

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

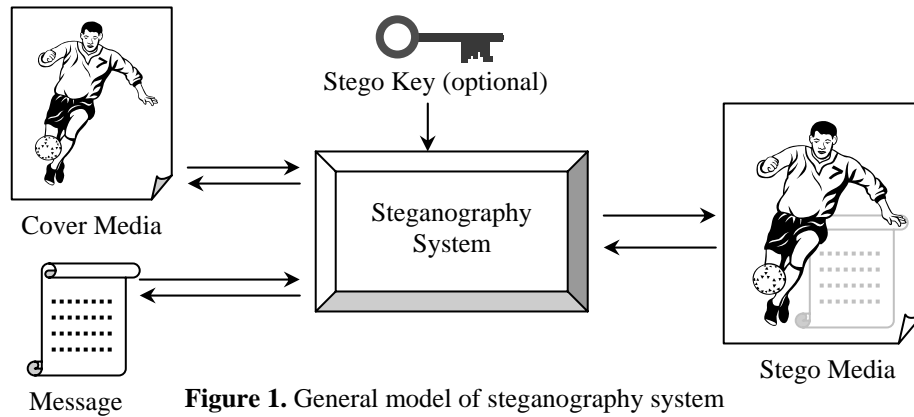
file such as image, audio and video file. Some other types like ASCII file, html and pdf files are also used. However, due to the nature of their inner file structure, they are not popular choice as cover media. Whereas JPEG file is one of the most preferred file type used in steganography [4]. There 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



message, an image or any digital media. The stego key is an optional parameter used to increase the security of this covert communication. The cover media, message and stego key will be the input to the steganography system. The steganography system will embed and hide the message inside the cover media and the outcome of this system is a stego media. As for an authorized person who wants to retrieve the hidden message from the stego media, the process is in reverse order of the processes described above. If stego key is used during the steganography process, then in order to retrieve the hidden message, the stego key should be given to the steganography system as well.

As stated in [9], the application of steganographic technique can be broadly classified as operating in two different domains, such as spatial domain and frequency domain. In spatial domain, the embedding and hiding process is mostly carried out by bitwise manipulation. For example, manipulating the least significant bit (LSB) in one of the colour components in an image. While, the frequency domain includes those that involve manipulation of transformed image such as discrete cosine transformation (DCT) and wavelet transformation. Such manipulation includes changing the value of the quantized DCT coefficients.

The simplest form of steganography is to embed the message into the cover media with the simple algorithm such as embedding in the header of the image or after the End of Image marker. Such system that employed this method can be found in [6], but this method provides a poor and weak steganography system.

In [8], the author suggested permuting the colour palette of the image instead of the image data. This process can hide the message without changing the appearance of the image. This will lead to a randomized palette which is rarely happened in a palette-based image. Since the number of the colour

palette is limited, so the steganographic capacity is rather limited [2].

In F5 [10], the steganography is implemented by a password-driven permutation that scatter around in the image. After that, matrix encoding is used to provide a minimal embedding changes. With these techniques, F5 can provide high steganographic capacity while still can withstand visual attacks and resistant to chi square attack. However, F5 was broken by Fridrich et al. [8] who managed to find distinguish statistical quantities that correlate with the number of modified coefficients, and obtained the baseline values of the statistical quantities which can consequently be able to estimate the size of an embedded message.

3. Review on steganalysis

Steganalysis is an attempt of discovering hidden data in stego media. A poor steganography technique will arise suspicion by doing visual observation. Whereas other steganography techniques may only be detected through some statistical testing. Some better steganography techniques may be able to withstand either visual or statistical detection. If there exist a method that can detect the existence of a hidden message with success rate better than random guessing, then the steganography system is considered broken [8]. Most of the embedding process in the steganography system is using the bits manipulating either in sequential or in some pseudo-random pattern. By enhancing the 1 bit-plane and observing this bit-plane, some suspicious artifacts will reveal the effect from steganographic process. In most of the cases, the 1 bit-plane is the LSB bit-plan and if the LSB is 1 then it is enhanced to the maximum pixel value otherwise if it is 0 then it is remained 0. This is the simplest steganalysis and known as visual attacks [3]. This steganalysis is applicable to detect LSB embedding in

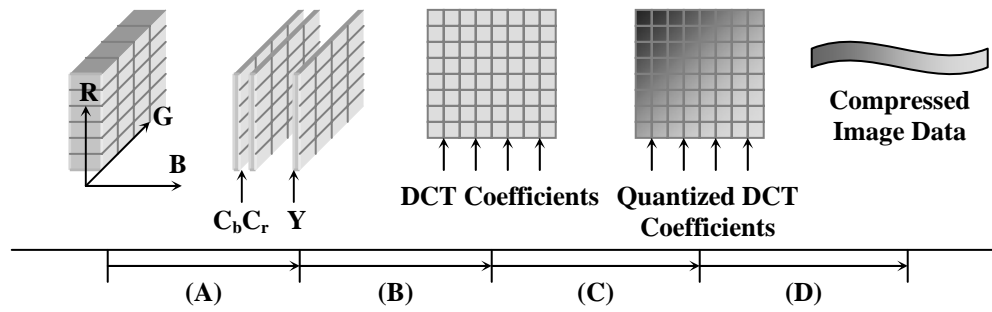


Figure 2. JPEG compression

spatial domain image and palette images, but not in transform domain image. A statistical analysis proposed by Pfitzner and Westfeld [11] is Pair of Values (PoVs). The idea of this steganalysis is that during the embedding, it is actually swapping one value, $A(2i)$ into another value, $B(2i+1)$ and vice versa. This does not change the sum of both values of occurrences in the image. Thus, this will form a pair of values and it is observed that before the embedding, these two values are distributed unevenly, but after the embedding, these values tend to become equal. As a result, statistical Chi-square test is a suitable tool to be used.

Fridrich et al. [3] introduced a method known as RS steganalysis. This method uses statistics derived from the spatial domain of an image. According to them, the LSB can be predicted up to certain level from the remaining of the 7 bits.

Apart from those steganalysis methods described above, there are also some other methods like universal blind steganalysis and unique fingerprints that can be found in [5]. There is also some steganalysis method that only attacks on a specific steganography system like the one proposed in [4] and known as targeted

steganalysis which needed further adjustment to be used as a general steganalysis tool.

4. Baseline JPEG compression

Since the proposed technique is applied on DCT coefficient of JPEG file, it is worthwhile to mention the baseline JPEG compression technique in this paper. The compression process is illustrated in Figure 2.

The first process (A) is a colour space conversion process from RGB components to $YCbCr$ components. Each component is subdivided into 8×8 pixels non-overlapping blocks. Later, in process (B) the 8×8 blocks are then transformed by using discrete cosine transform (DCT) as defined in Equation (1) into 64 DCT coefficients.

The next process (C) is to quantize the transformed DCT coefficients. This can be done by using element-wise division and rounding the result as in Equation (2).

Finally, in process (D), the compressed image data is produced after the zig-zag ordering and entropy encoding (Huffman coding) process. For the decompression process, it is the reverse order of the

$$F(u, v) = \frac{1}{4} C(u)C(v) \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (1)$$

where $x = y = u = v = 0, 1, \dots, 7$, $f(x, y)$ is the particular pixel colour space

$$\text{component and } C(k) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$$

$$F'(u, v) = \text{Round}\left(\frac{F(u, v)}{Q(u, v)}\right) \quad (2)$$

where $Q(u, v)$ is the indices from either the luminance or chrominance quantization matrix

processes discussed above. Refer to [1] for detailed description of the JPEG compression.

5. Reparation technique in steganography

After acquired sufficient understanding of the JPEG compression, this paper utilized the advantages in the frequency domain image which is manipulating the quantized DCT coefficients. The main contribution of this paper is the reparation technique used on the quantized DCT coefficients.

Since JPEG coefficients are grouped in blocks of 8 x 8 coefficients as shown in Figure 3, so the reparation technique explained below will be based on this organization. The proposed technique will use the Alternating Current (AC) of the quantized DCT coefficients for the embedding process.

During the embedding process, the message bits will be embedded to the LSB of the selected DCT coefficient. This will yield 3 possibilities on the changes as shown in Figure 4, namely an increment to the absolute value of the even DCT coefficient, a decrement to the absolute value of the odd DCT coefficient or the absolute value of the DCT coefficient is remained unchanged.

For the embedding that happened to be either possibility 1 or possibility 2 as shown in Figure 4, reparation technique is employed. In reparation process, before a particular DCT coefficient is embedded with message bit, the initial value and the altered value of this coefficient is stored and used as the criteria for the reparation. The following DCT coefficients are searched for a match to the altered coefficient value. If it is found, then these two DCT coefficients are swapped.

For instance, assume AC_{01} in Figure 3 is an odd value of 5 and is intended to be embedded with the message bit 0, hence its value will be decremented to 4. So, assume that after the search, AC_{07} is found to have the value of 4, then this two coefficients will be swapped.

If there is no exact match then the closest DCT coefficient value will be used. The closest value defined here is referred to the LSB of a DCT coefficient, which will only differentiate to either even or odd value. Therefore the closest value should be the same type (even or odd) as the altered coefficient value.

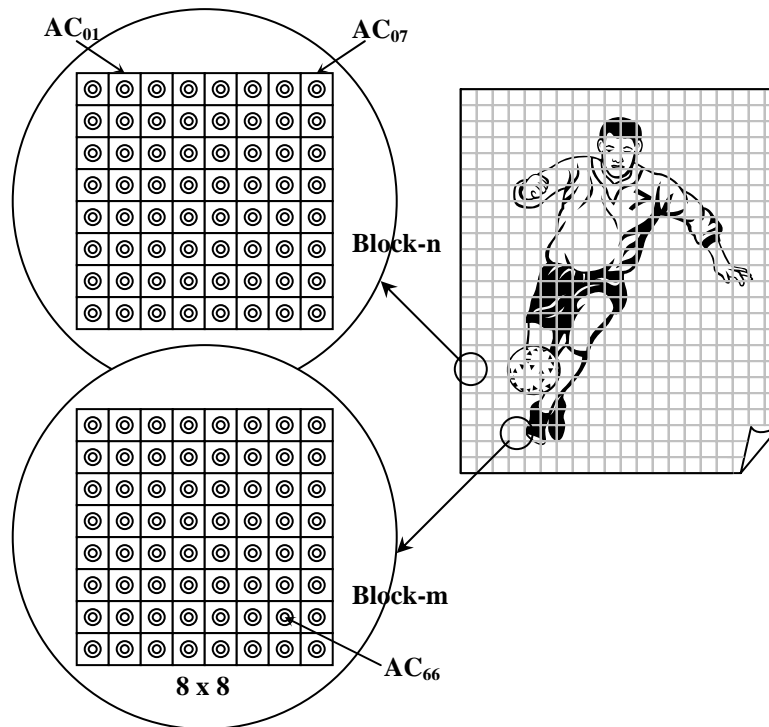


Figure 3. 8 x 8 blocks of JPEG image

$x = \text{abs}(-6)$,
 $y = \text{abs}(5)$, where -6 and 5 is the AC of DCT coefficient
 $LSB_x = 0$
 $LSB_y = 1$
 $MB_1 = 1$
 $MB_0 = 0$, where MB_1 and MB_0 is message bits of 1 and 0 respectively
 \oplus is the embedding operation

$LSB_x \oplus MB_1 = \text{increment on } x$ possibility 1
 $LSB_y \oplus MB_0 = \text{decrement on } y$ possibility 2
 $LSB_x \oplus MB_0 = x$ } possibility 3
 $LSB_y \oplus MB_1 = y$ }

Figure 4. Embedding possibilities

Finally, if the embedding falls in *possibility 3* then reparation process can be ignored. This is because the embedding process does not alter the LSB of that DCT coefficient.

6. Analysis of the proposed technique

The advantage of using frequency domain image like JPEG in steganography is that, the alteration of the content of the image will not easily cause visual artifacts that arise suspicion as compared to spatial domain image. However, it may not be able to withstand statistical attack. Therefore, embedding message to an image may still cause statistically different in the frequency of the image. This can be clearly noticed in the histograms of JPEG coefficient illustrated in Figure 5.

As discussed in previous section, embedding that fall in possibility 1 and 2 will cause modification to the LSB, consequently this will alter the JPEG coefficient histogram distribution as shown in histogram (b) in Figure 5. The differences between original histogram and histogram with embedded message bits are illustrated in histogram (c). These differences can easily be detected by statistical attack like Chi-Square

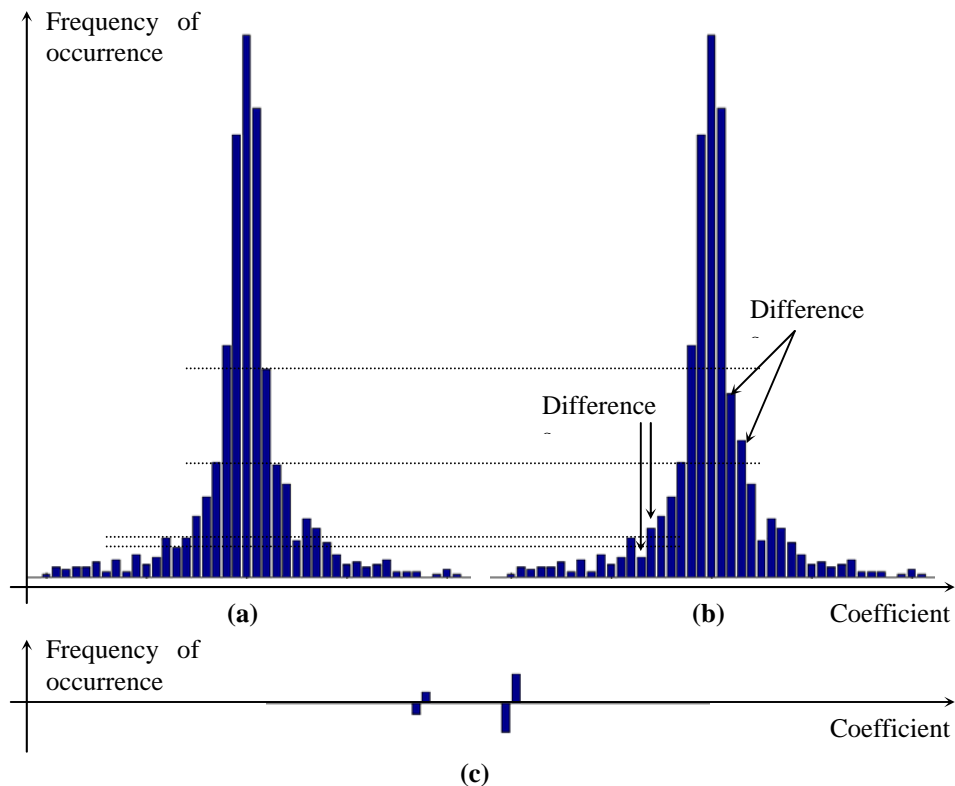


Figure 5. (a) Original histogram of an JPEG image, (b) Histogram with embedded message bits, (c) Differences between Histogram (a) and Histogram (b)

test if reparation is not applied because the more message bits are embedded, the more the histograms

will form pair values among $2i$ and $2i+1$ coefficient histograms. Figure 6 shows the result of chi-square

detection for 30% of message length embedded without reparation and Figure 7 shows the result for the same percentage of embedding with reparation technique. 30% of message length means 30% relative to the image size. It can clearly be seen that a drop from 1 to 0 at 30% of size of sample in Figure 6 indicates the success of detection for 30% of message embedded, whereas Figure 7 does not show any drop and remain in 0. Therefore, this result shows that the proposed technique managed to compensate this problem by using reparation technique as described above.

With this reparation, every time there is changed in the DCT coefficient during embedding process, the coefficient will be compensated by the following unused DCT coefficients. From the experiment, it is very rare that the system cannot find the following unused DCT coefficient for the reparation. The reason is that because every coefficient value in the histogram has 2 neighbouring values. For example, value of 6 has two neighbouring odd values which are 5 and 7. Therefore, there will always exist enough coefficients for the reparation.

7. Conclusion and future direction

In this paper, some steganography techniques have been highlighted and together with some common steganalysis techniques to give some ideas on how they work and serve as the requirement study. The reparation technique proposed in this paper is able to hide message in a JPEG image file and is capable to keep the image frequency differences to a minimum level that can withstand chi-square statistic test.

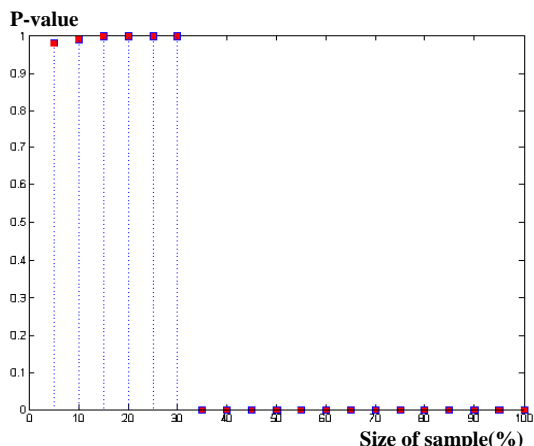


Figure 6. Probability of embedding without reparation

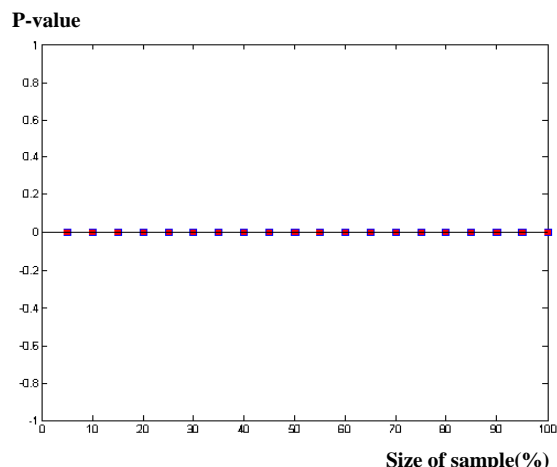


Figure 7. Probability of embedding with reparation

The future direction of this research will be directed towards the ability to preserve other higher order statistical test and also to increase the steganographic capacity. It is believed to be able to produce significant contribution in the embedding process.

8. References

- [1] T. Acharya, A. K. Ray, "Image Processing Principles and Applications". John Wiley & Sons, Inc., Publication, (2005).
- [2] J. Fridrich, R. Du, "Secure Steganographic Methods for Palette Images", Proc. The 3rd Information Hiding Workshop, LNCS volume 1768, pp. 47-60, Springer-Verlag, New York, (2000).
- [3] J. Fridrich, M. Goljan, "Practical Steganalysis – State of the Art", Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, Proc. SPIE Photonics West, Volume 4675, pp. 1-13, (January, 2002).
- [4] J. Fridrich, M. Goljan, D. Hoge, "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Information Hiding: 5th International Workshop, Book Series Lecture Notes in Computer Science, Volume 2578/2003, pp. 310-323, SpringerLink, Netherlands, (2002).
- [5] J. Fridrich, M. Goljan, D. Hoge, "New Methodology for Breaking Steganographic Techniques for JPEGs", Proc. SPIE Electronic Imaging, Santa Clara, CA, pp. 143-155, (January 2003).
- [6] Guillermito Zone (n.d.) "Analyzing steganography softwares" from <http://www.guillermito2.net/stegano/index.html> (accessed on 14 June 2007).

- [7] <http://en.wikipedia.org/wiki/Steganography>,
“Steganography From Wikipedia”, the free encyclopedia
(accessed on 3 August 2007).
- [8] M. Kwan, (Jan 21, 2003) “GIF colourmap
steganography”, from <http://www.darkside.com.au/gifshuffle>
(accessed on 03 June 2007).
- [9] J. Silman, “Steganography and Steganalysis: An
Overview”, SANS Institute (2001).
- [10] A. Westfeld, “High Capacity Despite Better
Steganalysis (F5 – A Steganographic Algorithm)”,
Information Hiding: 4th International Workshop, Lecture
Notes in Computer Science, Volume 2137, pp. 289-302,
Springer-Verlag, Berlin Heidelberg New York (2001).
- [11] A. Westfeld, A. Pfitzmann, “Attacks on Steganographic
Systems”, Information Hiding: 3rd International Workshop,
Lecture Notes in Computer Science, Volume 1768, Springer-
Verlag, Berlin Heidelberg (2000).