© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Confidentiality of Data Through Steganography

M. Himabindu., E. Susmitha
M.Tech Academic Assistant, IIIT RK Valley, RGUKT, Andhra Pradesh, India

ABSTRACT

Now-a-days providing security & making data to be confidential plays a major role. For the purpose of providing confidentiality we are employing the cryptography techniques. Even though the data get encrypted, the intruder easily modifies the data by knowing the presence of confidential data. Steganography, which can called as an extension to the cryptography. Hereby employing this technique, can remain the existence of information in confidential. For providing security an image is used as a carrier medium to hold the secret data. Thereby no one can have an idea there is a secret message with in an image. The LSB technique of steganography is going to be applied here and secret key is generated by using one of cryptography technique OTP. With this method we can hide the data efficiently and effectively.

Keywords: Cryptography, JPEG Lossy Compression, DCT, DFT, DWT

I. INTRODUCTION

Fast growth of computer networking in information sharing leads to the increasing threats of attacks. Cryptography [1] the secret writing of information refers to conceal text by using the encryption. By which, up to some extent we can secure the data. But the intruders even get successful in eavesdropping; with the reason the information mostly they acquire is in the form of text that gives the presence of message and once get to know the key they can easily modify or misuse the data.

Steganography, one of the hiding approach or an alternative method for providing security and privacy where an image is utilized as a medium/carrier to conceal the text. The aim of this approach is to avoid the existence of information or data to the intruder. The media that can be used for hiding the information not only limited to the image files can extend it to audio files, text files and video files. As images are more popular when compared to other to be used as cover object. Because of the slight variations to the image that has made in channels will be indistinguishable from original image by a human being.

While using images that are having high resolution can be compressed by using lossy and lossless process. If the image is of JPEG Lossy compression is employed and for BMP, gif & png we can use Lossless algorithm.

There is different number of stegan graphic techniques [4] are used for the image file format:

1. **SPATIAL DOMAIN TECHNIQUE**: Change some bits in the image pixel values with the hiding data.LSB is the simplest replacement technique.
2. **TRANSFORM DOMAIN TECHNIQUE**: Message is inserted into transformed coefficients of image giving more information hiding and more robustness against attacks. .., DFT and DCT and DWT.
3. **DISTORTION TECHNIQUE**: Hide information by signal distortion and to restore, measure deviation from the original cover in the decoding process.

From the different number of techniques LSB [3] insertion is a simple and efficient technique for embedding data in a cover file.

II. STEGANOGRAPHY

Steganography is the word derived from Greek. Stegano means covers and grafia means writing; defines Steganography as a covered writing. It is an art and science of secret communication, where it encodes the information in a way such that the information existence is invisible.

The features that characterize the embedding techniques are of:

INVISIBILITY: Imperceptibility of Steganography is an important necessity. The quality of Steganography lies in its capacity to see unseen by naked eyes.

PERCEPTUAL TRANSPARENCY: It is referred as an inability of eavesdropper to detect hidden data.

Within Steganography for hiding information a medium requires:

1. Cover object is referred by original file.
2. Stego image is referred as the file after embedding the secret information.
3. A key for encoding and to restrict the data from extracting or its detection.
4. Stegangraphy technique

III. IMAGE STEGANOGRAPHY

Image [5] is used as the cover medium for Steganography. A message embedded in digital image and encrypted by using a secret key and stego image is send to the receiver.

Digital images which are of gray scale use 8 bits for each pixel i.e.,1byte and displays up to 256 colours.The color images[6] of having 3 channels(R,G&B), totally having 24 bits thereby 256 different quantities of red, green and blue

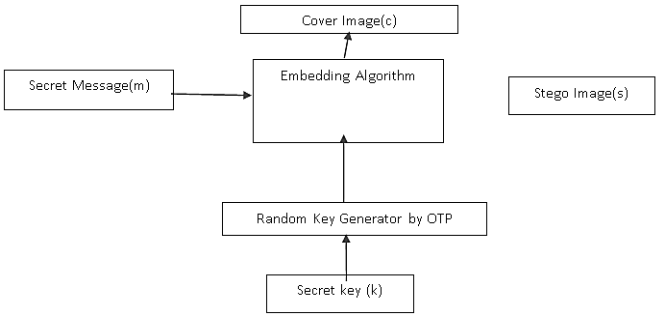

Fig: Block diagram of embedding algorithm

LSB (Least Significant Bit):

One of the Steganography technique used for hiding the data in the cover object by replacing the least significant bits of image with the secret data. The encrypted data has to be converted it into binary format by using ASCII. In cover image, bytes representing image taken in single array and generate the byte stream. Message bits taken sequentially and replace with LSB bit of image byte. Here we can extend to one more bit when message is large.

01001001

MSB. LSB

For e.g.: the message or data to send is ' I '.The ASCII value of 'I' is 73 & the binary value [2] of it is 01001001.This message has to be inserted in the right most bit of image pixel.

Consider the image of 3x3

01101010.	11110010.	00110110
01101001.	11110000	00110101
01100000	11101111	00110100

The message is embedded at the right most significant bit of the each pixel byte.

01101010	11110011	00110110
01101000	11110001	00110100
01100000	11101111	00110100

The digit highlighted with red are the bits of the secret message, are embedded in the cover object by LSB insertion.

The procedure for message embedding is as follows.
S (i,j)=C(i,j)-1, if LSB[C(i,j)]=1 & m=0
S(i,j)=C(i,j), if LSB[C(i,j)]= m
S(i,j)=C(i,j)+1, if LSB[C(i,j)]=0 & m=1
Where S(i,j) is the stego image, C(i,j) is the cover object & m is the message bit to embed.

The resulting stego image by the changes made to LSB is too small to be recognized by human eye. Because it allows high perceptual transparency's that the message is effectively hidden.

ENCODING TECHNIQUE

The data in the cover image is encrypted by using OTP (one time pad), which is a provably secure cryptosystem. An arbitrary long non-repeating sequence of 0's and 1's generated for the key as of same length as message. The encryption is done by adding the key to message, often said to be as Ex-OR(⊕).

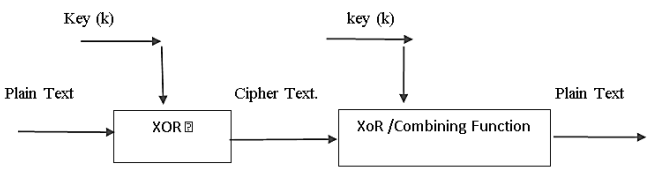

Fig : Vernam Cipher (One-Time Pad)

For e.g.: the data is HI

H- 01001000 and I - 01001001

The arbitrary long repeating random key is of : 01000110 01100010 10010101

Plain text - 01001000 01001001.
Ciphertext: 00001110 00101011
Key : 01000110 01100010
Key : 01000110 01100010
Cipher text(⊕) - 00001110 00101011
Plaintext: 01001000 01001001

In this manner, we encrypt the data that has to be embedded in the cover object.

Randomly generated key once used can't be repeated it again. By that intruder even have an idea about the key. In this way, the data get encrypted. After encrypting the message, it embedded in the cover image with LSB substitution.

APPLICATIONS

1. Secret communication
2. Feature tagging &
3. Copyright protection.

IV. CONCLUSION & FUTUREWORK

For secure communication over the internet, Steganography is the very useful technique and also effective method for hiding sensitive information. With this process, the message hidden is invisible. The cryptography technique OTP implemented to the data that is to be hidden in cover object provided with additional security. Only sender & receiver know how to extract and retrieve the data. No other person knows there is a data inside the cover object. The high perceptual transparency is allowed by the LSB embedding technique and advantage of this technique is its simplicity.

Future research can extend to the other cryptography techniques and generate a random key to choose the pixels randomly and embed the message. Data can be hidden in the LSB of a particular color plane of randomly selected pixel in RGB color space.

V. REFERENCES

[1]. Danny Adiyan Z, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni,"Implementation of Secure Steganography on Jpeg Image Using LSB Method ",International Journal of Applied Engineering Research , Volume 13, Number 1 (2018) pp.

[2]. M. Al-Husainy, ”A New Image Steganography Based on Decimal-Digits Representation, Computer and InformationScience”, vol. 4, no. 6, pp. 38-47, 2011.

[3]. Akash Modi, Manu Bansal, “An Enhanced LSB Steganography Algorithm for Data Hiding”,International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 5, May 2015.

[4]. Mukesh Gurg and A.P. Gurudev Jangra “An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques”Proceeding of the IJAECSSE, Volume 4, Issue 1, January 2014

[5]. Vandana Yadav & Sanjay Kumar Sharma,"A Survey Paper on Data Hiding in Images using Image Steganography",International Journal of Innovative Engineering Research (E-ISSN: 2349-882X) Vol 7, Issue 1, February 2017

[6]. Thakur Ramesh Kumar, Saravanan Chandran, “Analysis of Steganography with Various Bits of LSB for Color Images”, International Conference on Electrical, and Optimization Techniques , 2016.

VI. AUTHORS PROFILE

M. HIMABINDU, received M.Tech degree in Computer Science and Engineering (Computer Science) from Jntu Anantapur University, Anantapuramu, A.P, India, during 2014 to 2016. Her area of interests in Networking & Android. Currently working as an Academic Assistant in IIIT rgukt, rkvalley from 2016-2018.

E. SUSMITHA, received M.Tech degree in Computer Science and Engineering (Software Engineering) from junta anantapur University, Anantapur, A.P, India, during 2014 to 2016. Her area of interests is Android. Currently working as an Academic Assistant in Iiitrgukt, rkvalley from 2016-2018.