Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

Steganography Using Least Signicant Bit Algorithm

Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav
Maharashtra Academy of Engineering, Pune university
Department of Computer Engineering

ABSTRACT
The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. One of the most important factors of information technology and communication has been the security of the information. For security purpose the concept of Steganography is being used. Steganography is art and science of invisible communication. Our paper deals with image steganography. Various steganographic algorithms like Least Significant Bit (LSB) algorithm, Jsteg and F5 algorithms, out of these we are using LSB algorithm.

Steganography is the method through which existence of the message can be kept secret. This is accomplished through hiding information in another information, thus hiding the existence of the communicated information. This paper gives a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hidding the data into image which is implemented through the Microsoft .NET framework.

Keywords **– Carrier File, Decryption, Encryption, LSB, Stego key**

1. INTRODUCTION
Since the rise of the internet, the most important factor of information technology and communication has been the security of information. Cryptography is a technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the technique used for implementing this.

Steganography is the art and science of invisible communication of messages. This is done by hiding information in other information, ie. hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden in images. The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

The difference between Steganography and Cryptography is that the cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret. Steganography and cryptography both are ways for protecting information from unwanted parties. Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property of owner to identify customers who break their licensing agreement by supplying the property to third parties. This paper describes the LSB algorithm used for image steganography to illustrate the security potential of steganography for business and personal use.

2. PROBLEM DEFINITION
The aim of the project is to hide the data over an image using least significant steganographic algorithm and to send the stego file to the destination where the retrieving of the secret data is done.

2.1 Problem Solution
The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of the project is to

hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the destination securely without any
modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorised person to modify the data. So, the data encryption into an image and decryption and steganography plays an important role in this project.

3. MAJOR PERFORMANCE OBJECTIVES

The main objective of the project is to discuss the properties which help to transmit the secret message or information over a network without any modifications. The characteristics of information are:

1) Availability
2) Accuracy
3) Authenticity
4) Confidentiality
5) Integrity

4. PROPOSED SYSTEM ARCHITECTURE

The data hiding patterns using the steganographic technique in this project can be explained using this simple block diagram. The block diagram for steganographic technique is as follows.

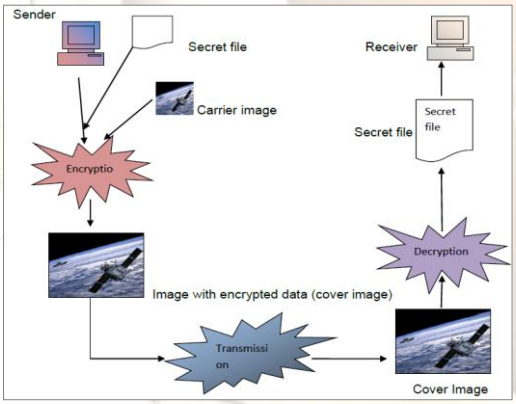

Figure: Block diagram for Steganography

The procedure for data hiding using steganographic algorithm is as follows:

1) The sender first uses the steganographic algorithm for encrypting the secret message.

2) For this encryption, the sender uses any text documents or audio or video files in which the data is written and the image file as a carrier file in which the secret message or text document or audio or video file to be hidden.

3) The sender sends the carrier file and text document or audio or video file to the encryption phase for data embedding, in which the text document or audio or video file is embedded into the image file. In encryption phase, the data is embedded into carrier file which was protected with the password. Now the carrier file acts as an input for the decryption phase. The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase. In the decryption phase, the original text document or audio or video file can be revealed using the appropriate password. The decryption phase decrypts the original text document or audio or video file using the least significant bit decoding and decrypts the original message.

As mentioned in the above block diagram, the data hiding and the data extracting will be done in three phases.

1) Encryption Phase:

The "Encryption phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image using "Least Significant Bit algorithm" (LSB) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image.

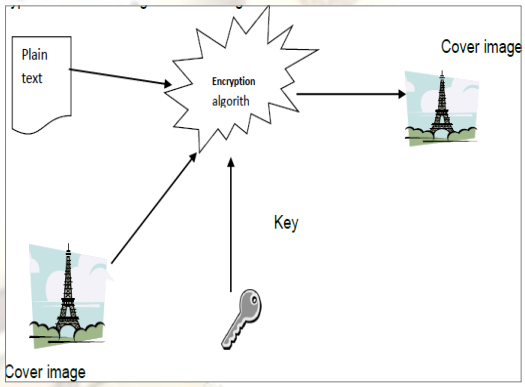

Figure: Encryption phase

2) Transmission Phase:

The transmission phase is one of the important sections for sending the data to destination securely.

3) Decryption Phase:

The Decryption phase is reverse to encryption phase. In decryption phase, the carrier image in which the data is hidden is given as an input file. The decryption phase uses the same password which was given for the encryption and decryption in order to secure from unauthorized access. After giving the correct password the decryption section uses the "Least Significant bit Algorithm" (LSB) by which the encoded bits in the image is decoded and turns to its original state and

gives the output as a text document or audio or video file as well as image.

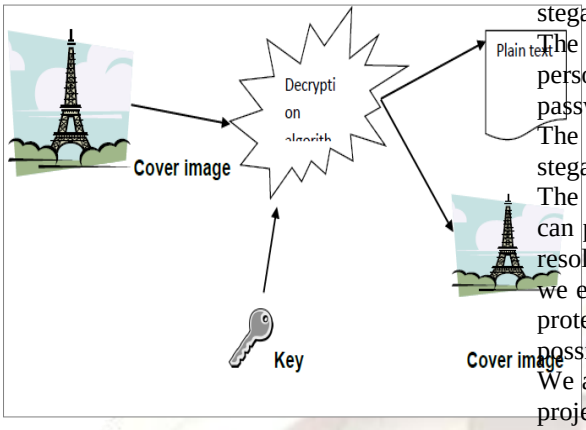

Figure: Decryption Phase

5. FUTURE SCOPE

The proposed approach in this project uses a steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured.
The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel.

We will use the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.
The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size as well as the carrier image size. The future work on this project is to improve the compression ratio. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

6. APPLICATIONS

1) Enables secret communication
2) Complements regular encryption: Harder to break: need to first find the encrypted secret text then it needs to be decrypted
3) Tremendous use in Military Applications

7. CONCLUSIONS

The proposed approach in this project uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured.
The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel. We are using the Least Significant Bit algorithm in this project for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithm.

8. MATHEMATICAL MODEL:

Discrete cosine transformations (DST)), are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each. Each DCT coefficient F(u, v) of an 8 x 8 block of image pixels f(x, y)is:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right]$$

where $C(x) = 1/\sqrt{2}$ when x equals 0 and $C(x) = 1$ otherwise. After calculating the coefficients, the following quantizing operation is performed:

$$F^{Q}(u,v) = \left[\frac{F(u,v)}{Q(u,v)}\right]$$

where Q(u, v) is a 64-element quantization table. A simple pseudo-code algorithm to hide a message inside a JPEG image could look like this:

Input: message, cover image
Output: steganographic image containing message
while data left to embed do
get next DCT coefficient from cover image
if DCT 6= 0 and DCT 6= 1 then
get next LSB from message
replace DCT LSB with message bit
end if
insert DCT into steganographic image
end while

9. ACKNOWLEDGEMENTS

It is our privilege to acknowledge with deep sense of gratitude towards our seminar guide, Prof. **Kavitha**, for her valuable suggestions and guidance throughout course of study and timely help given in the completion of our preliminary project work on
"Steganography using least significant bit ".

It is needed a great moment of immense satisfaction to express out profound gratitude, indebtedness towards our **H.O.D Uma Nagaraj**, whose real enthusiasm was a source of inspiration for us.

We would also like to thank all other faculty members of Computer Engineering department who directly or indirectly kept the enthusiasm and momentum required to keep the work towards an effective project work alive in us and guided in their own capacities in all possible.

11.REFERENCES

[1] Amirthanjan,R. Akila,R & Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application, 2(3), pp.2-10.

[2] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in Technology, 1(1), pp.05-11.

[3] Bloom,J. A. et al.,2008. Digital watermarking and Steganography. 2nd ed. Morgan Kaufmann.
Bishop, M., 2005. Introduction to computer security. 1st ed. Pearson publications.

[4] Chan, C.K. Cheng, L.M., 2004. Hiding data in images by simple lsb substitution: pattern recognition.vol 37. Pergamon.

[5] Cox, I. Miller, M. Bloom, J. Fridrich, J & Kalker, T. 2008. Digital watermarking and Steganography. 2nd Ed. Elsevi