Abstract

Background/Objectives: The goal of image steganography is to maintain communication between both parties without any intrusion from other parties. Image steganography is to embed a message into the cover image which is used as a carrier for embedding (messages) and produce stego-images (images that carry hidden messages). Method/Statistical analysis: It aims to provide an overview of image steganography, how to hide the secret message behind the image and analyze the perceptual quality of the stego image by using the method of least significant bit (LSB) algorithm. Findings: The result will report the Own-Develop Stegano application and the analysis of perceptual quality images by using the application. Discussion will discuss about the usability of this study. Application/Improvements: Conclusion and recommendation will suggest an enhancement to this application.

Keywords: Decryption, Hiding, Information, LSB, Own-Develop, Steganography

1. Introduction

In information security, Steganography and Cryptography are different where the cryptographic focus to keep secret the message content. Whereby, steganography focus to maintain the existence of secret messages with the art or science of hiding information or facts which communication occurs by concealing information in other information. Steganography is the art of communication that cannot be seen. Steganography is a method for hiding confidential information in any type of media. Steganography is also to cover information in a one-piece again. Generally, steganography is known as “invisible” or hide the existence of information in a medium such as video, audio, image or text.

Image is an object of protection which used by steganography. In digital images, various image file formats exist. Image file format can store data in compressed, uncompressed or vector format. After rasterize, the image will be a grid of pixels. There are various types of image file format that commonly used including JPEG, GIF, PNG, BMP and TIFF.

Generally, the pixel intensity techniques are used for hidden information in image steganography. It proves the images of grayscale is more suitable than color images for image steganography where interference between the various components can reveal essential trace. The domain image steganography categorized into two domains. The transform domain is images that first transformed, and then the message is embedded in the image. Domain images unused bit insertion and manipulation of the sound image that is protected. Its methods embed messages directly in the pixel intensity. For computers, it proved that image is a collection of numbers that form different light intensities in different places. Most of the pictures in the Internet contain a map of rectangular pixel (bit), which located at each pixel and its color.

This study is to develop steganography applications by using Least Significant Bit (LSB) algorithm. A perceptual
quality between cover-image and resulting stego-image will be analyzed using the application.

2. Purpose/Motivation/Problem Statement of the Study

The message may be exposed to the third parties when users send messages or any files to the destination. This situation makes the message easily be stolen by a third party during the transmission of messages. The purposes of this project are to produce new image steganography software to hide messages by using LSB technique, to analyze the quality and speed of image technique in this steganography application.

3. Method and Material

There are several algorithms for concealing information or messages, including embedding messages by using LSB. The LSB embedding algorithm is an approach that replaces every little bit of data to the message directly. The LSB is a technique in encrypting and decrypting secret information by converting redundant bit less important to the bit-nit confidential information. LSB will convey secret information to the recipient without being noticed by intruders. LSB algorithms have become the basis for many techniques to hide messages in multimedia data, and the value of the LSB is invisible to the human eye. The Least Significant Bit (LSB) substitution method is the simplest and well-known image steganographic method.

By using LSB make it divide into three important sections as shown in Figure 1 a. Encryption with LSB algorithm is used to help build better security of steganography application. b. Steganography with image categories as a carrier for data transmission and by using the “LSB algorithm”, which the messages will be put into bit pixel image. c. The decryption process is when the recipient wants to decrypt the data of the images by using the “LSB algorithm” for extracting data from an image by taking passwords as a reference.

There are three modules involved in this application. There are encryption module, data transmission module and decryption module. In encryption module, the message will be behind the cover-image of the original image file that is used as a carrier of a hidden message. The cover-image file that will be embedded by the method used, then a stego-image. Then, in a data transmission module, the stego-image is sent to a third party in which the third party does not know that the stego-image has a hidden message.

After receiver receives the stego-image, whereas it is in decryption module. A hidden message can only be extracted by using the stego-key (extracting algorithm) at the receiver end. To know the message, the receiver must enter the password and username which are the same as the sender. The process flow of this application by using the three modules is shown in Figure 2.

3.1 Encryption Module

The encryption module of steganography is the primary stage. In this stage, the sender sends the data as well as the image file which act as a carrier image to transfer the data to the destination. In this encryption module, text messages B will be embedded into the original image of A. The embedding process is done by using the method of LSB algorithm. Excess LSB (Least Significant Bit) algorithm is easy to understand, to implement, and data hidden in the stego-image appears to be highly visual fidelity. The LSB algorithm uses the LSBs of each pixel and replace with the significant bits of the text document, where the message will be encrypted into the image. This process makes the picture will not lose its resolution.
3.2 Data Transmission Module

The encrypted data is sent to the recipient or an authorized person with the help of transmission media such as emails. An image in which data is embedded acts as a carrier file, where data can be transmitted easily with high security. LSB algorithm will put the message into bits. It can be embedded properly in the place of LSBs of the image, where the image does not lose its resolution. So, the security will be high. The encrypted image is protected with a password, so it can avoid the damages which caused due to hackers or unauthorized persons.

3.3 Decryption Module

In the decryption module, the receiver receives the carrier image from sender through the transmission medium. The receiver then sends the image carrier to the decryption phase. In the decryption phase, the same LSB algorithm is implemented for decrypting the LSBs from the image to frame the original message bits. After successful arrangement, the file is decrypted from the carrier file and accessed as an original text document.

4. Results and Analysis

Stegano application by using LSB algorithm has been successfully developed as shown in Figure 3. Both sender and receiver must have this application to embed their message behind the image.

Data transmission or secret messages through e-mail have been tested by using this application, where senders need to choose any image. After the image has been embedded with secret messages, the sender will send images to a receiver that has been buried with a password that both sides know it. Third parties will not be able to open the image as long as the individual does not know the password. Receivers will decrypt the image to receive the message. From the perception quality analysis, it shows that the stego-images which produced by LSB technique is nothing difference if we see with naked eyes. An example, it can be tested by an image with a size of 380 x 400 as shown in Figure 4.

From the analysis, the results showed that the visual quality is same with a nothing difference if it be seen by the
Perceptual Quality Analysis using Own-Develop Image Stegano Application

naked eye. In either the colour or the distortions obtained from data embedding are hardly noticeable between the original cover-images and resulting stego-images. In another way, the difference can be spotted after analyzing the byte by using the hex editor application.

XVI32 is a freeware hex editor which running under Windows 9x/NT/2000/XP/Vista/7. Hex editing can be accomplished via a number of advanced text tools, which allow for altering and manipulating the binary data and defines the files. With the hex editor, it is able to view, inspect and modify the raw contents of any type of file in hexadecimal format. XVI32 fits the job perfectly, where it can deal with very large files, has a built-in data inspector and an efficient script interpreter for automating tasks.

Figures 5 and 6 show the size of the original image and stego image. The image at the top is an unaltered, with 109 KB image. Below it is the same image with a 110 KB scattered throughout its pixels. Through the naked eye, there is no difference in the two photos. It is not surprising as only the LSBs were altered. With each pixel is being represented by three color values namely red, blue and green, each of those colors ranging in values from 0 to 255 (1 byte each). A change in the LSB of each has virtually no effect from a visual standpoint. By using LSB scheme, it can hide a bit of each byte which is equivalent to three bits per pixel. In naked eye might not provide much, but if any clues, a direct comparison of image files may be found. Figure 7 shows the difference of hex representations of an image before and after modification.

As seen in Figure 7, by using this Hex-editor, it found that the first 89 bytes of each file are identical. This is the nature of a bitmap file to reserve the first 89 bytes of header information. This is obviously much more complex than a plain original image, which much more difficult to absorb. But, it is clearly that beyond the first 89 bytes, the rest of the file has clearly been changed.
5. Discussion

As seen with the naked eye, not much change in visual perception of image quality for detecting changes in the image quality. However, when it viewed each image by pixel bytes, it has the difference or changed after encryption. Higher sophisticated software certainly can identify more information than this simple algorithm.

While this program uses a simple and common scheme of using every LSB until the file has been completely embedded, another approach can be used to scatter the bits evenly throughout the file. An analysis such as this is still a valuable way of identifying the possibility of steganography.

6. Conclusion and Recommendations

LSB steganography which based on conventional techniques is capable of hiding a big secret enemy in the cover image without introducing any distortion of perception. This work can also be extended to include various types of media such as audio and video. It can also be tested using various sizes of files to compare the quality of the original image and encrypted image.

7. References

1. Poornima R, Iswarya RJ. An overview of Digital Image Steganography. International Journal of Computer Science and Engineering Survey. 2013; 4(1):23–31.
2. Channali S, Jadhav A. Steganography an Art of hiding Data. International Journal on Computer Science and Engineering. 2009; 1(3):137–41.
3. Li B, He J, Huang J, Shi YQ. A survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing. 2010; 2(2): 142–72.
4. Poornima R, Iswarya RJ. An overview of Digital Image Steganography. International Journal of Computer Science and Engineering Survey. 2013; 4(1):23–31.
5. Rameshkumar P, Monisha M, Santhi B. Enhancement of Information hiding in Audio Signals with efficient LSB based Methods. Indian Journal of Science and Technology. 2014; 7(5):80–85.
6. Lee YK, Bell G, Huang SY, Wang RZ, Shyu SJ. An advanced least-significant-bit Embedding scheme for Steganographic Encoding. Ed: Toshikazu W, Fay H, Stephen L, Advances in Image and Video Technology. Springer: Berlin Heidelberg; 2009.
7. Ramalingam M, Isa NA. A Steganography Approach over Video Images to Improve Security. Indian Journal of Science and Technology. 2015; 8(1):79–86.