Image Steganography Optimization Technique

Bassam Jamil Mohd[1], Sa'ed Abed[1], Bassam Al-Naami[2], and Sahel Alouneh[3]

[1] Computer Engineering Department, Hashemite University Zarqa, Jordan
{bassam,sabed}hu.edu.jo
[2] Bio-medical Engineering Department, Hashemite University Zarqa, Jordan
b.naami@hu.edu.jo
[3] Computer Engineering, German-Jordan University, Amman, Jordan
sahel.alouneh@gju.edu.jo

Abstract. This paper presents a novel steganography technique which combines Discrete Cosine Transform (DCT) and Least Significant Bit (LSB). The objective is to maximize the capacity and invisibility of the secret image with minimal modification to the cover image (at most k-bits per block). The secret image is transformed to frequency domain using DCT. An algorithm is employed to construct the optimum quantization to embed the DCT coefficients in k-bits. The k-bits are then hidden in the LSBs of the cover image. The performance (capacity and peak signal-to-noise ratio) of the proposed method is compared with LSB.

Keywords: Steganography, Image Processing, Quantization.

1 Introduction

Steganography is the art and science of hidden communication. The objective of steganography is to communicate information in a undetectable manner such that when the messages are observed by unintended recipient there will not be enough evidence that the messages conceals additional secret data. A steganography system consists of three elements: cover-object (which hides the secret message), the secret message and the stego-object (which is the cover-object with message embedded inside it.) Many different digital cover-file formats can be used such as text, audio, image and video. However, given the proliferation of digital images, especially on the internet, and the large redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography [1].One of the main image stegnography techniques is the Least Significant Bit (LSB) where the values of one or more of least significant bits to embed the secret information. Another technique is the Transform (DCT)-based steganography which embed the secret information in the frequency domain. LSB and DCT based steganography vary in their performance with respect to capacity a security. Typically, LSB is easily detectable [2] and has larger capacity [3]. On the other hand DCT-based

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 205–209, 2012.

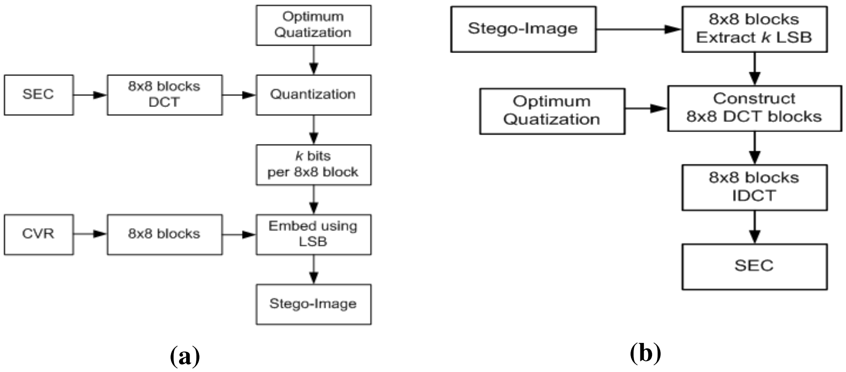
steganography has higher peak signal-to-nose ratio (PSNR) [3] and is more robust against statistical attacks 1].Reference [4] examined and evaluated LSB steganography techniques to hide messages in 8-bit and 24-bit formats. It evaluated the techniques for 2, 4, and 6 LSBs for .png and .bmp formats. Reference [4]presented an image steganography based on LSB, DCT, and compression techniques on raw images to enhance the security of the payload. The LSB algorithm is used to embed the payload bits into the cover image followed by applying DCT on the stego-image. Finally, quantization and run length coding algorithms are used for compressing the stego-image to enhance its security. Furthermore, [5] compared LSB steganography with embedding secret message in the LSB of the DCT coefficient. It demonstrated that PSNR of DCT&LSB is higher than LSB only. However, the amount of secret information in DCT&LSB is much smaller.This paper proposes an image steganography technique which combines the benefits of DCT and LSB steganography and mitigates their weaknesses. This is accomplished by embedding quantized DCT coefficients of the secret image in k-bits of cover image LSBs. An algorithm is designed to calculate an optimum quantization. The rest of the document is organized as follows. Section-2 describes the system model, illustrates the technique steps and explains proposed algorithm. Section-3 discusses some experimental results. Finally, section-4 presents concluding remarks and some future trends.

2 Proposed Model

The secret image (denoted as SEC) has a size of size N×N, and the cover mage (denoted as CVR) has a size M×M pixels. The model processes 8×8 pixel blocks of the SEC and CVR images. For each block (i) from CVR (referred as CVR_blocki) k bits are embedded, where k is determined based on the maximum distortion and accepted PSNR for the CVR. The rest of the section explains how to embed/extract secret message and discusses the optimization algorithm.

2.1 Embedding and Extracting Methods

Fig. 1 (a) illustrates the embedding method of the SEC image in CVR image. The SEC is divided into 8×8 blocks of pixels, where each block is transformed to the frequency domain using DCT. Next, the DCT coefficients are processed according to optimized quantization to represent DCT coefficients in k bits per block. The k bits are them embedded in an 8×8 cover message using LSB technique. Fig. 1 (b) demonstrates the extraction of the SEC from the stego-image. Initially, the k bits per block are extracted from the CVR least significant bits. Next, the DCT coefficients are constructed by applying reverse process of the optimum quantization on the k bits. Finally, Inverse Discrete Cosine Transform (IDCT) is applied on the DCT coefficients to retrieve secret image.



(a) **(b)**

Fig. 1. Embedding (a) and Extracting (b) Methods

2.1.1 Optimum Quantization

The quantization step calculates the optimum quantization which provides the best PSNR for SEC image. The objective is to pack as much information about the SEC in k bits (per block per color layer), which accomplished by the below algorithm. The algorithm is applied on colored images (for CVR and SEC images), where each pixel is described by three values ranging from 0 to 255. It is also assumed that the CVR image is colored image. The algorithm inputs are the SEC DCT coefficients (represented by C matrix) and k. The output of the algorithm is a matrix (Cbits), which determines the number of bits allocated for the DCT coefficients. Therefore, Cbits (i,j) states the number of bits used to quantize DCT coefficient C(i,j).

Hence, the dynamic range for C(i,j) is expressed as:

Dynamic range = [-2 Cbits(i,j)-1 , (2 Cbits(i,j)-1-1)]

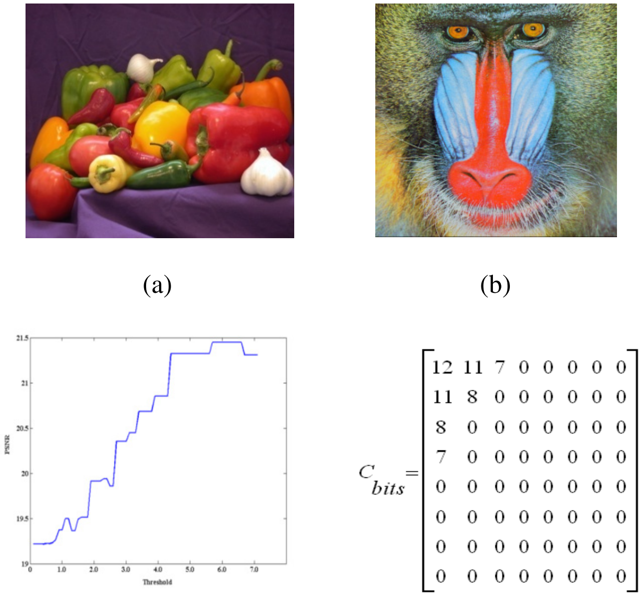
If C(i,j) is outside the rage, during the quantization it will be saturated to the closer of the limits of the dynamic rage. The algorithm searches for the optimum Cbits matrix. The algorithm consists of the following steps:

- The "average" or "weight" of C(i,j) across the blocks is determined:
- $C_w(i, j) = \frac{1}{B}\sum_{1}^{B} C(u, v)$
- whereB is the number of 8×8 blocks in SEC image. The k bits are distributed amongst the DCT based on Cw values. Larger Cw's are rewarded more bits than smaller Cw's.
- Next, the algorithm attempts to take bits from smaller owners of the bits and award them to larger owners. This accomplished by set Cbits(i,j) to zero if it is less than (δi), and redistributing the bits to other Cbits.
- Select Cbits associated with best PSNR.

Determining the min/max/step for δ requires examining many simulation runs. However, reasonable results suggest Min/Max values of 0/7.0/0.1.

3 Experimental Results

Fig 2 (a) and (b) show the CVR image (i.e. vegetables) and SEC (i.e. baboon). Both images are of size 512×512 pixels. We assume that k=64. First, the algorithm is executed to calculate optimum quantization. Fig. 2(c) illustrates the PSNR as a function of δ. The PSNR compares the original SEC vs. extracted SEC. The algorithm improves PSNR as it moved fromδ=0 to δ=5.5. In this interval, pruning small Cbits and giving the free bits to larger Cbits helped PSNR. The PSNR plateaued between δ=5.5 to δ=6.5 where PSNR is at 21.45 dB. Then PSNR starts declining after δ=6.5, because the algorithm started to remove important Cbits. The Cbits matrix associated with best PSNR is shown in Fig. 2(d).



$$C_{bits} = \begin{bmatrix} 12 & 11 & 7 & 0 & 0 & 0 & 0 & 0 \\ 11 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(a) (b)

(d) (c)

Fig. 2. The Cover Image (a) Secret Image (b)PSNR(c) and C_{bits} matrix (d)

Fig. 3 shows the stego-image and extracted image. The PSNR for the stego-image compared with CVR is 51.1 dB, which is considerably high. In fact 51.1 dB implies that ~1% of CVR data have been modified after embedding the SEC.Since only 1% of the CVR image data is modified with unknown quantization (except for the intended recipient), the embedded message is securely encrypted. Hence, the proposed steganography method provides high level of imperceptibility for the secret image.When compared with LSB, the proposed method provides better security since

(a)

(b)

Fig. 3. The stego-image (a) and recovered SEC image (b)

the quantization serves as an encryption. Additionally, the proposed method is superior in terms of capacity and PSNR.

4 Conclusion

In this paper, we have presented a steganography technique which is based on LSB and DCT methods. Existing LSB_DCT steganography methods suffer from limited poor PSNRStego as number of LSBbits increases. Furthermore, some of the existing methods have capacity issues.The proposed method embeds the entire SEC image while balancing the PSNR for CVR and SEC images by calculating an optimum quantization for SEC DCT coefficients. Moreover, the quantization improves imperceptibility for the secret message.

References

1. Morkel, T., Eloff, J., Olivier, M.: An Overview of Image Steganography. In: The Fifth Annual Information Security South Africa Conference (ISSA 2005), Sandton, South Africa (June/July 2005)
2. Wang, H., Wang, S.: Cyber warfare: Steganography vs. Steganalysis. Communications of the ACM 47(10), 76–82 (2004)
3. Walia, E., Jain, P., Navdeep: An Analysis of LSB & DCT based Steganography. Global Journal of Computer Science and Technology 10, 4–8 (2010)
4. Deshpande, N., Sneha, K., Jacobs, D.: Implementation of LSB Steganography and Its Evaluation for various Bits. In: 2006 1st International Conference on Digital Information Management, pp. 173–178 (2007)
5. Raja, K., Chowdary, C., Venugopal, R., Patnaik, L.: A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. In: 3rd International Conference on Intelligent Sensing and Information Processing, pp. 170–176 (2005)
6. Walia, E., Jain, P., Navdeep: An Analysis of LSB & DCT based Stegnography. Global Journal of Computer Science 10, 4–8 (2010)