Simulation of Different Image Formats with Network Security Techniques in Wireless Communication

Brajesh Sharma[1] Mrs. Shikha Singh[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Dr. C.V. Raman University, Bilaspur, Chhattisgarh-India

Abstract— *Steganography is the network security technique. In which many carrier file formats can be used, but digital images are the most used in the Internet. It is basically used for hiding information in the cover image to form stegoimage. Different applications have different requirements of the steganography technique used. For example in license, Pan card, aadhar card, smart card, Personal identification card the secret information is hidden in the stegoimage. This is a review paper on image steganography, its uses and techniques.*

Keywords— Network Security Technologies, LSB Cryptography, Steganography, Image Steganography

I. INTRODUCTION

In today's world since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Network is the combination of two or more devices in which information is exchanged. Network security is the important task to provide security to the information exchange between devices in the network. There are two types of network security techniques cryptography and steganography. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

II. NETWORK SECURITY (STEGANOGRAPHY)

Steganography is the advanced network security technique in wireless communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdroppers' suspicion.

A classical steganography system's security relies the encoding system's secrecy. Modern steganography is designed similar to the secret key system that is to be detectable only if secret information is known.

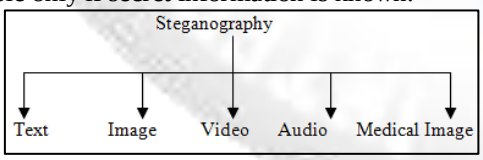

Fig. 1: Categories of steganography

A. Steganography Termenologies

- Image: An image is an array of numbers that represent light intensities at different points (pixels) and mathematically an image C is a discrete function assigning a colour vector c(x, y) to every pixel (x, y).
- Cover Image: The cover image is the carrier of the secret message. A cover is usually chosen in a way that seems more common and harmless and not arouses suspicion.
- Stego Image: The cover image with a hidden secret message inside is known as the Stego image. It is employed at the receiver site to pull out the hidden message.
- Stego Key: Stego key is a key to integrate the information inside cover medium and extract same information from the stego medium. Can be a number generated by a pseudo-random numbers or may be only a password to decode the embedding location.
- Embedding Domain: The Embedding domain refers to the cover medium characteristics that are exploited in embedding message into it. It may be spatial domain when direct modification of the constituent elements of the cover is modified (e.g. pixels in an image) or it can be the frequency domain or transform domain if mathematical transformations are carried on the medium.

III. METHODOLOGY

In this work, a new technique of LSB steganography is applied which is an improvised version of one bit LSB technique. One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is to use steganography. Stegnography is a technique of hiding information in digital media.

A. LSB Method

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image. The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater that that perceivable by average human vision. Therefore, an altered image with slight variation in its colors will be indistinguishable from the original by a human being, just by looking at it. The secret message is embedded on cover image through different stegonographic technique. The embedded cover image with secret message is called stego image. The embedding process involves input cover image, stego-key, secret message and output stego image the pixels of the cover image is replaced by secret message.

B. LSB Insertion Mechanism

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.

For example, suppose one can hide a message in pixel of an image (8-bit grayscale). Suppose the original pixel is

(11101010 11101000 11001011)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.

(11101010 11101001 11001010)

The following figure 4.3 shows the mechanism of LSB technique

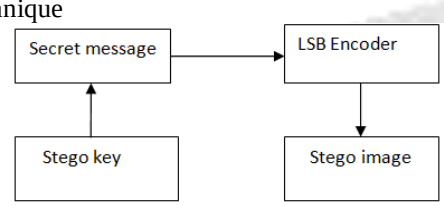

Fig. 2: shows the mechanism of LSB technique

C. LSB Extraction Mechanism

The extraction process involves inputs stego-image, stego-key, and output secret text message. The following figure 4.4 shows the mechanism of LSB extraction technique

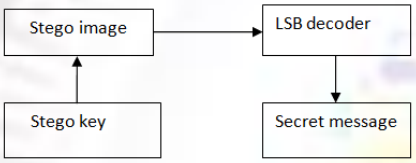

Fig. 3: Shows the mechanism of LSB extraction technique

D. Different type of image file format

1) TIFF

The TIFF (Tagged Image File Format) format is a flexible format that normally saves eight bits or sixteen bits per color (red, green, blue) for 24-bit and 48-bit totals, respectively, usually using either the TIFF or TIF filename extension.

2) BMP

The BMP file format (Windows bitmap) handles graphic files within the Microsoft Windows OS. Typically, BMP files are uncompressed, and therefore large and lossless; their advantage is their simple structure and wide acceptance in Windows programs.

3) PNG

The PNG (Portable Network Graphics) file format was created as a free, open-source alternative to GIF. The PNG file format supports eight-bit paletted images (with optional transparency for all palette colors) and 24-bit truecolor (16 million colors) or 48-bit truecolor with and without alpha channel – while GIF supports only 256 colors and a single transparent color.

IV. MODELING & SIMULATION

A. Evaluation of Different Techniques

All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. The authors propose a set of criteria to further define the imperceptibility of an algorithm. These requirements are as follows:

- Invisibility: The invisibility of a steganographic algorithm is the first and foremost requirement
- Payload capacity: Unlike watermarking, which needs to embed only a small amount of copyright information.
- Robustness against statistical attacks: Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data..
- Robustness against image manipulation: In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information.
- Independent of file format: With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties.
- Unsuspicious files: This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

B. Simulation Parameter

The input image is a cover image of lena 256*256.The image is converted into integer bit 65536*8.The secret message is embedded on cover image. The LSB insertion mechanism is used for generation of stego image. After LSB method a new integer bit is 65536*7.The integer data applied is 65536/8.The integer to bit conversion is 65536/8*8.The channel noise i-e SNR (Signal to Noise ratio) applied to the stego image varies from 1 to 10.The embedding bit are k=1 and k=2.The embedded bit k=1 is used and bit k=2 is used. The insecurity is major threat in transmission of secret data. The LSB insertion and extraction mechanism is involved in both transmission and reception

1) Bit Error Rate (BER)

The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferring bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage.

$$\text{BER} = \frac{\text{No. of bit errors recieved}}{\text{Total number of bits transmitted}}$$

2) Signal-to-Noise Ratio (SNR)

Signal-to-noise ratio is defined as the power ratio between a signal (meaningful information) and the background noise (unwanted signal):

$$SNR = \frac{P_{signal}}{P_{noise}}$$

3) Measure of Image Quality

The effectiveness of the stego process proposed has been studied by estimating the following three metrics.

C. Bit Error Rate (BER) and Bit Error

The BER for the Stego image (Is) is the percentage of bits that have errors relative to the total number of bits considered in Ic. Let I_{cbin} and I_{sbin} are the binary representations of the cover image and stego cover then,

The total number of bit errors,

$$T_e = \sum_{i=1}^{n} |I_{cbin} - I_{sbin}|$$

And the bit error rate BER = Te / T_n

D. Peak Signal to Noise Ratio (PSNR)

The PSNR is calculated using the equation,

$$\text{PSNR} = 10 \log_{10} \left(\frac{I_{max}^2}{MSE}\right) \text{db}$$

Where Imax is the intensity value of each pixel. Higher the values of PSNR better the image quality.

E. Mean Square Error (MSE)

The MSE is calculated by using the equation,

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{i,j} - Y_{i,j}\right)$$

V. RESULT & DISCUSSION

A. Test Images with Different File Format

1) Lena.PNG

Fig. 4: Cover image (Lena.PNG)

[Secret message to be embedded into cover image
Secret message = "Mr. Brajesh Sharma M.Tech (D.C)"]

2) Lena.TIF

Fig. 5: Stego image with Secret message

3) Flower.BMP

Fig. 6: Cover image (Flower.BMP)

[Secret message to be embedded into cover image
Secret message = "Mr. Brajesh Sharma B.E (ECE) CEC"]

4) Flower.TIF

Fig. 7: Stego image with Secret message

VI. CONCLUSION & FUTURE SCOPE

The result shows the embedding of different message in different file format like PNG, TIF, BMP. The cover image is embedded secret message called stego image. The LSB insertion is applied into transmitter part & in the receiver part LSB extraction mechanism is applied. After receiving image we can calculate its BER, PSNR, MSE, SNR. The future scope of this paper is that we can apply this in X-Ray, MRI image.

REFERENCES

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav/Interna-tional Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012, Steganography Using Least Signicant Bit Algorithm.
[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,
[3] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2011
[4] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999
[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, Oct 2014
[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998
[7] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999
[8] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002
[9] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001
[10] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983
[11] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
[12] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996
[13] Handel, T. & Sandford, M., "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, June 1996
[14] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002
[15] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998
[16] "Reference guide: Graphics Technical Options and Decisions"