International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Image Steganography using DWT and Data Encryption Standard (DES)

Ketan Shah[1], Swati Kaul[2], Manoj S.Dhande[3]

[1, 2]Student of Shah and Anchor Kutchhi Engineering College, Chembur, Mumbai,India

[3]Professor, Department of CS, Shah and Anchor Kutchhi Engineering College, Chembur, Mumbai, India

Abstract: ***Steganography is an important area of research in recent years involving a number of applications. It is the science of Embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. In this paper we present an image steganography that combines Discrete wavelet transform(DWT),Least significant bit(LSB) and Encryption techniques on raw images to enhance the security of secret message. Intially, DWT algorithm is used to transform image from spatial domain to frequency domain. Then we encrypt our message using DES. Finally we embed secret bits into the cover image to derive stego-image using LSB.***

Keywords: Text hiding, discrete wavelet transforms, Data encryption standard, least significant bit, Haar transforms

1. Introduction

Steganography is derived from the Greek word steganographic which means covert writing. It is the science of embedding information into cover objects such as images that will escape detection and retrieved with minimum distortion at the destination. Steganography and cryptography are closely related. Cryptography provides confidentiality. Steganography on the other hand hides the message and there is no knowledge of the existence of the message. Steganography finds applications in watermarking, finger printing, and the modem multimedia message service; to name a few. The resultant image object obtained after embedding information into the cover image is called as stego object.In our project we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security.[1]

2. Background

Security systems can be divided into two parts:

- Cryptography and
- Information hiding

There are various types of Steganography: Image, Video, Audio and Text. The most popular cover object is image to perform steganography. Images are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye 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 then message is encoded like discrete cosine transforms (DCT), discrete wavelet transforms (DWT) and many others.

3. Architecture

In our system we use cryptography and steganography together. We first enrypt the message to be sent using data encryption standard (DES) algorithm and then hide it in our image. Before hiding, the image is transformed from spatial domain to frequency domain using DWT(Discrete Wavelet Transform) algorithm. DWT divides the image into sub-bands in which we hide out text. Text is hidden using least significant bit algorithm in frequency domain. The Stego-image is obtained which is sent to receiver. Message is extracted and decrypted to get original message. Figure 1 illustrates the block diagram of system.

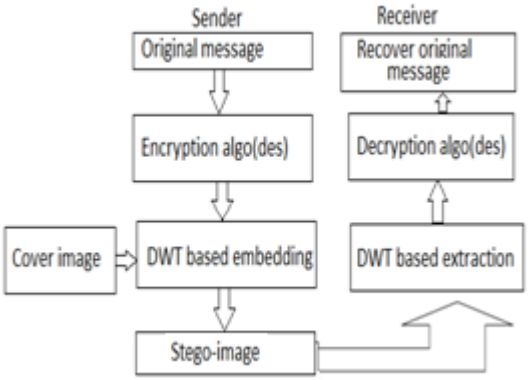


Figure 1: Block diagram of out methodology

Sender side:
1. Write text message.(original message).
2. Encrypt message using Data Encryption Standard 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 Data Encryption Standard algorithm.

4. Get original message.[3]

4. DWT: Discrete Wavelet Transform

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. Wavelets are mathematical functions that divide data into frequency components, which makes them ideal for image compression. In contrast with the JPEG format, they are far better at approximating data with sharp discontinuities.

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis function. Discrete Wavelet Transformation has its own excellent space frequency localization properly. The DWT of an image represents the image as sum of wavelets.DWT uses filter banks to analyze and reconstruct signal. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. 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 .The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient [2] In 1D-DWT average of fine details in small area is recorded.

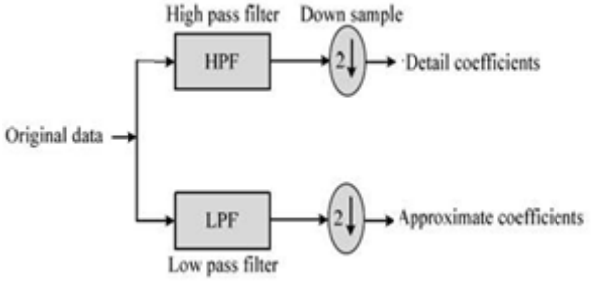


Figure 2:1D-DWT

In 2D DWT First we apply a 1-D filter bank to the rows of the image. Then we apply same transform to the columns of each channel of the result.

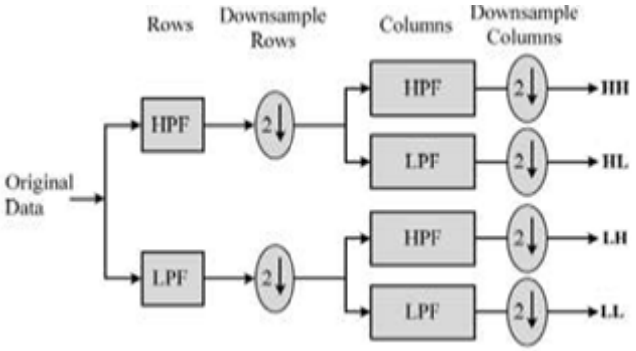


Figure 3:2D-DWT

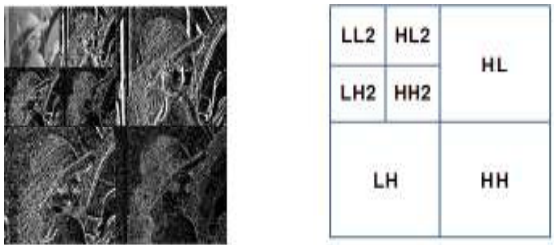


Figure 4: Illustration of 2D DWT

5. Haar DWT

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one. 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 neighbouring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 2. 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).

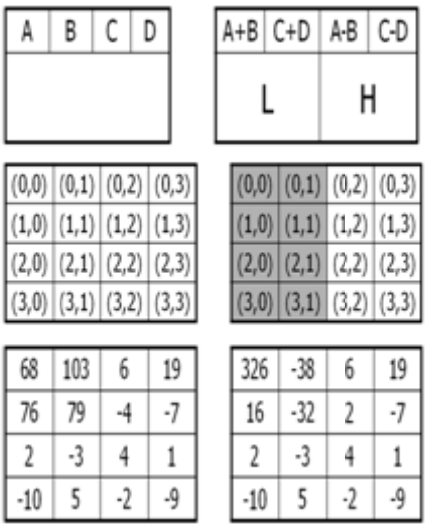
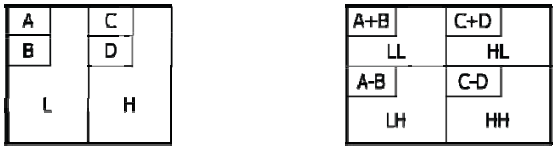


Figure 5: Step 1 of Haar Transform

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 3. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.[3]



(0,0)	(0,1)	(0,2)	(0,3)
(1,0)	(1,1)	(1,2)	(1,3)
(2,0)	(2,1)	(2,2)	(2,3)
(3,0)	(3,1)	(3,2)	(3,3)

(0,0)	(0,1)	(0,2)	(0,3)
(1,0)	(1,1)	(1,2)	(1,3)
(2,0)	(2,1)	(2,2)	(2,3)
(3,0)	(3,1)	(3,2)	(3,3)

20	15	30	20
17	16	31	22
15	18	17	25
21	22	19	18

35	50	5	10
33	53	1	9
33	42	-3	-8
43	37	-1	1

Figure 6: Step 2 of Haar Transform

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. 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.

Least Significant Bit

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data . For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference .In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key.

6. Data Encryption Standard algorithm

Principle of the DES: It is a symmetric encryption system that uses 64-bit blocks, 8 bits (one octet) of which are used for parity checks (to verify the key's integrity). Each of the key's parity bits (1 every 8 bits) is used to check one of the key's octets by odd parity, that is, each of the parity bits is adjusted to have an odd number of '1's in the octet it belongs to. The key therefore has a "useful" length of 56 bits, which means that only 56 bits are actually used in the algorithm.

The algorithm involves carrying out combinations, substitutions and permutations between the text to be encrypted and the key, while making sure the operations can be performed in both directions (for decryption). The combination of substitutions and permutations is called a product cipher.

The key is ciphered on 64 bits and made of 16 blocks of 4 bits, generally denoted k_1 to k_{16}. Given that "only" 56 bits are actually used for encrypting, there can be 2^{56} (or $7.2*10^{16}$) different keys.[5] The main parts of the algorithm are as follows:

- Fractioning of the text into 64-bit (8 octet) blocks;
- Initial permutation of blocks;
- Breakdown of the blocks into two parts: left and right, named *L* and *R*;
- Permutation and substitution steps repeated 16 times (called rounds);
- Re-joining of the left and right parts then inverse initial permutation.

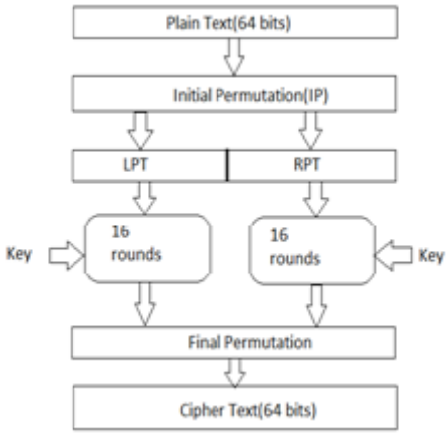


Figure 7: Block diagram of DES

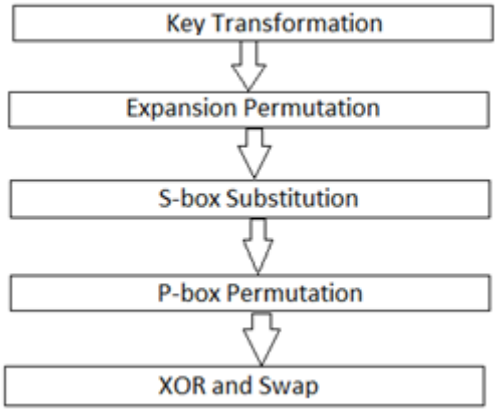


Figure 8: Steps in 16 rounds of DES

7. Steganalysis

Hiding information within electronic media requires alterations of the media properties that may introduce some form of degradation or unusual characteristics. These characteristics may act as signatures that broadcast the existence of the embedded message, thus defeating the purpose of steganography. Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attacker may also embed counter-information over the existing hidden information. Due to space limitations we will look at two methods: detecting messages or their transmission and disabling embedded information. These approaches (attacks) vary depending upon the methods used to embed the information in to the cover media.

Our goal is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illicit hidden information. Some amount of distortion and degradation may occur to carriers of hidden messages even though such distortions cannot be detected easily by the human perceptible system. This distortion may be anomalous to the "normal" carrier that when discovered may point to the existence of hidden information. Steganography tools vary in their approaches for hiding information. Without knowing which tool is used and which, if any, stego-key is used; detecting the hidden information may become quite complex..[6]

8. Result and Analysis

In our proposed method for lossless data hiding, we combined both cryptography and steganography. The major importance is given on the secrecy as well as the privacy of information. Secrecy is maintained using symmetric encryption algorithm DES(data encryption standard) and privacy using Discrete Wavelet Transform.First we convert our message into cipher text using DES and symmetric keys. An image is taken as cover image(24-bit jpeg).Image was transformed into Frequency domain and sub-bands were obtained. Cipher text was then embedded into jpeg image by pixel variation into high coefficient band to obtain stego-image. The stego-image has high PSNR value even after subjecting the image to various attacks. Hence, the observer will not be aware of the existence of the secret message.

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.

9. Conclusion and Future Scope

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. Data Encryption Standard (DES) algorithm is used for encryption. Steganograhy method used is Discrete Wavelet Transform. It transforms image into frequency domain by providing sub-bands. We studied the implementation and the efficient algorithm (Haar) of discrete Wavelet transform. Encrypted message is embedded in the sub band of the cover image. So there is a small visual change in between cover image and stego image.

To reduce the extra data in the stego-images, We have to compress the size of ”Key matrix” as far as possible. Some novel coding schemes are available for this kind of problem. As a result, the file sizes of the original image and that of the corresponding stego-image will not differ too much. Another issue is to efficiently integrate the proposed scheme in the JPEG2000 flow which is based on DWT as well. Nowadays, discrete wavelet transform has become the most useful tool for signal processing and it still has many potentialities.

References

[1] Po-Yueh Chen* and Hung-Ju Lin *“A DWT Based Approach for Image Steganography”* International Journal of Applied Science and Engineering 2006. 4, 3: 275-290 Int. J. Appl. Sci. Eng., 2006. 4, 3 275

[2] Tanmay Bhattacharya* ,Nilanjan Dey** and S. R. Bhadra Chaudhuri*** *“A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum*” International Journal of Modern Engineering Research (IJMER)

[3] Mrs.Archana S. Vaidya,Pooja N. More., Rita K. Fegade., 4Madhuri A.Bhavsar., Pooja V. Raut. “*Image Steganography using DWT and Blowfish Algorithms”* IOSR Journal of Computer Engineering (IOSR-JCE)

[4] Barnali gupta banik, Prof. Samir K. Bandyopadhyay “ *A DWT Method for Image Steganography”* #International Journal of Advanced Research in Computer Science and Software Engineering

[5] Mark Stamps *“Information Security Principles and Practice”* Wiley Publications

[6] Neil F. Johnson and Sushil Jajodia “*Steganalysis: The Investigation of Hidden Information”* Center for Secure Information Systems, George Mason University, MS:4A4, Fairfax, Virginia

Author Profile

Swati Kaul, graduate (B.E) in computer engineering from Shah and Anchor Kutchhi Engineering college, Chembur, Mumbai, India .

Ketan shah, graduate (B.E) in computer engineering from shah and anchor kutchhi engineering college, Chembur, Mumbai, India

Manoj S.Dhande Senior Professor of computer engineering department in shah and anchor kutchhi engineering college, Chembur, Mumbai, India.