ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Survey on LSB Based Image Steganography Using Java Encryption API

Sangeeta, Ajit Singh

M.Tech Scholar, Dept. of CSE, TIT&S Bhiwani, Haryana, India

Assistant Professor, Dept. of CSE, TIT&S Bhiwani, Haryana, India

ABSTRACT: Steganography is one of the most powerful techniques to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects for Ste-ganography and in this work image steganography is adopted LSB is well know method for stegnography. There are several changes suggested by different researchers time to time on LSB and stegnography. A large number of commercial steganographic programs use the Least Significant Bit (LSB) embedding as the method of choice for hiding data as it has low computation complexity and high embedding capacity.

KEYWORDS: Image based steganography, LSB method, image encoding algorithm, image decoding algorithm

I. INTRODUCTION

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages. After embedding a secret message into the cover image a so – called stego-image is obtained. Two other technologies that are closely related to steganography are watermarking and fingerprinting.

Type of steganograpy : There are 4 different types of steganography.
a. Image
b. Audio
c. Video
d. Protocol

Text steganography using digital files is not used very often since text files have a very small amount of redundant data.
Audio/Video steganography is very complex in use. In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file.

Image steganography is widely use for hiding process of data. Because it is quite simple and secure way to transfer the information over the internet. Image steganography has following types:
a. Transform domain
i. Jpeg
b. Spread spectrum
ii. Patch work
a. Image domain
i. LSB and MSB in BMP
ii. LSB and MSB in JPG

It is most efficient (in term of data hiding) method of image steganography. Because the intensity of image is only change by 1 or 0 after hiding the information.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

II. LITERATURE REVIEW

Steganography in Greek means "covered writing". Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view.
There are varieties of steganographic techniques available to hide the data depending upon the carriers we use. Steganography and cryptography both are used for the purpose of sending the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption and secret key. In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption.

Mamta Juneja, and Dr. Parvinder S. Sandhu (2013), proposed an improved LSB (least Significant bit) based Steganography technique for images imparting better information security. They present an embedding algorithm for hiding encrypted messages in non adjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret message, and detects edges in the cover-image using improved edge detection filter. Message bits are then, embedded in the least significant byte of randomly selected edge area pixels and 1-3-4 LSBs of red, green, blue components respectively across randomly selected pixels across smooth area of image.

M.Rajkamal and B.S.E.Zoraida (2014), developed a new technique of image steganography inside the embedding the encrypted Data file or message using Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The developed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the carry image. This technique makes sure that the data has been encrypted before embedding it into a carry image. Embedded-text in images usually carries important messages about the content.

In another article by Hemalatha .Set. Al. Integer Wavelet Transform (IWT) has been suggested to hide multiple secret images and keys in a colour cover image which is more efficient. The cover image is represented in the YCbCr colour space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

In Keith .L. Haynes article the author studies the use of image steganography to breach an organization's physical and cyber defences. The proposed method utilizes computer vision and machine learning techniques to produce messages that are undetectable and if intercepted cannot be decrypted without key compromise. To avoid detection DWT (Discrete Wavelet Transform) is used.

III. PROPOSED STUDY

- To hide the message or a secret data into an image which acts as a cover Medium.
- The primary motivation of my current work is to increase efficiency and accuracy of the stego image.
- To develop a software system (Java Based) for stegnography of images. The system will be able to hide the message within image and will be able to retrieve the message back from the image.
- The Software system used LSB method for stegnography and encryption using Java APIs.

We investigated the methods of stenography with the special emphasis of method of LSB. Also we developed a Java based system to hide the message inside an image and to retrieve the information back from the information.

Least significant bit (LSB) method

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image, audio and video steganography.

To the human eye, the resulting image will look identical to the cover object. For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

ENCRYPTION USING JAVA

Encryption is the process of converting plain data (plaintext) into some other format that appears to be random and meaningless (cipher text). Decryption is the process of translating cipher text back to original format of text (plaintext). To encrypt more than a small amount of data, symmetric encryption is used. Java uses javax. crypto package for encryption and decryption. Here central class is Cipher, which is used to encrypt and decrypt data. Cipher Input Stream and Cipher Output Stream are utility classes that use a Cipher object to encrypt or decrypt streaming data. Sealed Object is another important utility class that uses a Cipher object to encrypt an arbitrary serializable Java object. The Key Generator class creates the Secret Key objects used by Cipher for encryption and decryption. Secret Key Factory encodes and decodes Secret Key objects. The Key Agreement class enables two or more parties to agree on a Secret Key in such a way that an eavesdropper cannot determine the key. The Mac class computes a message authentication code (MAC) that can ensure the integrity of a transmission between two parties who share a Secret Key. A MAC is akin to a digital signature, except that it is based on a secret key instead of a public/private key pair.

Algorithm for Encryption Using Java

1. Take string to be Encrypt.
2. Calculate key for encryption
a. Use Secret Key Spec.
b. Secret Key Spec's constructor take user define bytes array to generate Key
3. Create Cipher's object basis on key.
4. It encrypts string data and Encodes using Base64Encoder.
5. And return encrypted message.

Algorithm for Decryption Using Java

1. Take string to be Decrypt.
2. Get key for decryption
3. Create Cipher's object basis on key.
4. It decrypts string data and decodes using Base64Encoder.
5. And return Decrypted message.

IV.CONCLUSION

This paper is a short introduction to the world of steganography. We have shown how the simplest methods work and how they can be explored. We have used symmetric encryption algo to provide more security. For security of encrypted data, a lot of complex algorithms were suggested by researchers. Most of these algorithms were very effective but these algorithms are a bit complex in understanding and implementation. So we used our own algorithm for storing length of message, for encoding message location etc.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

REFERENCES

[1] Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research, vol 39(1), pp 231-239.
[2] Aneesh Jain, IndranilSen Gupta, ―A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images‖, TENCON 2007 - 2007 IEEE Region 10 Conference, vol.2
[3] Attalla M. Al-Shatnawi, "A New Method in Image steganography with improved image quality", Applied mathematical science, Vol. 6, no79, 2012.
[4] A Joseph Raphael et al(2012), Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3) pp 626-630
[5] Bassam Jamil Mohd Saed Abed and Thaier Al- Hayajneh, Computer Engineering Department Hashemite University, Zarqa, Jordan Sahel Alouneh,ComputerEngi-neering Department, German-Jordan University, Amman, Jordan, "FPGA Hardware of the LSB Steganography Method" IEEE 2012.
[6] CHIN-CHEN CHANG, H.W .TSENG. ,"A steganographic method for digital images using side match. Pattern Recognition Letters, 2004, vol. 25, p.1431-1437.
[7] Himanshu Gupta et al(2013), Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6 pp 212-214
[8] Mamta Juneja (2013), An Improved LSB based Steganography Technique for RGB Colour Images, 2nd International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18
[9] Masoud Nosrati (2013), an introduction to steganography methods, World Applied Programming, Vol (1), No (3) pp 191-195
[10] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, Image Steganography and: Concepts and Practice", Department of Electrical and Computer Engineering Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201, USA.