Steganography

Jaisairun P Srinivasan

Tarun Anand

INTRODUCTION

Communication plays a vital role in today's world. Communication includes transmitting messages from one destination to another, and at times these messages are needed to be kept secret. As the time progresses the means of communication have increased and so has the need to secure these means of communication. One of the techniques used to secure communication is Cryptography. The cryptography involves encrypting and decrypting through various methods and thus securing the channel of communication. The cipher text obtained by encrypting the message is easily noticed when passed through a channel, thus informing others that the channel is monitored. Thus a better means of communication for plain text while maintain message secrecy were researched and that lead to Steganography. [1]

[2] Steganography is the art of hiding the fact that communication is taking place by hiding information in other information .In steganography the message is hidden inside a carrier file such that the change is not noticeable to a naked eye. Stenography techniques are classified based on the cover modifications applied during the embedding process is as follows:

A. Least significant bit (LSB) method

This is a very simple and common approach. The least significant bit (LSB) of the pixels in the image is replaced with the bits of the message. The resulting stego-image will look same as. [3-4]

B. Transform domain techniques

In this approach the secret message is embedded in the frequency domain of the signal, Transform domain methods which hide the message in area of cover message such that the cover image is immune to attacks such as compression, cropping and image processing

C. Statistical methods

In this approach the message is embedded by changing the statistical properties of the cover image and uses a hypothesis for testing the extraction.

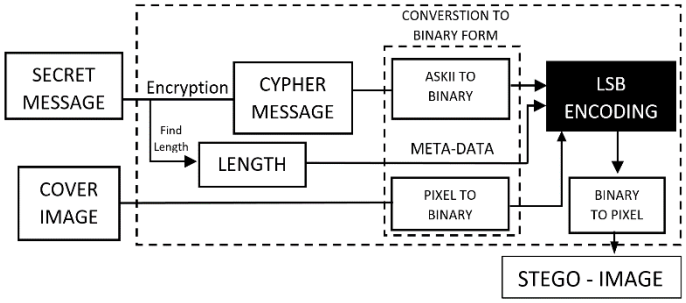

Figure A : Encrypting & Embedding Workflow

THE PROPOSED SCHEME

The proposed scheme consists of 4 steps for embedding and extracting the message in such a way that

- cover-image has no visible changes,
- message cannot be decoded easily
- large messages can also be embedded

I. Encrypting

In this scheme RSA or Diffie Hellman algorithm is used to encrypt the message. To make the message secure the ASCII value of the message is obtained to be encrypted. The encrypted message called the cypher message is used for embedding.

II. Embedding

The encrypted message obtained is converted to its binary form, the image pixels of the cover image are also converted to its binary form and the cover image is uses to embed the encrypted message. This is done by replacing the LSB of the pixels with the LSB of the encrypted message. The pixels which are modified are chosen in such a way that the pixels which are changed are distributed uniformly. The meta-data is also embedded in the first row of image in the same manner. The resulting image is called Stego-image.

III. Extracting

The Stego-image is converted to its binary form, meta-data is obtained first by reading the LSB of pixels in the first row. Using the meta-data the cypher message is extracted from the image by reading the LSB of the image pixels.

IV. Decrypting

The cipher message is then decrypted using the decryption algorithm and the original message is obtained.

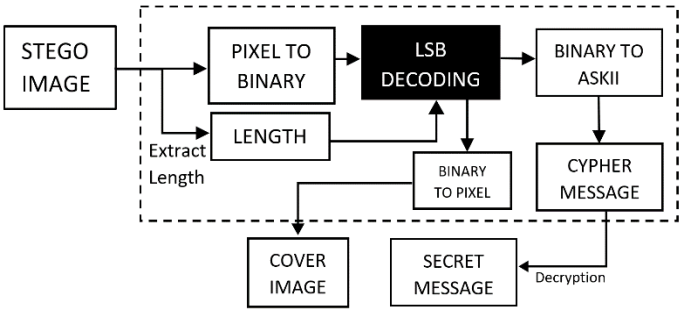

Figure B : Extracting & Decrypting Workflow

Imperceptibility Measurement

This section discusses the statistical analyses used to measure the quality of the stego-image. An imperceptible of stego-image should be high that is the image should have low distortion. There are several Imperceptibility measurements available for such as RMSE, MSE, SNR, PSNR, WPSNR, AD, R, Q index and SSIM .The paper considers the following metrics for evaluation of the performance of an algorithm used in the LSB encoder

- *Mean Square Error (MSE)*

The MSE between the original image I (M,N) and the stego-image J (M,N) is calculated by comparing the pixel bits of the two images using the formula (1)

$$MSE = \frac{1}{Mx\,N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2 \quad (1)$$

Where M and N are the number of rows and columns of the input images. The p_{ij} and q_{ij} are the pixels of the cover image and stego-image at i^{th} row and j^{th} column respectively. The MSE value should as low as possible. When the cover image and the stego-image are same the MSE value is equal to zero.

- *Signal to Noise Ratio (SNR)*

The SNR is a parameter used to measure the amount of imperceptibility in decibels. It is the ratio of signal power to the noise power. Larger SNR value indicates a huge distortion between the cover image and the stego image, and in contrast a small SNR value indicates less distortion. It can be calculated using the equation (2)

$$SNR = 10x \log_{10}\left(\frac{\sum_{i=1}^{HxW}(Ci)^2}{\sum_{i=1}^{HxW}(Ci-Si)^2}\right) \quad (2)$$

Where C_i represents the cover-image pixels and S_i is the stego-image pixel.

- *Peak Signal to Noise Ratio (PSNR)*

The PSNR is similar to SNR but is calculated with respect to the MSE values, it can be calculated using the equation (3)

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (3)$$

Where MAX = Maximum pixel intensity value which is 255.

Result

IMAGE SIZE	LENGTH OF CHARACTERS	MEAN SQUARED ERROR	SIGNAL TO NOISE RATIO	PEAK-SIGNAL TO NOISE RATION
2400 X 3840	5	0.0005	74.6449	81.1983
2400 X 3840	590	0.0007	73.1048	79.6582
2400 X 3840	5274	0.0024	67.7657	74.3192
2400 X 3840	27837	0.0106	61.3252	67.8787
550 X 550	5	0.0034	67.8767	72.7719
550 X 550	590	0.0096	63.3990	68.2942
550 X 550	5274	0.0622	55.3009	60.1961
550 X 550	27837	0.3081	48.3485	53.2437

REFFERENCE

[1] Ashwak ALabaichi , Maisa'a Abid Ali K. Al-Dabbas , Adnan Salih “Image steganography using least significant bit and secret map techniques” International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020, pp. 935~946 ISSN: 2088-8708,

[2] Shailender Gupta , Ankur Goyal , Bharat Bhushan “Information Hiding Using Least Significant Bit Steganography and Cryptography” I.J.Modern Education and Computer Science, 2012, 6, 27-34 Published Online June 2012 in MECS (http://www.mecs-press.org/)

[3] Gandharba Swain, Saroj Kumar Lenka ,“A novel steganography technique by mapping words with LSB array”, Int. J. Signal and Imaging Systems Engineering, Vol. 8, Nos. 1/2, 2015

[5] “Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats” Mohammed Mahdi Hashim , Mohd Shafry Mohd Rahim , Fadil Abass Johi , Mustafa Sabah Taha , Hassan Salman Hamad

[4] Johnson, N. F., and S. Jajodia, “Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no. 2, 1998, pp. 26-34.