Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.166 – 169

RESEARCH ARTICLE

Image Steganography Approach

Ghania Al Sadi

[1] Computing Department, Sohar University, Oman

ghanialsadi@gmail.com

Abstract— Steganography is a technique used to embed and hide secret data into another type of data for security purposes. A number of steganographic methods are used to hide secret data in different type of objects. This research discussed steganography approach and illustrates LSB insertion as a steganographic method to hide secret data in image files.

Keywords— Steganography, Steganalysis, LSB, JPEG, Hide

I. INTRODUCTION

Steganography is one type of data security techniques that is used to protect data from being detectable by unauthorized actions during transmission over public communications. Referring to security techniques, both cryptography and steganography are techniques used to secure data while transferred over network from illegal actions and thus secure communication between the communicated parties. However, both techniques have different concepts in term of securing data. Cryptography is used to secure the contents of the message during transmission while steganography is used to hide data of the message to be undetectable. Technically, both steganography and cryptography can be used together to ensure high level of security applied to data during transmission. On the other hand, another term is introduced in this term which is Steganalysis. Steganalysis is the reverse meaning of steganography. It is an art of investigating and analysing suspected objects to discover and extract any hidden data embedded inside transmitted objects.

Originally, steganography is driven from a Greek word “Stego” that means “cover” or “cover writing” (Das and Kushwaha 2015). Steganography is an old practice used to hide messages during transmissions using different carriers or cover media. Over years, steganography has been evolved to accommodate the digital world by developing advanced and sophisticated methods to hide digital data during transmission over network. However, the idea and principle of steganography still unchanged. Typically, the new steganography technique utilizes digital objects like digital files or network protocols as a cover media to embed secret data. The modern technique of steganography enable hiding digital data inside a cover-media like image, audio or video files that are used in daily exchange actions where hidden data are not easily detectable. Using this technique, a large amount of data can be hidden inside files with different file format where the change is not noticeable in the file contents (Bhavana and Sudha). Selecting a proper media to hide data inside is mandatory to keep data undetectable by attackers. Generally, the size of media that contain secret data is one factor of easy detection of these secret data. Whenever the size of media is increased, the possibility of detection increases. Therefore, steganography system usually is based on hiding data in fixed-size media.

II. STEGANOGRAPHY FRAMEWORK

Basically, digital steganography is distributed among three types which are pure, symmetric and asymmetric. Symmetric and asymmetric steganography are used when encryption is applied in term of securing data during transmission where a secret key (stego-key) is required to be exchanged before sending data. On the other hand, pure steganography requires no key to be exchanged. When both cryptographic and steganography techniques are combined to protect data, a high level of security will be provided. The data will be doubly secured, by encrypting message prior to hide it into a cover media(Ali et al. 2008) .

Mainly, Steganography technique is composed of cover media that is used to hide data inside and secret data that is referred to data or message to be hidden inside the cover media. The combination of the cover media and secret data is referred to as Stego-media. It can be identified as the result of steganography. Along with these components, Stego-key may be used when data is encrypted using cryptography techniques before concealing data by stenographic techniques. As illustrated in Figure 1, same stego-key must be used by the receiver of the message to conduct steganalysis process to extract the embedded secret data from the stego-media.

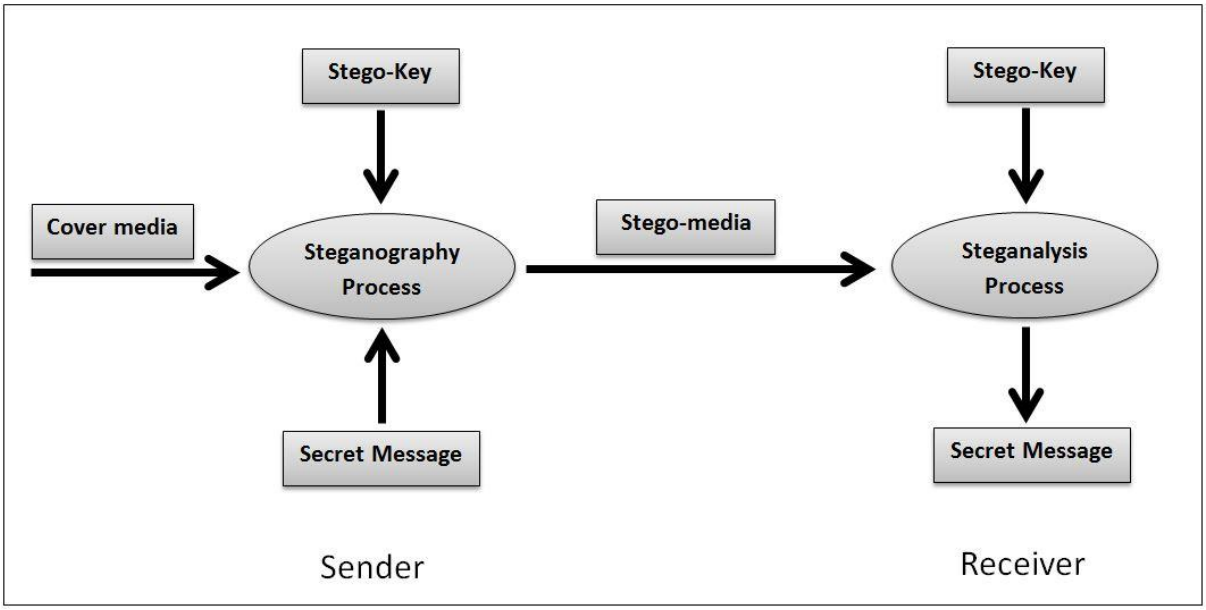

Fig 1: Steganography Scheme

Figure 1 shows the process of embedding secret message into cover media by steganography process using the stego-key to produce stego-media. Stego-media is then sent to the intended destination. The receiver requires the stego-key that is used in steganography process in order to extract the secret message from stego-media during steganalysis process. During steganography process, user must ensure that stego-media look identical to the cover media.

III. LEAST SIGNIFICANT BIT (LSB) INSERTION

Least Significant Bit (LSB) insertion is a simple and primary method of steganography that is used to hide data into any type of media like image, video and audio. Mostly, LSB insertion is applied to hide data inside an image because it is considered as more safe and attractive. It is based on replacing least significant bits (LSB) of pixel colours in the cover image by bits of the hidden message data. Least significant bit (LSB) can be defined as the last bit in each binary number that is located at the right side of each binary number. The change of the last bit has less effect on the original binary value of the cover image. Usually one bit can be hidden in one byte in the cover image (Ali et al. 2008). LSB insertion technique can use 8-bit image type or 24-bit image type to hide data where each type has its strengths and weaknesses. 8-bit image has a small size with less number of colours that is 256 colours only where each pixel represented by one byte only. Embedding data in this type of image will be more detectable while the change of the image will be obvious. However, gray colour is more used with 8-bit image where the gradual change in the colour will be less detectable when embedding data inside the image. On the other hand, 24-bit image is more desirable by steganography technique because it has a large number of colours that allow for more data to be hidden inside the image. In 24-bit images format, three bytes represent each pixel colour where each pixel has three bytes of data to represent RGB (the three basic colours Red, Green, Blue) values. Therefore, each pixel can represent (256x256x256) different colours while

one byte represents 256 colours. This is considered as a large number that enable steganography to hide amount of data in this type of images.

LSB insertion technique changes the LSB for each colour where each pixel has three RGB colour. Depending on this base, hiding a message inside a 24-bit image requires three bits to be hidden in every pixel. This means that one bit can be stored or hidden in one byte. For example to hide any letter in a 24-bit image, three pixels will be used to hide one letter as illustrated in Figure 2.

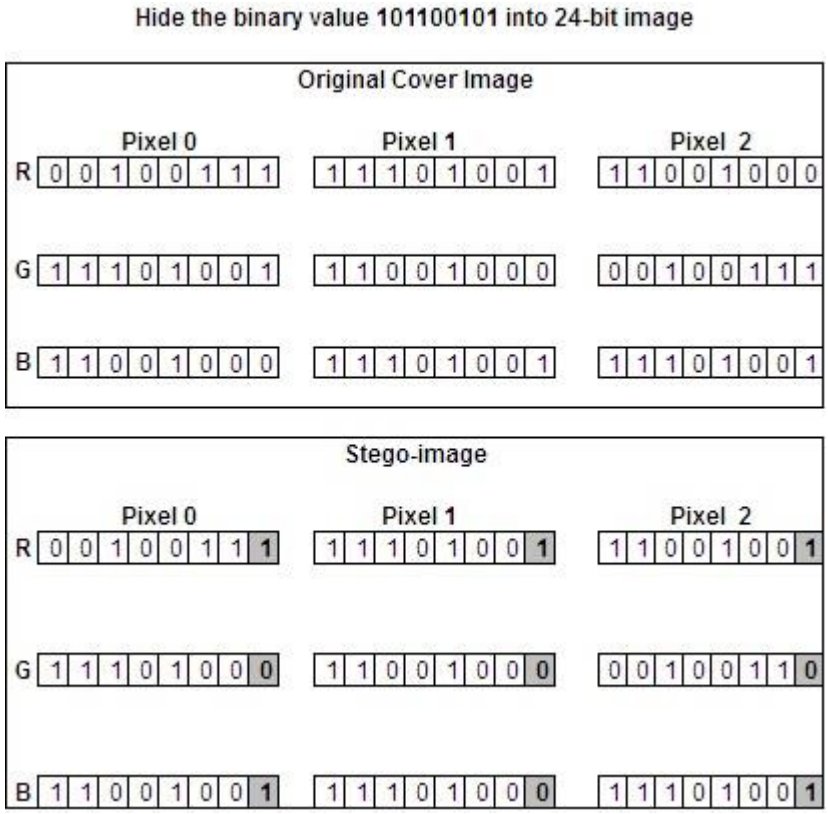

Fig 2: hiding data in 24-bit image using LSB

In fact hiding three bits in each pixel will not affect the view of the image especially in large images. So, large image that use 24-bit colour are more attractive to be used by steganography due to the large number of colours used in this type of images where we can hide large amount of data without aware of being detectable by attackers or man in middle. One the other hand, by using 8-bit image format, only one bit can be hidden in one pixel whereas each pixel is represented by one byte only. This type of format limits the size of secret data that can be embedded in cover images where the high size of embedded data will rise the ability to detect these embedded data by attackers.

The common image format used by LSB insertion to hide data is JPEG image format. It makes use of Discrete Cosine Transformer (DCT) to be applied for image content transformation. Some steganography tools hide data in LSBs of the quantized DCT coefficient. JPEG format is more preferred to be used as a cover image due to its high usage over the internet or even locally by users. Also, it is desirable because of its high quality with high ability of maintenance. Moreover, it provides large ratio of compression (Sachdeva and Kumar 2011). Stego-image with JPEG format is less suspected to have hidden data, so it is less detectable by visual attacks. Visual attacks referred to the technique of seeking for hidden data on the low bit planes of the image by overwriting visual structure(Provos and Honeyman 2003).

High amount of data can be hidden in JPEG format. The maximum number of bits that can be hidden in a cover image is referred to as steganographic capacity where the size of the hidden data is relative to the size of the Stego-image. Based on steganography goal, high steganographic capacity is required with less detection but both are going in reverse way. High amount of hidden data in one cover image means more change will be applied while more artifacts will be introduced in Stego-image. Thus it will be more detectable by attacks regardless of the image size (Sachdeva and Kumar 2011). However, JPEG images still has the ability to store high amount of secret data without affecting its view. Figure 3 shows two JPEG used in steganography process

to embed secret data. The first image is the original image that is used as a cover image to embed secret data. The second image is the stego-image that contains the embedded data. As illustrated embedding data inside the image didn't affect the image where both image looks identical to each other. Thus it is not suspected that it contains some hidden data.

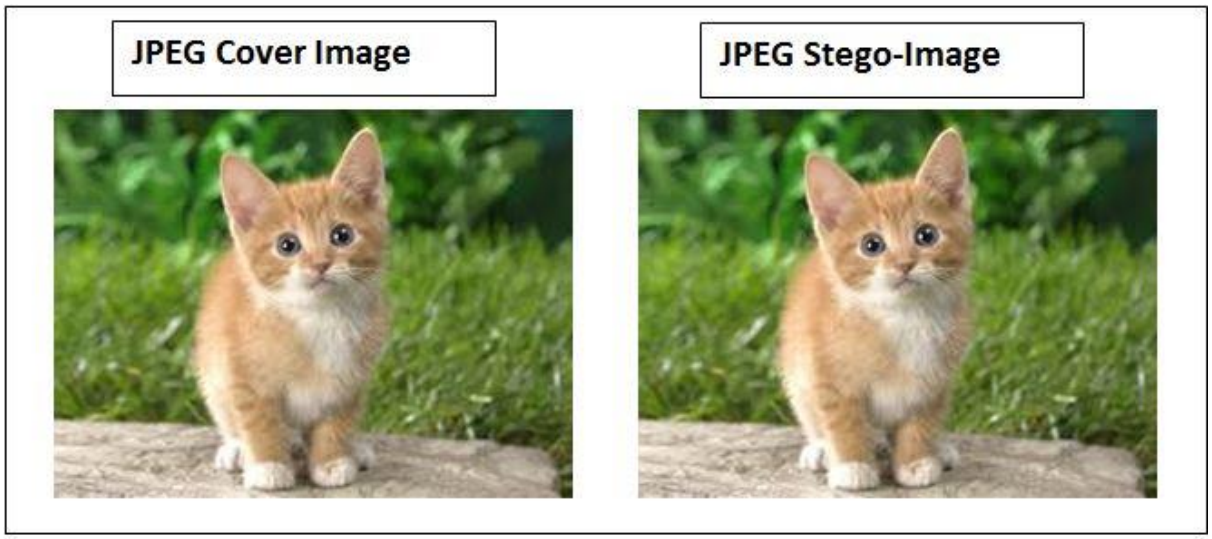

Fig 3: Hiding secret data in JPEG image

IV. CONCLUSION

Modern steganography technique is a powerful system used to secure secret data while transmission over network. This research introduced image steganography to hide data using LSB insertion method. As mentioned, JPEG image format has more ability to embed secret data inside without affecting the original view of the image where both cover image and stego-image look identical to each other that make it unsuspected by attackers during transmission. The next research will take LSB into practice using different type of images to hide secret data and measure the steganographic capacity in each image.

REFERENCES

[1] Ali M, Younes B, Jantan A. A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion. Int J Comput Sci Netw Secur. 2008;8(6):2–9.
[2] Bhavana S, Sudha KL. T Ext S Teganography Using Lsb Insertion.
[3] Das P, Kushwaha SC. MULTIPLE EMBEDDING SECRET KEY IMAGE STEGANOGRAPHY USING LSB SUBSTITUTION AND ARNOLD TRANSFORM. 2015;(Icecs):845–9.
[4] Provos N, Honeyman P. Hide and seek: An introduction to steganography. IEEE Secur Priv. 2003;1(3):32–44.
[5] Sachdeva S, Kumar A. Colour image steganography based on modified quantization table. Proc - 2012 2nd Int Conf Adv Comput Commun Technol ACCT 2012. 2011;309–13.

