Data Security Using Image Steganography And Weighing Its Techniques

Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan

Abstract: Steganography is the art of covering secret and confidential information within a carrier which could be an image file, video file or audio file. It is a technique which provides invisible communication since an image file which has the secret information embedded within it is delivered to the receiver instead of the secret information itself. The focus of this paper is to provide immense understanding of the Image Steganography technique – its history, advantages over cryptography, process model and comparison of its techniques.

Index Terms: carrier, cover, embedded, obscurity, Stego-image

1 INTRODUCTION

With the upcoming innovations in technology, there is a demand to provide a technique to deliver secret information over the Internet without it being altered and viewed by the eavesdroppers. Such a technique is Steganography which has been derived from the two Greek words “steganos” meaning covered or hidden and “graphein” which means to write. Thus, it is the practice of hiding private information within another file also known as the carrier. Image file has been popularly used as the carrier because of its accessibility, availability and usability. A Stego-image is obtained after the secret information is embedded within the digital image using an algorithm. All recipients except the desired recipient who receive the Stego-image are unaware of the fact that it has a secret information embedded within it. Thus, this technique has gained its supremacy since it hides the very existence of the secret message i.e. only the sender and the intended receiver suspect the existence of the secret information. It is also known as a form of security through obscurity.

2 HISTORY

The history of Steganography can be traced back from 440 B.C

2.1 Wax Tablets

In ancient Greece, people wrote secret messages on wood and then covered it with Wax. Also, a normal message was written over the wax to cover the secret message.

Fig.1 Wax Tablets

2.2 Shove Heads

This was also used back in ancient Greece. Slave’s heads were shove and secret messages were written on the scalp. Then, the slave’s hair was allowed to grow and the secret message was exposed to the recipient after shaving the head again.

Fig.2 Shove head with the secret message

2.3 Invisible Ink

Secret messages were written using invisible ink which became visible only when the paper carrying the message was heated. Liquids such as milk, vinegar and fruit juices were used as invisible inks. This method was used by the French Resistance during World War II by writing secret messages on the back of couriers using invisible ink.

Fig.3 Invisible ink

- *Pritam Kumari, Chetna Kumar, Preeyanshi, B.Tech (IT), Ansal Institute of Technology, Guru Gobind Singh Indraprastha University, India, E-mail: pritamkumari17@yahoo.com, Chetna.kmr@gmail.com, preeyanshi118@yahoo.com*
- *Jaya Bhushan, Assistant Professor, Ansal University, India, E-mail: jayabhushan@ansaluniversity.edu.in*

2.4 Morse Code

Secret messages were written in Morse code on the knitting yarn. A cloth was made out of the yarn which was worn by the carrier. Also, Jeremiah Denton blinked his eyes in Morse code to spell the word “Torture” in a Television conference. This ensured the US Military that American POWs were tortured in North Vietnam.

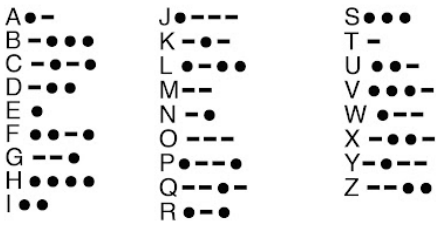

Fig.4 Morse coding for each alphabet

3 Steganography Model

Basic Steganography model consists of secret message, cover message, secret key and embedding algorithm.

3.1 Secret Message

The secret message is information which needs to be hidden into some suitable digital media.

3.2 Cover Message

It is the carrier of message such as image, audio, video or other digital media.

3.3 Stego Key

It is used to embed message depending on the hiding algorithm. Embedding algorithm is the method of embedding the secret message into the cover. The *cover-object* with the secretly embedded message is then called the *Stego-object.* Steganography process basically consists of encoding at the sender end to obtain the Stego-Image and decoding at the receiver end to provide the secret or private information.

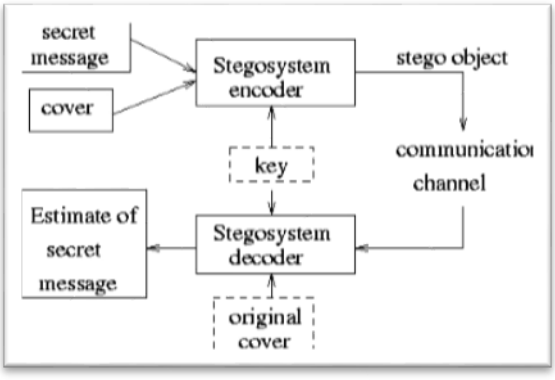

Fig.5 Steganography Encoding and Decoding

- **Encoding**

The secret message can be a text file or a text itself. The cover file in Image Steganography model is Image. The secret text message is initially encrypted using an encryption key. This secret message is embedded within the Image file using a Steganography algorithm. The output obtained from the encoding process is a Stego-Image.

- **Decoding**

The Stego-Image is fed into the decoder which uses a decryption algorithm to provide the original cover and the secret message as output. The secret message obtained here is in encrypted format. Using the decryption key, the original secret message is hence obtained at the receiver end.

4 Steganography vs. Cryptography

Steganography and Cryptography are closely related. The word Cryptography is derived from the Greek word kryptos which means hidden. It is a technique of protecting information by transforming into unreadable format called *cipher text.* Only those who possess a secret key can decrypt or decode the message into *plain text.* Steganography and Cryptography though being data encryption techniques differ in the following terms:

4.1 Invisible Encryption

In case of cryptography, the output is also text. Thus, it is easy for anyone to perceive that secret message has been passed over, making it prone to attacks. On the contrary, the output in Steganography is the media file i.e. Image in this case. Thus, it is difficult for anyone to perceive that a secret message has been sent, making it more secure.

4.2 Modifiability

The encrypted message can be modified easily by anyone in case of Cryptography since it is a text file. The encrypted message is not visible to anyone in Steganography. Thus, it cannot be modified.

4.3 Supported Formats

Cryptography supports text to be converted into cipher text. Steganography supports image file, audio file and video file as carriers.

4.4 End Result

The end result in case of Cryptography is a cipher text while in Steganography, the end result is a Stego- Object i.e. Stego-Image, Audio or Video.

4.5 Goal

The goal of Cryptography is to prevent any interceptor to retrieve the plain text from the cipher text. The goal of Steganography is to prevent any interceptor from even gaining knowledge of the fact that the secret data is present.

5 Steganography Techniques

Image Steganography uses digital images that can be of various formats. The image may be compressed using any of the two techniques which are lossy and lossless compression. Lossy compression creates small files, eliminates excess image data and some data might be lost.

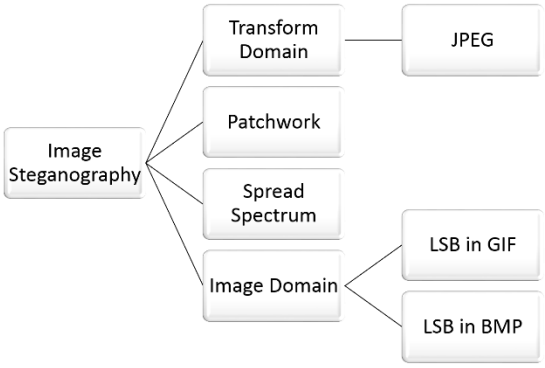

Fig.6 Techniques of Image Steganography

JPEG (Joint Photographic Experts Group) is compressed using this technique. Lossless compression is used in GIF (Graphical Image format) and BMP (Bit Map) image files. It does not remove any data as it uses mathematical formulae to perform the compression.

5.1 Image / Spatial domain

The secret message is embedded in the intensity of pixels directly. Image is compressed using lossless data compression. This steganography technique is dependent on the image format to be used as cover.

5.1.1 LSB

Also known as least significant bit. In this technique, the bits of the secret data are embedded in the least significant bit of certain bytes of the cover image. Secrecy can be implemented by taking secret key into consideration that will specify the bytes that need to be manipulated. It usually considers BMP files as they use lossless data compression.

5.1.2 Palette Based LSB

It uses GIF files as cover images that are basically indexed images which stores colours in a palette or lookup table. The colours in a palette are arranged as per their usage. When LSB is applied, the palette changes that causes tremendous changes in colour values. The remedy to this is to sort the palette so that the colour differences are minimised. Another remedy is to add new colours similar to the existing colours of the palette. Instead, Greyscale images can be used as they have 256 shades of grey.

5.2 Transform / Frequency domain

The cover images are first transformed and then the secret message is embedded in significant areas of the cover image. This steganography technique is independent on the image format to be used as cover.

5.2.1 JPEG Steganography

RGB value is converted to YUV value where Y indicates brightness and UV indicates colour. Since human eye is sensitive to brightness, we down sample colour to reduce the file size. Transformation of image is performed using DCT or DFT that spreads the location of pixel values over image parts. Quantisation reduces the strength of high frequencies and all values are divided in a block by quantisation coefficient. The resulting integer values are rounded off. In JPEG steganography, during the transformation phase, rounding errors occur that are not noticeable. DCT and quantisation is lossy and Huffman is lossless. So steganography takes place between these two stages i.e. LSB occurs before Huffman encoding. This is advantageous as it is difficult to detect since it is not in visual domain.

5.3 Spread Spectrum

The secret data is considered as a set of narrowband signal frequencies that are spread over a wideband of frequencies i.e. white noise. The secret data is hidden in noise, combined with the cover image to obtain the Stego-Image. The power of the embedded signal is very low as compared to the power of the cover image, so the secret is imperceptible to the human eye.

5.4 Patchwork

It uses redundant pattern encoding to embed the secret data in the cover image. Redundancy is added to the secret data, then the bits are scattered throughout the cover image. Consider two patches of image: Patch A whose pixels are lightened and Patch B whose pixels are darkened by the same constant value. The drawback of this technique is that it encodes only one bit. More bits can be embedded by dividing the image into sub images. The advantage of this technique is that if one patch is destroyed, other are still left. So, data is not lost.

6 Conclusion

This paper presented the research work in the field of image steganography describing its history in brief, the encoding and decoding process of steganography model, advantages of Steganography over Cryptography and the comparison between its techniques.

Acknowledgment

We would like to present immense gratitude to our mentor Ms. Jaya Bhushan for giving her advice about this topic. We would like to thank her for guiding us along each step of this research work. Also, we would like to thank her for supporting us throughout.

Parameters	LSB in BMP	LSB in GIF	JPEG Compression	Patch work	Spread Spectrum
Invisibility	High	Medium	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Unsuspicious files	Low	Low	High	High	High
Independent of file format	Low	Low	Low	High	High

Table. 1 Comparison of Image Steganography algorithms

REFERENCES

[1] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008

[2] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108

[3] Y.K.Lee and L.H.Chen "High capacity image steganographic model"

[4] Atallah M. Al-Shatnawi "A New Method in Image Steganography with Improved Image Quality," in Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[5] Khalil Challita and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions," in International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208 The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085)

[6] Rosanne English," Comparison of High Capacity Steganography Techniques"

[7] S Usha, G A Sathish Kumar, K Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography" in 2011 International Conference on Computer Science and Network Technology

[8] Arvind Kumar and Km. Pooja, "Steganography- A Data Hiding Technique" in International Journal of Computer Applications (0975 – 8887)

[9] Kevin Curran and Karen Bailey, "An Evaluation of Image Based Steganography Methods," in International Journal of Digital Evidence, Fall 2003, Volume 2, Issue 2

[10] Kanzariya Nitin K. and Nimavat Ashish V., "Comparison of Various Images Steganography Techniques" in International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013, ISSN 2278-733X

[11] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, "Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography," in The 18th International Conference on Pattern Recognition (ICPR'06) 0-7695-2521-0/06 $20.00 © 2006

[12] Alaa A. Jabbar Altaay, Shahrin bin Sahib, Mazdak Zamani, "An Introduction to Image Steganography Techniques," in 2012 International Conference on Advanced Computer Science Applications and Technologies

[13] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images," in Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, 2012, DESIDOC

[14] A. Joseph Raphael and Dr. V. Sundaram, "Cryptography and Steganography – A Survey," in Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630 ISSN: 2229-6093

[15] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview," in International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012

[16] Namita Tiwari and Dr.Madhu Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format," in International Journal of Computer Applications (0975 – 8887) Volume 6– No.2, September 2010