SECURE DATA TRANSMISSION USING CRYPTOGRAPHY AND STEGANOGRAPHY

1.SYEDA FARHANA TASNEEM , farhana.tasneemsyeda@yahoo.in ,MTECH FROM SIT(JNTUH)
2.S DURGA BHAVANI, PHD,3.K. SURESH BABU, MTECH,kare_suresh@yahoo.co.in

ABSTRACT:

Information security is the important task while transmitting any data by using the network transmission. We have many theoretical approaches of encryption and respective decryption algorithms. In this project, we present the practical implementation for some of the algorithms like DES, triple DES and AES etc. But, transmission of encrypted data directly through the network is not much secure. So, we are going to insert that data as watermark in an image by using some watermarking algorithms.

In this Project, Cryptography and Steganography methods are used to increase the security of the data while transmitting through networks. In the discrete wavelet transform, an image signal can be analyzed by passing it through an analysis filter bank. Another technology, the digital watermarking is the process of embedding information into a digital (image) signal which may be used to verify its authenticity or the identity of its owners. In this project, the watermark to be embedded is 'text'. Before embedding the plain text into the image, the plain text is encrypted by using Advanced Encryption Standard (AES) algorithm. The plain text can be any sentence in English, and the key can be anything in English with a length of 8-characters.The encrypted text is embedded into image using steganographic technique using Discrete Wavelet Transform (DWT) method and the resultant image is transmitted to the receiver. At the receiver's end, from the image the encrypted text is extracted by using DWT method and the result is decrypted using AES.

Keywords — Image Steganography, AES Cryptography, Discrete Wavelet Transform, LSB Steganography.

INTRODUTION

A huge amount of confidential data is being lost every year during transmission by the intruders. Ciphering techniques are widely used to encrypt and decrypt data. But sometimes data encryption does not seem enough and hiding of the data itself is needed more. The technique used for this idea is called Steganography. Steganography is the process of concealing information in a carrier such as text, image, voice, video, or protocol. Digital images are one of the common and most popular ones due to their frequency on the Internet and high capacity of data transmission without degrading effect on images quality. It is a high security technique for long data transmission. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its color. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The best known Steganographic method that works in the spatial domain is the LSB, which replaces the least significant bits of pixels selected to hide the information. This method has several implementation versions that improve the algorithm in certain aspects.

The image in which the secret message is embedded is called cover image and the image containing the secret message is Stego image. In spatial domain scheme, the secret messages are embedded directly. The most common and simplest

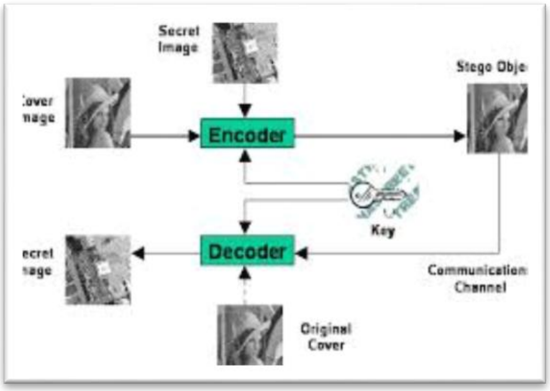
Steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding. A basic classification of Steganographic algorithms operating in the spatial domain as the method for selecting the pixels distinguishes three main types: non-filtering algorithms, randomized algorithms and filtering algorithms.

Sometime Steganography will not cover the total security of secret massage. So an additional security need to the secret massage. For this purpose AES (Advanced Encryption Standard) encryption system is used in our proposed Steganographic system. The Advanced Encryption Standard (AES) is a symmetric key cryptographic algorithm which was published in 1977. AES allows for three different key lengths: 128, 192, or 256 bits and 128 bits block size. It supersedes the Data Encryption Standard (DES) which is also a symmetric -key cryptographic algorithm. The overall structure of AES for encryption and decryption using 128 bits key. In our proposed technique we improve the default LSB technique. We use MSB bit for filtering the pixel, whether it is eligible for hiding message bit or not. We introduced new concept status bit. We do not just embed the message bit in the LSB bit but we embed the status message. So if anyone tries to find secret message by collecting LSB bit from image he/she failed to get the original message. This will make the secret message more secure. For more security we use AES encryption technique.

For maintaining higher security and authentication of this embedded data transform domain is used. In transform domain digital media converted into frequency domain by using DWT (discrete wavelet transform). Transform domain has good robustness in comparison to spatial domain. Transform domain has high computational complexity but good robustness against attacks. Wavelet based steganograhy provides a good picture quality with high resolution. Steganography in transform domain has ability to tolerate signal processing operations and noises. In this less significant coefficients of cover image are used for embedding significant coefficients of secret data. In this DCT (discrete cosine transform) techniques are frequently used. So here we proposed DWT (discrete wavelet transform) to decompose an image.

PREVIOUS WORK

There are lots of techniques available that implement Steganography on a variety of different electronic mediums. The secret key encrypts the hidden information and then it is stored into different position of LSB of image. This provides very good security. A method in which the information is hidden in all RGB planes based on HVS (Human Visual System). This method used to hide the secret message which increases the capacity and also Stego size. S. Roy and R. Parekh proposed an improved steganography approach for hiding text messages within lossless RGB images which will suffer from withstanding the signal processing operations. Minimum deviation of fidelity based data embedding technique has been proposed by J. K. Mandal and M. Sengupta where two bits per byte have been replaced by choosing the position randomly between LSB and up to fourth bit towards MSB. A. Sejul, et al. proposed an algorithm in which binary images are considered to be secret images which are embedded inside the cover image by taking the HSV (Hue, Saturation, Value) values of the cover image into consideration. The secret image is inserted into the cover image by cropping Signal & Image Processing. In this method the capacity is too low. In this method Less security will be provided by using only cryptography As well as Message hiding capacity is low and Quality of the image would be degraded.



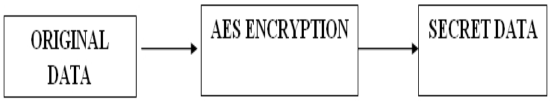
PROPOSED TECHNIQUE

A digital image consists of different pixels. In this method we used color image. As we know, a colored pixel can be represented as a mixture of red, green and blue color with appropriate proportions. In binary notation, a color level is represented by a stream of 8 bits. Therefore in total, 24 bits are required to denote a pixel. Thus an image is an array of many bytes each representing a single color information lying in a pixel. In the proposed method, a group of three sequential bytes from such an array is used to embed a bit of the entire message.

The proposed technique has two main parts:
i. Changing the secret message (plain text) to cipher text by AES Cryptography
ii. Hiding the cipher into image by a proposed Steganographic technique

128 bits AES Cryptographic algorithm takes a password and encrypts the plain text to cipher text. This cipher text will be embedded into a cover image using our Steganographic technique. In the Steganographic technique, a filtering algorithm has been used to hide the information. The MSB bit specify the area where to embed the secret message. Our algorithm has the concept of randomly select an image.

Encryption:

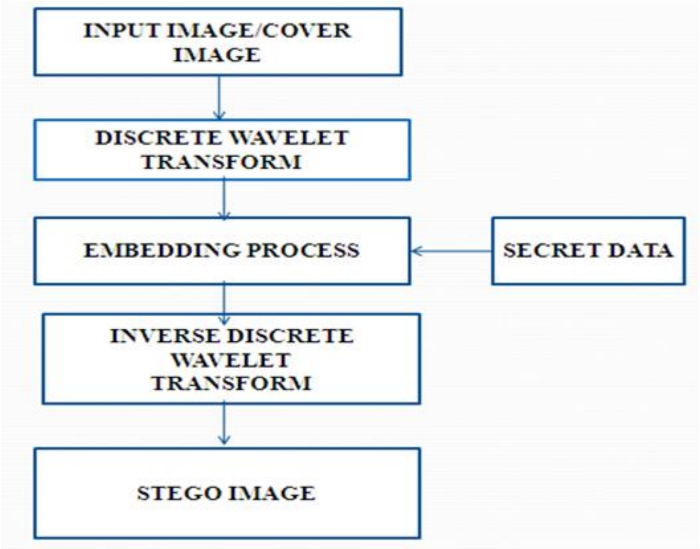


We present our algorithm for gray scale images of dimension 256x256 or 512x512. The human eye has different visual sensitivity for different frequency. Low frequency component are basically used for embedding data. We are using DWT (Discrete Wavelet Transform) for hiding stego data in cover image. For higher security we use AES encryption. To embed Cipher text into original image we used embedding process.

Steps of embedding process are as follows:

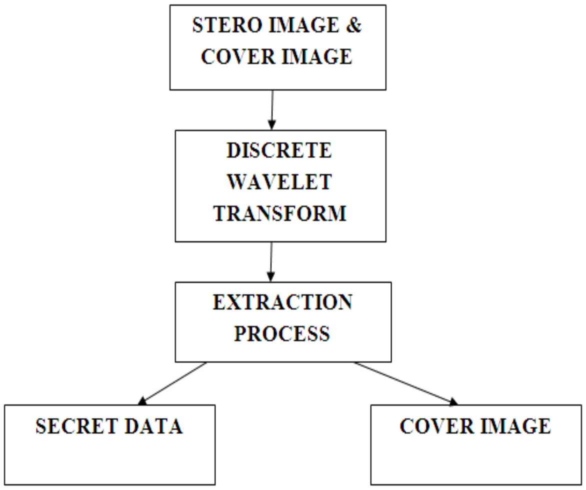
Step1: First take the secret key and convert this into cipher text using the AES Encryption.
Step2: And the cover image (C) of size NxN and then apply Discrete Wavelet Transform using the lifting scheme method.
Step3: After applying the wavelet transform we get 4 sub bands. They are nothing but one sub band is nothing but Approximated coefficients (LL), and three Detailed Coefficients (LH, HL, HH). These are horizontal coefficients, Vertical coefficients and are Diagonal coefficients
Step4: Horizontal approximation coefficients are used for the embedding data.
And embedded the cipher text into the sub band using lsb algorithm process
Step5: And then Apply 2D IDWT (inverse discrete wavelet transform) to get stego image

Embedding Process:



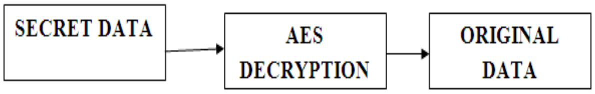
After completing this process we get the final stego image.
Steps of Extracting process are as follows:
Step 1: Apply 2D DWT on the stego image
Step 2: Apply Inverse LSB algorithm on the separated wavelet coefficients and get the scrambled secret cipher text.

Extracting Process:



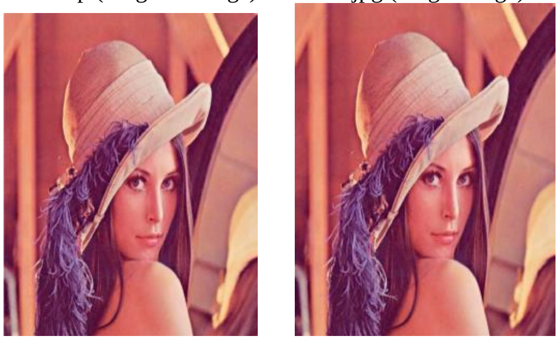
After extracting the cipher text apply the AES Decryption on the Cipher text. And we get perfect original secret data.

Decryption:



SIMULATION RESULTS

We performed simulation on MATLAB2010a, version 7.10, under the Windows 7 professional with dual Core CPU and 4 GB RAM. The cover images of size 512x512 from USC SIPI image database (freely available at http://sipi.usc.edu/database) are used. Initially we measured the perceptual fidelity of stego images using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) then these stego images were subjected to common image processing attacks to check the robustness of the scheme and the results are shown below. From the simulation results, it is clear that the proposed scheme is ideal for Secret data communication as it meets key requirements including security, better perceptual Fidelity and robustness.


Lena.bmp (Original Image) Lena.jpg (Stego Image)

Simulation results on Lena.

CONCLUSION

This paper proposes a novel technique for secret data communication that can thwart specialized reverse engineering techniques by resolving the data interception problem. During data transmission if data is intercepted it can be successfully extracted by attacking the cryptographic algorithm. We proposed an image steganography scheme based on LSB algorithm that hides the encrypted message inside cover images imperceptibly. Breaching the communication system would involve intercepting, identifying, extracting, reverse engineering and decoding. Thus combining cryptography with steganography offers an ideal system for secret data transmission with higher consistency with respect to stand-alone cryptographic techniques. Thus this scheme provides two tier securities, first using cryptographic key and second using stego key where the secret message is encrypted before embedding and decrypted after decoding.

The STEGO -image is looking perfecty intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image or secret data is perceptually similar to the original secret image or data.

REFERENCES

[1] http://en.wikipedia.org/wiki/Time-lapse.
[2] Handbook of image and video processing by Alan Conrad Bovik, Elsevier

Inc., ISBN 0-12-119192-1.

[3] Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.

[4] R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.

[5] Adnan M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. On Image Processing, vol. 13, no.8, Aug, 2004.

[6] Avcibas, N. Memon, and B. Sankur Steganalysis using image quality metrics, IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003.

[7] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani,Dual layer data hiding using cryptography and steganography in IJSET volume 1,issue 4,ISSN : 2277-1581