Steganography: DCT Coefficients Reparation Technique in JPEG Image

Chiew Kang Leng, Jane Labadin, Sarah Flora Samson Juan
FCSIT, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, MALAYSIA
klchiew@fit.unimas.my, ljane@fit.unimas.my, sjsflora @fit.unimas.my

Abstract

Due to the ever-growing usage of the computer, it has led to a rapid increment in the data that is being exchanged, published and stored in an assortment of digital form. This phenomenon has urged an active participation in the research area of the security domain. One of the main areas of this security domain in providing confidentiality, authentication and data integrity is steganography. This paper proposes a steganography technique for hiding information in images through reparation technique in frequency domain. The purpose of reparation is to correct any static deviation from the cover image after embedding hidden message. The proposed technique is able to withstand visual attacks and statistical attacks. Thus, it can be used to strengthen the security of a steganography system. The proposed technique will be tested by using chi-square steganalysis.

Keywords

Steganography, steganalysis, discrete cosine transform, image histogram, Chi-square

1. Introduction

The technique of hiding some data inside another cover media is known as steganography. The chosen cover media should be an innocuous-looking media to avoid arousing suspicion. The outcome of the steganographic system is a stego media which is perceptually indiscernible compare to the cover media, but with embedded hidden data.

Steganography is not something new; it can be traced back to 440BC where a message was tattooed on a shaved head of a slave. After the hair had grown back, the message was hidden [7]. The cover media used was the head of the slave. However, in modern steganography, digital media is used as the cover media. Most of the cover media is from multimedia file such as image, audio and video file. Some other types like ASCII file, html and pdf files are also used. However, due to the nature of their inner file structure, they are not popular choice as cover media. Whereas JPEG file is one of the most preferred file type used in steganography [4]. There are also some other steganography techniques that use file system in a hardisk drive as a cover media, but it is beyond the scope of this paper.

This paper proposes a new technique to increase the stealthiness of steganography by indemnifying the changes caused during the embedding process. This indemnification is done by incorporating reparation technique. With this, the statistically perceptible artifacts can be reduced to a minimum level. The technique discussed in this paper is applied on a frequency domain cover media which is the JPEG file; however, in general it should be applicable to other domain as well.

In the next section, a background study on the current steganography will be discussed. After that, some methods used to detect the existence of steganography which is known as steganalysis will be highlighted in section 3. Before moving to the main contribution of this paper, the fundamental of baseline JPEG compression is given in section 4 to provide certain level of understanding in the frequency domain. In section 5, the detail of the reparation technique is elaborated and followed by the analysis of the proposed technique in section 6. Finally, the paper is concluded in the last section with some discussion for future directions.

2. Review on steganography

The diagram shown in Figure 1 below is the general model for a steganography system. Cover media is the media used to embed or hide the message. The message in Figure 1 is the content or information that is intended to be hidden. It can be an ordinary text