Embedding secret data into images using Edge detection and Modified LSB

Gnana Lakshmi.V¹
Assistant Professor  
Dept of Electronics and Communication  
Mepco Schlenk Engineering College, Sivakasi, India.

Sundhara Dhaarani.C²
UG Scholar  
Dept of Electronics and Communication  
Mepco Schlenk Engineering College, Sivakasi, India.

Uma.L³  
UG Scholar  
Dept of Electronics and Communication  
Mepco Schlenk Engineering College, Sivakasi, India.

Abstract—The Internet is becoming a popular communication channel. However, the data transmitted over the channel have some issues. The primary goals of Network security are Integrity, Confidentiality and Availability. The intruder may attempt to violate these goals. Hence a secure communication method is required to transmit the data. Cryptography and Steganography are the most commonly used techniques for implementing security mechanisms. In this paper, Advanced Encryption Standard (AES) is used. Here 128 bit AES is used. Canny edge detection is used to detect the edges where the data is to be hidden. Modified LSB based steganography is implemented. This modified LSB algorithm is more efficient than standard LSB technique. The quality of the obtained stego image is analyzed using some of the metrics like PSNR, MSE and ER. A high value of PSNR indicates better quality of the image. Since a high value of PSNR is obtained, it is an efficient technique to hide the secret data into the images.

Keywords—AES cryptography, Canny edge detection, Modified LSB steganography.

I. INTRODUCTION

People can transmit large amount of data via Internet. However the security of the network is insufficient and the transmitted data may be intercepted by the intruders. In order to provide security to the data, different techniques can be used. Cryptography is the science and art of transforming the message to make them secure. Steganography is also one such method to secure the data. It is the art and science of hiding the secret data into the cover media such as image, audio and video. Cryptography means “secret writing”, steganography refers to “covered writing”. In cryptography the intruder may know the presence of data in the channel, whereas in steganography the secret data is hidden inside the cover media and the data is not exposed. When both these methods are combined, the level of security can be enhanced.

Among various cryptography algorithms, AES is standardized high security algorithm. AES is the extension of Data Encryption Standard (DES). DES is an insecure algorithm because of the small key size which is 56-bit. Sombir Singh et al, 2013[1], proposed a technique to overcome the weakness of DES which involves enhancing the security of DES using transposition technique. The plaintext is converted to cipher text using transposition technique which is given as input to DES. This improves the security of DES but it is computationally complex.

AES is a block cipher which works on fixed length group of bits called blocks [2]. AES uses three different key sizes 128, 192 and 256 [16]. Depending upon the key size the number of rounds may vary. The number of rounds is represented as N, which takes the values 10, 12 and 14. In this paper 128 bit AES cryptography is used. The input to AES is 128 bits plaintext and produces the cipher text of same size. Since the key size is 128, the number of rounds used is 10.

Image steganography is the art of concealing secret data into images and is classified into spatial domain, transformation domain, spread spectrum domain and model based steganography. Here spatial domain technique is used where the secret data are embedded in the LSBs [6]. The key terms in steganography are Cover image, payload and Stego image. Cover image refers to the image where the secret data are embedded. The embedded data is known as payload. The image containing the embedded data is called stego image.

Combining both cryptography and steganography will increase the level of security. Rashedul Islam et al, 2014[3], proposed a technique to combine both cryptography and steganography. The secret data is encrypted using AES and an improved method of LSB is used. It hides large data in a bitmap image using filtering based algorithm which uses MSB bits for filtering. It uses the concept of status checking for the insertion and retrieval of message.

The secret data can be embedded anywhere in the image. The smooth/flat region in the image will be contaminated after embedding. But the edges can tolerate sharper changes than smooth area. Hence a potential edge detection method is required. Edge detection is the process of identifying the sharp discontinuities in an image [6]. The different edge detectors are Previtt, Sobel, Robert Cross, Differential and Canny. Wei Qi Luo et al, 2010[4], proposed an edge adaptive method. Here the embedding regions are selected based on the size of the secret data and the difference

ISSN : 2348 – 8549  www.internationaljournalssrg.org  Page 114
in pixels. The edges can tolerate larger changes. For low embedding rates, sharp edge regions are chosen. As the embedding rate increases, more edge regions can be released for data hiding.

Among the different edge detectors canny is found to be widely used. Canny has some advantages over other operators such as better detection, improved signal to noise ratio and insensitive to noise [7]. This paper Saiful Islam et al, 2014 [5], proposed a method for hiding the data at the edges using Canny edge detector and LSB technique. The amount of distortion occurred due to embedding is reduced.

LSB replacement is the well-known steganographic method [2], [11]. The LSBs of the cover image are replaced by the secret bits. However, when steganalysis is performed the existence of the secret data is detected [13]. In order to overcome this issue and to improve the imperceptibility of image, modified LSB technique is implemented. H.Dadgostar et al, 2016 [6], proposed an interval-valued intuitionistic fuzzy edge detection to distinguish between the edge and non-edge pixels. The data is embedded at the edges and non-edges using modified LSB technique. By combining edge detection and modified LSB substitution, the embedding capacity and imperceptibility can be increased.

II. PROPOSED SCHEME

In the proposed scheme, the secret data is encrypted using Advanced Encryption Standard (AES). The encrypted data is then embedded at the edges of the image. These edges are detected by canny edge detection. Modified LSB substitution method is used to embed the data. The encrypted data is extracted from the stego image and is given as input to AES to decrypt the original data.

A. Encryption and Decryption

If the data is embedded as such in any cover media, the intruder can obtain the original message while performing steganalysis. To improve the imperceptibility, encryption of the secret data is needed and by this the intruder can obtain the encrypted data which is meaningless. They should know the right key to decrypt.

The proposed scheme uses Advanced Encryption Standard (AES). AES is a block cipher [2], [16]. It is a symmetric key cryptographic algorithm which was published during 1977. AES uses three different key sizes: 128, 192 and 256.The overall structure of AES-128 is shown in Fig. 3.

AES- 128 has 10 rounds. Each round has four processes namely sub byte, shift rows, mix columns and add key [15]. The last round has only three steps excluding mix columns. Round keys required for the operation are generated using Key expansion. AES operates on 4x4matrix called state. The input and the output from each round is a state. In the first process of each round, each byte is substituted by s-box value. It involves 16 independent byte to byte transformations. The second process involves shifting of rows. During encryption left shift is performed and during decryption right shift is performed. In the next process, the column is multiplied by a constant 4x4 matrix. The last round involves adding round keys. The decryption is the inverse process of encryption. The structure of each round is shown in Fig. 4.
B. Edge detection

Edges are preferred to smooth areas for embedding because edges can tolerate sharp changes. Canny edge detector is used to distinguish between the edges and non-edges. It was first developed by John Canny [9], [7]. It involves 5 steps.

- Apply Gaussian filter to smoothen the image.
- Find the intensity gradient of the image.
- Apply Non maximum suppression.
- Apply double threshold.
- Track the edges of the image.

In order to extract the data accurately, and with no distortion the edge pixels before and after embedding should be the same. A common issue after embedding is that the edges change to non-edges and vice versa [6]. Thus it becomes impossible to retrieve message correctly from the stego image. Hence it requires edge preserving mechanism.

C. Edge preserving mechanism

The Edge preserving mechanism tries to preserve the edges unchanged after embedding. It consists of two stages. In the first stage, some $p$ LSBS of the cover image is set to zero before detecting the edges. The resultant image is called the modified image which is given as the input to edge detector. The second stage is applied to check whether any edge pixel is changed during embedding.

D. Modified LSB

Pixels are embedded by the $k$-bit LSB substitution in which $k$ LSBS of each pixel is replaced by the message. Embedding a message in the LSBS is given by

$$y' = y \oplus_k m$$

where $y$ is a pixel value in the cover image and $m$ is the secret message and $y'$ is the stego pixel after embedding and $\oplus_k$ denotes embedding $k$ bits in the $k$ LSBS.

To improve the quality of the stego image, modified LSB substitution method is applied. By applying the $k$-bit modified LSB substitution, pixel values may be modified at distance $2^k$ by increasing or decreasing the MSB part. Thus, a pixel with the value of $y$ is changed to $y+2^k$ or $y-2^k$. A flowchart for modified LSB is shown in Fig. 5.

Consider the cover image pixel $y=10001011(139)$. After converting the $p$ LSBS to zero the resultant pixel value is $s=10000000(p=4)$. This pixel is called modified pixel. Assuming this pixel as the edge pixel, it’s $k$ LSBS are substituted by the message bits. Consider $m=01110101(117)$
and $k=4$, $y'$ is calculated from (1) as $y'=10000101(133)$. Since $y-y'=2^4$, $y''=y'+2^4 (y''=10010101(149))$. Apply the second stage of edge preserving mechanism to check whether the 4 MSBs of $y$ have changed during embedding. It is evident that 4 MSBs of $y$ and $y''$ are different. Hence $y'$ is chosen as stego pixel.

E. Extracting process

Once the stego image is obtained, $p$ LSBs of the stego image is set to zero. This resultant image is called $s$ (modified image). Then the canny edge detection is applied on the modified image $s$. Once the edge pixels are detected, by the canny edge detection the $k$ bits are extracted from each edge pixels. This gives the data that is embedded at the edges. The extracted data is meaningless. Hence this is given as input to the AES decryption which will produce the secret data.

III. IMPLEMENTATION RESULTS

The entire process is implemented in MATLAB. The cover image used here is lena which is shown in Fig. 6a. Fig. 6b shows the edges of the cover image.

![Fig. 6a.Cover image](image1)

![Fig. 6b.Edge pixels of Cover image](image2)

The secret data to be embedded is taken as “hi hello World.” and the cipher key is “I am from India.”. After AES encryption, the encrypted data is shown below.

< 6N 1 -> \( \text{ATEV} \)

The encrypted data are embedded in the cover image using Modified LSB. The stego image obtained is shown in Fig. 6c. Fig. 6d shows the edge pixels of the stego image.

![Fig. 6c.Stego image](image3)

![Fig. 6d.Edge pixels of Stego image](image4)

The secret data that is embedded at the edges of the cover image is extracted from the stego image. The extracted data is decrypted using AES decryption.

Performance analysis is done on the obtained stego image. The image quality metrics like Peak signal to noise ratio (PSNR), mean square error (MSE) and Embedding ratio(ER) are calculated. A good quality image requires high PSNR and low MSE.

$$\text{PSNR} = 10 \log_{10} \left( \frac{255}{\text{MSE}} \right)$$

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (x(i,j) - x'(i,j))^2$$

Where $x(i,j)$ and $x'(i,j)$ are the pixel values of the cover and the stego image, respectively. The result of the performance analysis is shown in Table 1.

<table>
<thead>
<tr>
<th>Size of the image (pixels)</th>
<th>Stego Image</th>
<th>Performance measures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PSNR(dB)</td>
</tr>
<tr>
<td>200x200</td>
<td></td>
<td>63.9561</td>
</tr>
<tr>
<td>256x256</td>
<td></td>
<td>64.4148</td>
</tr>
<tr>
<td>225x225</td>
<td></td>
<td>62.6678</td>
</tr>
<tr>
<td>512x512</td>
<td></td>
<td>70.6727</td>
</tr>
</tbody>
</table>

Table.1. Performance analysis
IV. CONCLUSION

This paper provides a higher level of security that eases the transmission of secret data. AES encryption provides a better encrypted result. Embedding the encrypted data at the edges of the cover image using modified LSB provides better imperceptibility. Double AES -128 bit can be used to increase the length of the secret data.

V. REFERENCES


