Data Embedding using Image Steganography

Ashish S[1], Manjunath P[2], K S Prateek[3], Ashith Kiran Parlakoti[4], Dr. Bhuvana Suganthi D[5]

[1,2,3,4] UG-BE, Dept. of Electronics and Communication Engineering, BNMIT
[5]Associate Professor, Dept. of Electronics and Communication Engineering, BNMIT, Karnataka, India

---

Abstract - *This paper provides a secured communication using both steganography and cryptographic techniques, which gives the maximum security in the communication link. AES algorithm is used to encrypt and decrypt the text. The text obtained from the above process is embedded and extracted using DWT algorithm. Stego-image is emailed to the intended receiver. MATLAB is used for the above-mentioned process. The model contains sender GUI and receiver GUI which performs the simulation. Integrating steganography and cryptographic techniques higher levels of security can be achieved.*

***Key Words*: Advanced Encryption Standard (AES), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Least Significant Bit (LSB), RSA (Rivet-Shamir-Adleman), Graphical User Interface (GUI).**

1. INTRODUCTION

Security is the major reason, where the communication engineers are more concerned about. Thus, the engineers develop more and more complex algorithms to secure the channel from the attackers, which are known as "Cryptographic" techniques. Techniques like RSA (Rivet-Shamir-Adleman), AES (Advanced Encryption Standard), DES (Data Encryption Standard), Diffie-Helman Key Exchange and many more are introduced. But these techniques became usual to public thus, the techniques are vulnerable to the hackers or the middle man. [1]

Earlier, people used steganography to send the secret message. Techniques like pin punching, using invisible ink, word patterns and many more are used. But the secret message is easily decoded. So, using only steganography does not meet requirements of security. Thus, engineers used both steganography and cryptographic techniques to achieve the maximum security.

AES algorithm is used on the given data thus we obtain encrypted text in the sender GUI and decrypted text from the receiver GUI, generally the text obtained is known as "AES Encrypted Text", where the algorithm has different number of rounds depending on the key size. The text obtained is embedded to an image in sender GUI and extracted from the image in receiver GUI. The process of embedding and extracting process is done using DWT Algorithm. The embedded image is known as "Stego-Image". Here, the stego-image is emailed using SMTP protocol using google as the server.

2. COMPARATIVE ANALYSIS

Various algorithms for cryptography (AES and RSA) and steganography (DWT, DCT and LSB) are compared. AES is a symmetric key encryption system, whereas RSA is an asymmetric key encryption system. Table 1, shows the results obtained. [3]

AES is compared with RSA, where the former is more advantageous. Since throughput and confidentiality of AES is higher than RSA, so AES algorithm for the encryption stage is implemented.

Table -1: Cryptographic Analysis

SL. NO.	Features	AES	RSA
1	**Type**	Symmetric	Asymmetric
2	**Throughput**	High	Low
3	**Confidentiality**	High	Low

Different algorithms for the steganography stage are DWT, DCT and LSB are compared in Table 2. [2][4]

Table -2: Steganographic Analysis

Method	DWT	DCT	LSB
Invisibility	High	High	Low
Robustness	High	Medium	Low
PSNR	Low	High	Medium
MSE	High	Low	Medium

DWT has more features favoring for the results that we intend to get. Though DWT has high MSE, we have other features that gains high marks compared to other algorithms hence the trade-off.

The following sections gives the AES and DWT implementation and the results obtained.

3. AES (ADVANCED ENCRYPTION STANDARD)

AES is the symmetric cryptosystem in which single key is used for both encryption and decryption. Figure 1, shows the first level of security using AES encryption technique. In AES there are different stages which is iterated number of times based on the length of the key used.

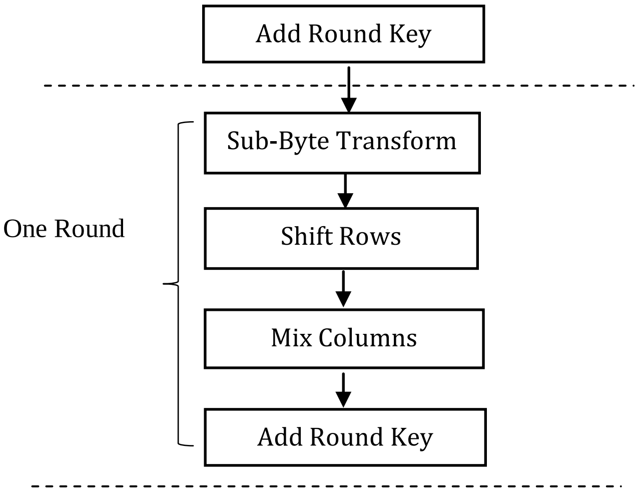

Figure -1: Encryption Process of AES algorithm

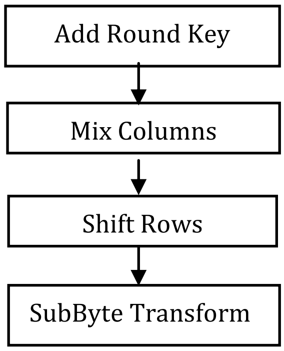

Figure -2: Decryption Process of AES algorithm

The process of AES is shown in Algorithm 1.

Algorithm-1: Advanced Encryption Algorithm

Step 1: Obtain the key from user and encrypt the same.
Step 2: Convert the key and message into the matrix form.

Step 3: Add the key to the message matrix as initial stage.
Step 4: Circular shift elements of the above obtained matrix to right once for each row except for first row.
Step 5: Add the random matrix to the above matrix which gives mixed column Matrix.
Step 6: Add the key again to the above matrix.

For decryption, in figure 2 the same steps are followed where the message matrix is replaced with cipher text matrix. All stages in each round is performed using the key sent by the sender which will be in encrypted form. Three stages add round key, shift rows and mixed columns are used. Substitute byte transform is not included.

The pivotal feature of AES technique is the flexibility to use the desired key lengths which indeed increases the complexity. AES allows the sender to use the large size keys. The number of rounds is also decided by the length of the key used. Table 3 shows the number of rounds and key size.

Table -3: Number of Rounds and Key Size

Key Size	Number of Rounds
10	128
12	192
14	256

4. DWT (DISCRETE WAVELET TRANSFORM)

Steganography techniques can be implemented in mainly two categories, namely spatial and transform domain. Spatial domain makes use pixel values of cover image to embed the secret data. The transform domain makes use of more complex frequency domain of image to store data. One such multi resolution analysis technique is DWT. DWT having its own localization property of space frequency and highly efficient method for decomposition of signals in sub band. Wavelet transform disseminates the base image to wavelet coefficients, which are stored efficiently than pixel blocks. Since DWT is a 1-D filter to be applied on a 2-D image, once along the rows of the image and then along columns or vice versa is referred as 2-D DWT. DWT process firstly transforms time domain to frequency domain image sub-bands. Transform domain splits the image signal into high and low frequency components by passing it through filters, only high frequency part (edge component) is used for data embedding as human eye senses less change in edges. Current common lossy image compression jpeg 2000 is built based on wavelet transform. [5]

2-D wavelet transform is applied in horizontal direction, then followed by vertical direction for single level decomposition, which leads to LL1, LH1, HL1 and HH1 sub-bands. 2-D wavelet transform functions by decomposition on array of the rows, dividing the array into two halves of vertical with average coefficients in the first half and containing detail coefficients in second half. Same process repeats itself for array of columns leading to generation of 4 sub-bands within pre-defined array with the presence of filters as shown in Figure-3. HH sub-band is used for successive level decomposition, and also make use of HL if HH is saturated for embedding of data. HH sub-band further decomposes to four sub-bands on application of DWT to obtain second level decomposition. Data embedding in HH has its own advantage of non-detectability. Signal decomposition to various frequency bands make it possible to process independently. [6]

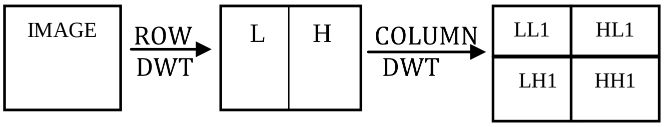

Figure -3: Sub-Band Generation

Inbuilt MATLAB function YCbCr is a variety of color space that can be used as a part of color image and digital photography, Y stands out for luma or luminescence (brightness level) and C for chroma (Intensity of color). Instead of representing an image in RGB, we can make use of only two colors blue and red and one brightness level in between black and white to represent the same RGB image which provides more space to embed secret data. Haar wavelet is a discontinuous step function, used for ortho normal system in the unit interval. Consisting of two operation, one is the horizontal and the other in the vertical direction. Scanning of pixels from left to right row wise, and performs addition and subtraction of pixel values. This technique is mainly used for pairing up the input values with storing difference and passing the sum repeatedly to obtain one final sum. Haar wavelet is one of the simplest types of wavelet and simple compression technique computing average and difference terms and reconstructing matrix similar to input image matrix. [7]

The process of embedding the text into the image is shown in Algorithm 2.

Algorithm-2: Embedding Process

```
Step 1: Reading the cover image.
Step 2: Reading the encrypted text message.
Step 3: Convert the given image to YCbCr color space.
Step 5: Construct the Haar wavelet (MATLAB inbuilt
        function: Liftwave).
Step 6: Apply the DWT to image on Cb channel (MATLAB
        inbuilt function: LWT2).
Step 7: Embedding data in HH sub-band.
Step 8: If HH sub-band is saturated, use HL.
Step 9: Restore matrix dimensions.
Step 10: Apply IDWT to obtain Stego-image.
```

The process of extracting the text into the image is shown in Algorithm 3.

Algorithm 3: Extracting Process

```
Step 1: Read the stego-image.
Step 2: Extract the blue difference chroma Cb.
Step 3: Construct the Haar wavelet.
Step 4: Apply the DWT to the Stego-Image, on Cb channel.
Step 5: Read the data from HH/HL regions.
Step 6: Convert the data from binary to ASCII.
```

5. RESULTS OBTAINED

MATLAB r2016a or higher version is used. MATLAB requires a minimum RAM of 3GB and Windows 7 & above Operating System.

The steps for transmitting the message using sender GUI is given below:
Step 1: Enter the message.
Step 2: Binary conversion of message.
Step 3: Enter the secret key.
Step 4: Apply AES encryption algorithm.
Step 5: Browse the image.
Step 6: Embedding the data.
Step 7: Enter the receiver email to send the image.
Step 8: Calculate Hiding Capacity, Peak signal To Noise Ratio and Mean Square Error.

Hiding capacity is calculated using inbuilt function capacity ( ). Mean square error is calculated using the formula

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \qquad (1)$$

where I is the input image and K is the stego image. Peak signal to noise ratio is calculated using

$$\text{PSNR} = 10\log_{10}\frac{255^2}{MSE} \qquad (2)$$

5.1. GUI FOR SENDER:

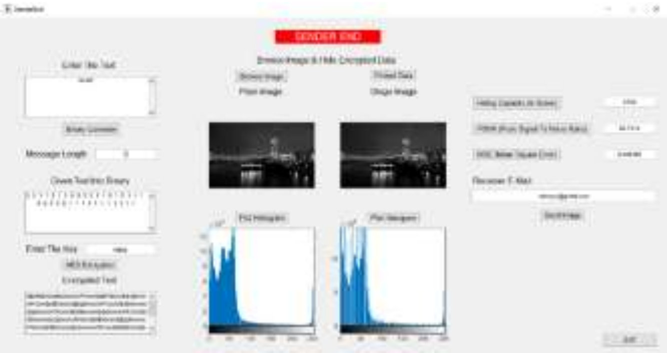

Figure-4: Sender End GUI

The steps for receiving the message using receiver GUI is given below:

Step 1: Browse stego-image.
Step 2: Extract the data.
Step 3: Enter the secret key.
Step 4: Decrypt the data.
Step 5: Binary conversion.

5.2. GUI FOR RECEIVER:

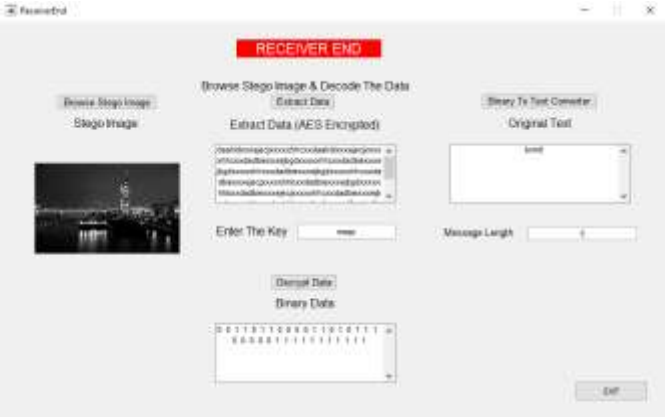

Figure-5: Receiver End GUI

ACKNOWLEDGEMENT

We would like to thank our guide, Dr. Bhuvana Suganthi for her guidance and valuable feedback with regards to processing forward with this project thus far.

REFERENCES

[1] “A Survey on various types of Steganography and Analysis of Hiding Techniques” Navneet Kaur, Sunny Behal. (May- 2014).
[2] “Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application Using Steganography” Saravanan Chandran, Ph.D., MIEEE. (Januar-2015).
[3] “A Comparative Analysis of AES and RSA Algorithms” Shaili Singhal, Dr. Niraj Singhal. (May-2016).
[4] “A Survey on different techniques of steganography” Harpreet Kaur, Jyoti Rani. (2016).
[5] “Image Steganography Using Discrete Wavelet Transform– A Review” Tushara M, K. A. Navas. (Februa ry-2016).
[6] “A Novel DWT based Image Securing Method using Steganography” (2016) Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michael.
[7] “A DWT Based Approach for Image Steganography” Po-Yueh Chen, Hung-Ju Lin.