the receiver and the reverse process is done in order to get back the original plain text. Our experimental results show that our system is unique in its design as well as it is suspicion less.

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

Introduction

Steganography and Cryptography are two important and famous techniques which are used to encoding and hiding of data. Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence.

These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication

Cryptography protects information by transforming it into an unreadable format. It is useful to achieve confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called cipher text via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the cipher text into plain text. Cryptography systems can be broadly classified into symmetric-key systems that use a single key (i.e., a password) that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

On the other hand, cryptography protects information by transforming it into an unreadable format. 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. Many types of wavelet, such as Haar wavelet, Daubechies wavelet, the more let 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.

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

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:

ISSN: 2277-9655
Impact Factor: 1.852

a=s-d/2 (2)
b=s+d/2

Conceptually, Hare 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. 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)={1/2,n=k,k+1 0,elsewhere (3)

d(n)={1/2,n=k -1/2,n=k+1 0,elsewhere (4)

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

Literature Review of Cryptography and Steganography

Lot of research has been done in this area in the recent past and various techniques of cryptography and steganography have been suggested.

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.

Cryptography

- Cryptography is the study and practice of protecting information by data encoding and transformation techniques.
- There are two types of cryptographic schemes available on the basis of key namely symmetric key Cryptography and Asymmetric or Public Key Cryptography.

Steganography

- This is a type of security technique which is of the form “security through hiding”.
- In this method the data which is to be sent is concealed in any multimedia file like image, video or an audio file.

Wavelet Based Steganography

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.

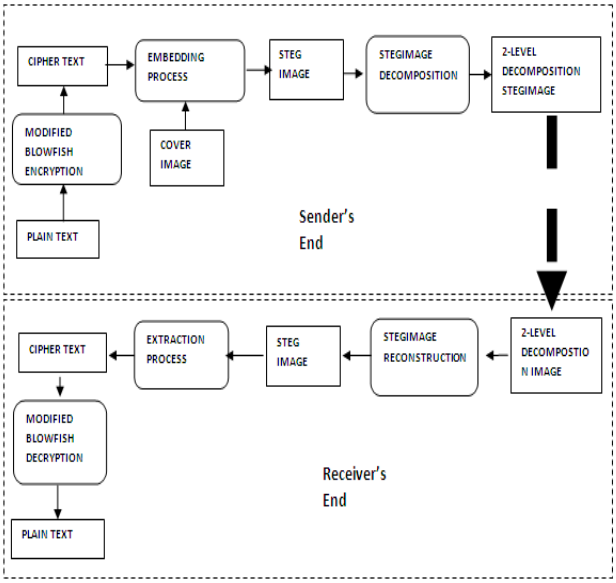
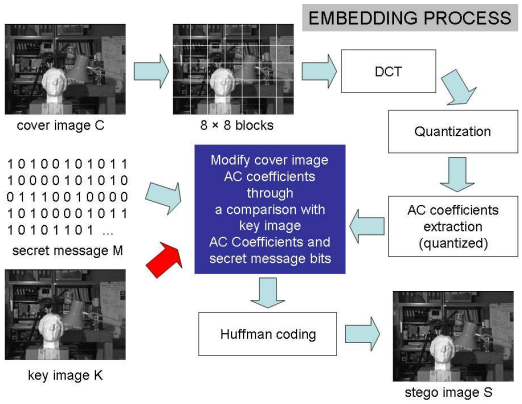


Image Based Steganography and Cryptography

ISC Embedding Process



The embedding process will be a modification of the JPEG encoding scheme. First of all, we subdivide C in a set of 8 x 8 pixel blocks and compute the Discrete Cosine Transform (DCT) on each block obtaining a set of DCT coefficients; then they are quantized.

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

ISSN: 2277-9655
Impact Factor: 1.852

manner. 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 Haar Wavelet(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.

Cryptographic Approach

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

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.

Modified F-function

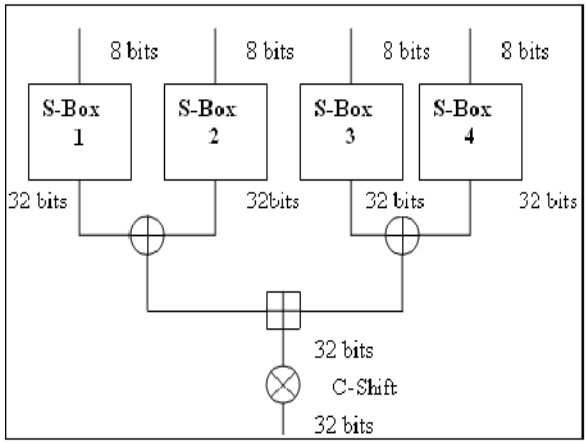
Function F plays an important role in the algorithm, and we decided to modify function F. Original function F is defined as follows.

F(X) = ((S1 + S2 mod 232) XOR S3) + S4 mod 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 XOR S2 mod 232) + (S3 XOR S4 mod 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. The block diagram of the modified F-function is shown below



Steganographic Approach

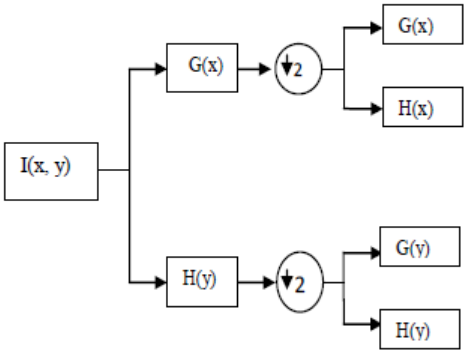
In the case of Steganographic algorithm we chooses LSB Hiding algorithm which hides the very presence of the text inside an image. Least Significant Bit (LSB) insertion is a simple approach to hide information in any multimedia cover file: it overwrites the LSB of a pixel with an M's bit. We can able 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.

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. The first band represents the input stegimage filtered with a Low Pass Filter (LPF) which compresses the image into half of its original dimension. 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

ISSN: 2277-9655
Impact Factor: 1.852

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.



Block diagram for a 4-band wavelet decomposition

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 perpecr reconstruction using 2D DHWT and IDWT respectively.

Simulation

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

Examples of steganography

Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.
Isman hard hit. Blockade issue affects pretext for embargo on byproducts ejecting suets and vegetable oils.

Take second letter of each word to get message:
Pershing sails from NY June 1

Figure 1.is a snapshot of the encryption process. This encrypted text is embedded in an image of size 256x256 which is shown in Figure 2. After this we reduce the image into 128x128 which is shown in Figure 3.

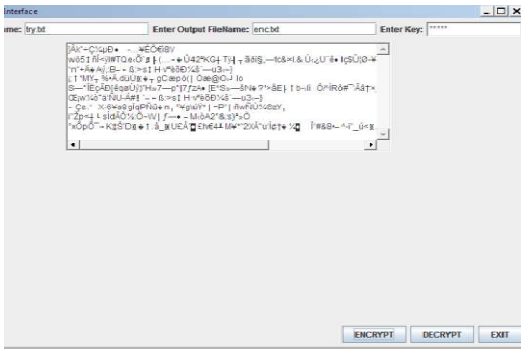


Figure 1: Encryption process

Figure 2: Stego-image with size 256x256

Figure 3: Reduced Stego-image with size 128x128 Figure

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 4.

ISSN: 2277-9655
Impact Factor: 1.852

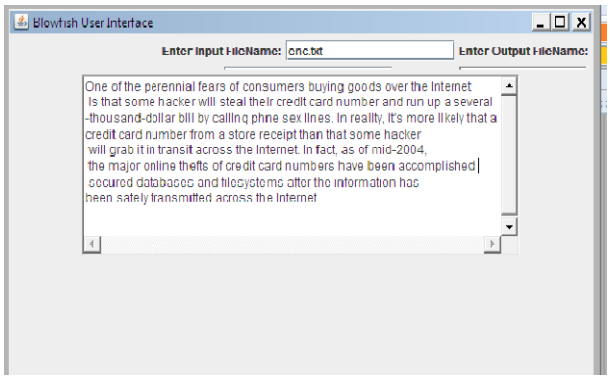


Figure 4: Decryption process

Wavelet Transform 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.

Conclusions

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] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[3] Kerckhoffs, A. (1883). La cryptographie militaire. Journaldes Sciences Militaries, 9th series (IX):5–38

[4] Menezes, A., van Oorschot, P., and Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.

[5] Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83, pages 51–67. Plenum Press.

[6] 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.

[7] 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.