IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 5 Issue 12 December, 2017

Image Steganography Techniques using LSB Method

Debasish Hati[1] ; Arnab Pal[2]; Tapanjan Dutta[3]

Lecturer, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]
Final Year Student, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]
Final Year Student, Technique Polytechnic Institute, Hooghly, West Bengal, India[1]

debasishhati2013@gmail.com[1]; arnabpal9999@gmail.com[2]; tapanjandutta99@gmail.com[3]

ABSTRACT

This paper, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.

*In this paper I purposed an image based steganography that Least Significant Bits (LSB) techniques and pseudo random encoding technique on images to enhance the security of the communication. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In Pseudo-Random technique, a random-key is used as seed for the Pseudo-Random Number Generator is needed in the embedding process.***Keywords:** Steganography, LSB, Random-key, Image, secret message, stego-key,cover image,Techniques.

1. INTRODUCTION

The use of multimedia digital signal has become very popular in the last decade due to the spread of wireless Internet-based services such as introduction of the fourth-generation mobile communication systems, user can transfer data up to 1Gbps.Due to the availability of low cost editing tools, digital data can be easily copied, modified and retransmitted in the network by any user. To effectively support the growth of multimedia communications, it is essential to develop tools that protect and authenticate digital information. In this contribution, we present a novel embedding scheme based on the LSB technique. If the value of the pixel of an image is changed by a value of '1' it does not affect the appearance of the image. This idea helps us to for hiding data in an image. Steganography is the art and science of invisible communication in the sense that it does not specify anything whether any communication is taking place or not. This is accomplished by hiding information in any other form of information, thus hiding the existence of the original information to be transmitted . Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means "cover writing". Steganography means to conceal messages' existence in another medium (audio, video, image, communication). Steganography is different from cryptography in the sense that cryptography focuses only on keeping the contents of a message secret, whereas steganography focuses on keeping the existence of a message secret. We have used image steganography in which the information is hidden exclusively in images. We are using LSB algorithm for image steganography.

Image steganography terminologies are as follows:-

• **Cover-Image:** Original image which is explicitly used as a carrier for hidden information to be transmitted.

- **Message:** Actual information which is used to hide into images. Message could be a plain text or some other image.

- **Stego-Image:** After embedding message into cover image what we get is known as stego-image.

- **Stego-Key:** A key that is used for embedding or extracting the messages from cover-images and stego-images.

2. TYPES OF STEGANOGRAPHY

Depending on the type of the cover object there are many suitable stenographic techniques which are in order to obtain security.

a) **Image Steganography:** The process of concealing the secret message in an image file is known as image steganography. It has certain limitations like you cannot embed a large amount of data in an image because it may distort which may arise suspicion that the image might contain any information.

b) **Video Steganography:** The process of concealing the secret message in an Video file is known as Video steganography. Video Steganography is far more safe and efficient as compared to that of the image steganography as you can embed large amount of data in audio and frames of the video.

c) **Network Steganography:** Network Steganography method uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relations between exchanged PDUs, or both (hybrid methods). It is Highly secure and robust.

d) **Audio Steganography:** In Audio Steganography audio is used as the cover to hide the secret information it is also very robust in nature but with limitation of the amount of data one can hide.

e) **Text Steganography:** Secret Data is hided in a text file. This method lacks robustness and is not that much efficient in hiding the data. It can be easily detected by the eyes of intruders.

3. LITERATURE SURVEY

Champakamala .B.S et.al: on their paper state the Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. A new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.

Dr. Rajkumar L Biradar & Ambika Umashetty have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications. It proposes different techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods .

Bibhudendra Acharya et.al: On their paper proposed a novel advanced Hill (AdvHill) encryption technique which uses an involutory key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background.

Mohammad Ali Bani Younes & Aman Jantan worked on a steganography method to embed information within an encrypted image data randomly. The approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Experimental results show that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image, and reduces the chance of the encrypted image being detected.

T. Morkel et.al, discussed on their paper that there exists a large selection of approaches to hiding information in images with different strong and weak points. Where one technique lacks in payload capacity, the other lacks in robustness. Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he wants to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

4. PROPOSED METHODOLOGY

We have used LSB and IDEA algorithm both together for hiding and securing of data. At sender's side we are first applying IDEA algorithm to the plaintext. Then after we get the cipher text, we are using LSB for hiding the encrypted data. In this way even if an attacker comes to know the existence of secret data he/she must first have to deal with the cover image then comes the encrypted data, Which obviously does not make any sense unless decrypted. So, the proposed

technique helps in improving the data security, thus prevents the data from being attacked and tempered.

4.1 LSB Algorithm:

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 100, which binary representation is 1100100, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

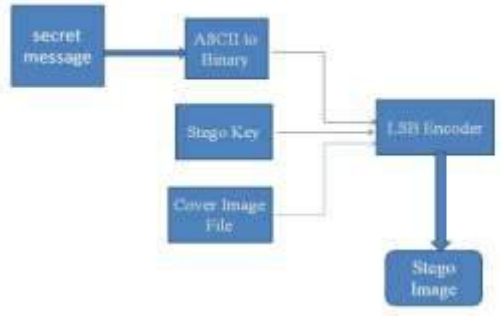
(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101101 01100011)

For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images.

Fig: LSB Insertion Mechanism



LSB METHOD WITH AN EXAMPLE

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement.LSB replacement steganography changes the last bit of each of the pixel values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale color value. Suppose the first eight pixels of the original image have the following gray color values:

01010010

01001010

10010111

11001100

11010101

01010111

00100110

01000011

To hide the letter Z whose binary value of ASCII code is 10110101, we would replace the LSBs of these pixels to have the following new values:

01010011
01001010
10010111
11001101
11010100
01010111

00100110

01000011

Note that, on average, only half the LSBs need to change.The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats for the color image are difficult to detect contrary to 8 bit format.

5. ADVANTAGES & DISADVANTAGES

Steganography has unique advantages for net-espionage agents. Even if a file is known or suspected to contain Steganographic software, it is almost impossible to

extract the information until the correct password is obtained. Steganography is beneficial for securely storing sensitive data, such as hiding system passwords or keys within other files. In places where standard cryptography and encryption is outlawed, Steganography can be used for covert data transmission. Key distribution.

6. COMPLEXITY OF ALGORITHM

Complexity of algorithm is depend on size of key and text it is approximately equal to O (mn) where m and n is size of key and text respectively.

7. APPLICATIONS

Steganography can be used in supplementary to cryptography, watermarking and fingerprinting. Steganography can be used to conceal and transfer an encrypted document containing some acquired information in military applications.

8. FUTURE SCOPE

Still efforts have to be made to increase the embedding capacity and maintain secrecy. In this method we can hide text file equal to the size of the image. Efforts can be made to hide text files having more size than image size. The secret keys have to be known to both sender and receiver. Keys are not sent in cover-images but are distributed separately. A technique can be evolved so that these keys can be generated and distributed covertly. The Transform Domain method can be utilized if more security is required. If Steganography is used with Cryptography, it will prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques.

9. CONCLUSION

This paper has looked in detail at the major techniques used for data hiding in image files. The enhanced LSB technique described in this project helps to successfully hide the secret data into the cover object without any distortion. Matlab function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively.

10. REFRENCES

[1] Sara Khosravi, MashallahAbbasiDezfoli, Mohammad HosseinYektaie, " A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication" , Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.

[2] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA,2000.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.

[4] Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at:http://www.krenn.nl/univ/cry/steg/article.pdf

[5] Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.

[6] ShashikalaChannalli et al ," Steganography An Art of Hiding Data "International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[7] Gruhl D, Lu A, Bender W. Echo hiding. *Lecture Notes inComputer Science*, 1996, 1174: 295-315.

[8] Xu Chansheng, Wu Jiankang, Sun Quibin, et al. Applications of digital watermarking technology in audio signals. *Journal of Audio Engineering Society*, 1999, 47(10): 805-812.

[9] Garcia R A. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In: 107th AES Convention. New York, USA, 1999:2713-2720.

[10] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algo-rithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012.

[11] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh, Computer Engineering Department Hashemite University, Zarqa, Jordan Sahel Alouneh,Computer Engi-neering Department, German-Jordan University, Amman, Jordan, "FPGA Hardware of the LSB Steganography Meth-od" IEEE 2012.

[12] Atallah M. Al-Shatnawi, "A New Method in Image ste-ganography with improved image quality", Applied mathe-matical science, Vol. 6, no79, 2012.

[13] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M, "Image Steganography Techniques: An Over-view", International Journal of computer science and securi-ty, vol (6), Issue (3), 2012.