International Journal of Electrical and
Electronics Engineering (IJEEE)
ISSN(P): 2278-9944; ISSN(E): 2278-9952
Vol. 7, Issue 4, Jun - Jul 2018, 23-28

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

MODIFIED LEAST SIGNIFICANT BIT BASED ON MATRIX PATTERN ON RGB IMAGES FOR IMAGE STEGANO-KEY

***Pratibha. M. Motwani*[1] *& Rahul Nawkhare*[2]**

[1]*Research Scholar, Wainganga College of Engineering and Management, Nagpur, Maharashtra, India*

[2]*Assistant Professor, College of Engineering and Management, Nagpur, Maharashtra, India*

ABSTRACT

Steganography is the hiding of a secret message with just an ordinary message and extraction of it from source to destination. It takes the process of Cryptography further advanced by hiding an encrypted message so that no one suspects it exists. It is just hidden data within data. This technique can be applied to images, an audio or video file. Data hiding embeds data into digital media for the purpose of Identification, annotation and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subjected to distortions, eg. Lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. This technique is evaluated in three applications: Copyright protection, tamper proofing, and augmentation data embedding. The main goal of data hiding is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically not distinguishable from d.

KEYWORDS: *Steganography, Cryptography, Watermark, LSB, Secret message, Encryption, Decryption, Stego-key.*

Article History

***Received:* 12 Jun 2018 | *Revised:* 27 Jun 2018 | *Accepted:* 31 Jul 2018**

INTRODUCTION

Steganography is the method of Embedding or fixing and hiding secret messages in a medium known as cover text. The concept of Steganography is completely related to Cryptography and the idea behind is that one can keep the message secret by Encoding. In contrast to Cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.[1] The goal of the Steganography is just a covert communication to hide the existence of any message. It differs from Cryptography the method of secret message which is intended to make the message undetectable by someone but it does not hide the existence of the secret message.

The methods used in Steganography make it more difficult to detect the presence of a hidden secret message inside a normal file. By this way, one can not only hide the secret message itself but also the fact that one is sending the message from source to destination. This feature makes Steganography the ideal science for hiding or concealing any message on the web. The primary goal of Steganography is to hide any message inside any other message in such a way that it prevents any suspicion of the transmission of any hidden message from source to destination. Nowadays 2D and 3D images are the most paper cover objects which are used for Steganography where an altered image with slight or little

changes in its colour or shape will be undifferentiable from an actual image by an individual, and thus the application of the Image Steganography has been highlighted.[1]

The image with secret data message hidden (embed) inside it is called as Cover Image or Stegano Image. The most common or frequently used Image Steganography technique is Least Significant Bit (LSB). The LSB substitution can be extended up to 4 LSB planes to achieve higher embedding capacity.[2] The LSB of the bytes inside an image is changed correspondingly to a bit of the secret image. The advantage of LSB embedding is its simplicity and many techniques use these methods.[3]

OVERVIEW OF STEGANOGRAPHY

Steganography is the method or an art of secret writing in the form of covered or hidden data. The term actually means "covered or secret writing". The main Objective or motive behind this is to hide the existence of the message or communication from a third party. It can hide data of different types inside a Stegano Image or cover file. The resulting or final stegano file (or image) also contains embedded hidden data irrespective of being identical to the cover file. It is used like a watermark to protect a copyright on information.[4]

Steganography exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography).[5] The secret data can be embedded inside an image or cover file using the method of Least Significant Bit (LSB) insertion. The cover image is introduced by the network of grid of 2-D matrix pattern.[1] Changes in the value of LSB are so subtle that it cannot be perceived by normal human eye. Apart from Least Significant Bit (LSB) technique, Spatial Domain technique also uses the method of Matrix Embedding in the method of Steganography.

In LSB, we can take the binary representation of data (to be hidden) and overwrite the LSB of each byte within the cover Image.[4]

The Cover Images are 2D or 3D Images. To denote coloured Images, 8 bits and 24 bits are used by gray images and Coloured images like RGB respectively.

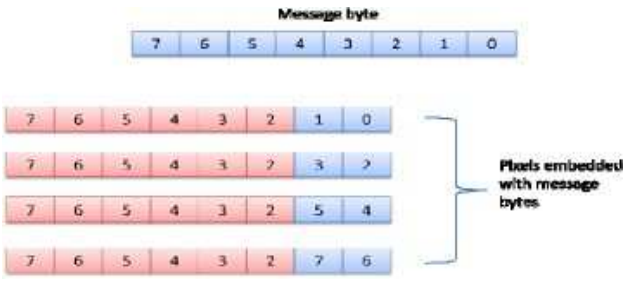

Figure 1: Proposed LSB Algorithm

The method and concept of LSB embedding and insertion is convenient to be applied. It is the process of inserting and fixing the Least significant Bit pixels in the cover image inside which the secret message is to be hidden. It is based on the fact that modifying the pixel intensity will not create enough intensity to be detected by the human eye.[6] For an 8-bit image the Least Significant Bit i.e.8th bit of each type of the image will be replaced by the 1 bit of the secret message.[7] For 24 bit image the colour of each component like RGB (Red, Green, Blue) will be changed.[7]

HARDWARE AND EXECUTION

Transferring a secret message in an unsecure network channel is an important aspect in an Information Security. The main technique used for improving security in unsecure communication is Cryptography. In Cryptography a secret message or any communication is changed in such a way that a third party would not be able to detect or read the message or communication between Source and Destination.

The Tools and Platform so required for the implementation purpose are: Laptop (Hardware), MATLAB R 2014a and Graphical User Interface (GUI) (Software).

Encryption Method: Initially, the secret and the cover images are converted to gray scale images such that the secret image is encoded with the binary, MSB bits are replaced by LSB and divided in the RGB parts. The secret message (image) is embedded in the cover Image on which a Stego-function is applied along with a stego- key or password to form a stego-object.[8] At the sender side the user embed the secret message in cover image using stego-function along with stego-key.[8]

Decryption Method: To recover the secret message from stego medium we require the cover medium and the decoding stego key.[8] It is known as Decryption.

HOW TO PERFORM SIMULATION IN MATLAB

MATLAB Simulation Process

MATLAB is nothing but a high-performance language for technical computing. MATLAB function are easy to use, graphic user interface (GUI) function guides a user by the process of encoding & decoding a message into or from image. In this method, MATLAB is used for processing the LSB Steganography technique for the different frame size 256*256, 128*128, 64*64 and the simulation results are thus shown.

There are four steps involved in implementing the LSB Steganography method as shown below.

Conversion of an Image to a Matrix

In the process of conversion of an image into the matrix, the input cover image is converted to matrix values which are stored in the text file.[1] In this process, the image should be converted to the gray scale which was originally in the RGB form.

A binary image is nothing but the digital image which has only two probable values for each pixel. The two colors that are used for binary image are black and white. The color used for an object in an image is a foreground color while rest of an image is background color. In document-scanning industry, it is often known as "bi-tonal". The Binary images are also referred to as bi-level or two-level. That means each pixel is stored as an unique single bit—0 or 1. White, B&W, Monochrome or Monochromatic is generally used for this method, but also represent images that have one single sample per pixel, like grayscale images. The images in Photoshop Parlance, binary image is same as image in "Bitmap". Binary images are often used in digital image processing as masks or the result of several operations like Segmentation, Thresholding and Dithering. Some I/O devices, like Laser printers, Fax machines, and Bilevel Computers, handle only bilevel images. The binary image may be stored in memory as bitmap, the packed array of bits. The 640×480 image occupies 37.5 KB storage. Due to the small size of the image, Fax machine and Document Management Solutions mainly use the same format. Most binary images compress with the simple run-length compression schemes.

Other category of operations are based on the notion of filtering with the structuring element. Structuring element is the binary image, which is small, that is passed over to the target image, in the exactly same manner to the filter in the gray scale image processing. As the pixels only have two values, morphological operations are erosion (unset pixels in structuring element cause a pixel to be unset) and dilation (set pixels in structuring element cause a pixel to be set). The Important operations used in this method are Morphological opening and Morphological closing that consists of erosion followed by dilation and vice-versa, using same structuring element. The opening leads to enlarge the small holes, eliminate the small objects, and separate the image. The grey image is then resized to the particular size of 256*256. Each individual image has an individual intensity values for every pixel; here those intensity values are stored in the text file. Figure 4 shows the cover image that is used here.

Figure 5, shows the intensity values of the cover image that are obtained while converting an image into matrix.

Figure 2: Cover Image

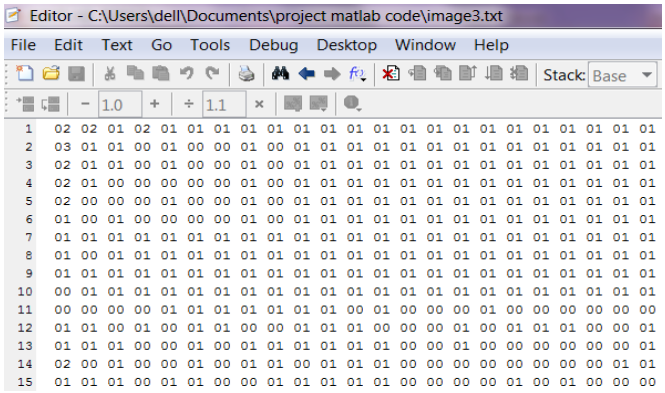

Figure 3: Cover Image Intensity Values so Obtained

The Embedding Method

In this process, the secret data or the message can be hidden or embed inside an image, after converting that image in the matrix form. The resulting image so obtained is called as stego image. It allows the user to select the appropriate image which is best suited for the cover image and in the same time also less susceptible to the steganalysis attack.[9]

Figure 4: Secret Image

Converting the Matrix into an Image

For the conversion of the matrix into an image, the intensity values of the cover image so used are transformed again to the image.[1] The resulting image i.e stego image embeds the hidden data.

The Method of Extraction

In this process of Extraction, the hidden message is extracted which was embedded earlier. This is nothing but Decryption. Decoding is exactly the reverse process of Encoding. In this step, a secret key is used to convert the cipher text into plain text. Mapping the pixels into an image is called as Extraction.[9] The requirements for data extraction are watermarked image and secret key.[10] Figure 7 shows Intensity values of Stegano Image so obtained.

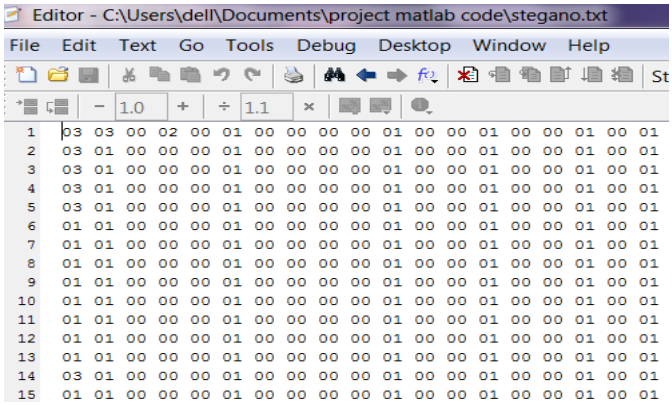

Figure 5: Intensity Values of Stegano-Image

Figure 6: Stegano Image

CONCLUSIONS

Steganography using LSB technique proposed in this project presents multiple aspects of data hiding and thus help to hide the data inside the cover object. This project mainly focuses on the design of encoding and decoding system rather than the contents of the transmitted message. Also, MATLAB features a family of add –on application specific solution called toolboxes. Very important to the users of MATLAB, toolboxes allow us to learn and apply specialized technology.

REFERENCES

1. *Champakamala. B. S, Padmini. K, Radhika.D.K. Assistant Professors, Department of TCE, Don Bosco Institute of Technology, Banglore. "Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology (IJACT), ISSN: 2319-7900.*
2. *S. Guneswari, R. Balu "A New Paradigm of LSB based Image Steganography with Cryptography using DIFFIE Helman Algorithm ", International Journal for Research in Applied Science & Engineering Technology (IJRASET); Vol.5, Issue XII, December 2017, ISSN: 2321-9653.*
3. *International Journal of Computer Science Engineering Technology (IJC-SET) "Modern Steganographic technique: A Survey ", by Pratap Chandra Mandal Asst. Prof, Department Of Computer Application B.P.Poddar Institute of Management Technology.*
4. *Ronak Doshi, Pratik Jain, Lalit Gupta "Steganography and its applications in Security", International Journal of Modern Engineering Research (IJMER); Vol. 2, Issue.6, Nov- Dec 2012, ISSN: 2249- 6645.*
5. *Sheelu, Babita Ahuja "An Overview of Steganography" IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 1 (May- June 2013) e-ISSN: 2278-0661, p-ISSN: 2278-8727*
6. *Jassim Mohmmed Ahmed and Zulkarnain Md Ali "Information Hiding using LSB technique" IJCSNS International Journal of Computer Science and Network Security; Vol.11, No 5, April 2011.*
7. *Anil Kumar, Rohini Sharma "A Secure Image Steganography Based on RSA Algorithm and Hash LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering ; Volume 3, Issue 7, July2013, ISSN: 2277-128X*
8. *Sneha Bansod, Gunjan Bhure, "Data Encryption by Image Steganography" International Journal of Information and Computation Technology; Vol.4, No.5, 5 November 2014, ISSN: 0974-2239.*
9. *Preeti Kumari, Ridhi Kapoor " Image Steganography for data Embedding & Extraction using LSB technique" International Journal of Computer Applications & Information Technology Volume 9, Issue 2, July 2016, ISSN: 2278-7720*
10. *P. Thiyagarajan, G. Aghila "Reversible Dynamic Secure Steganography for Medical Image using Graph Coloring" Health Policy and Technology. Vol.2, No.3, 2013, pp. 151-161*