Image Steganography

Yan-Yu Yang
National Tsing Hua Univeristy
Hsinchu, Taiwan

***Abstract*—This paper presents a comparative study of digital image steganography techniques implemented in the spatial and frequency domains. Specifically, least significant bit (LSB) replacement and discrete cosine transform (DCT) based embedding methods are analyzed in terms of imperceptibility, robustness, and embedding capacity.**

The performance of each approach is evaluated using peak signal-to-noise ratio (PSNR) and bit error rate (BER) under both noise-free and filtered conditions. To assess robustness, stego images are subjected to Gaussian low-pass filtering, which commonly occurs in image processing and compression pipelines. Experimental results demonstrate that while LSB-based steganography offers high embedding capacity and excellent visual quality in ideal conditions, it is highly fragile and suffers from severe degradation after filtering. In contrast, the DCT-based method exhibits significantly improved robustness to filtering, maintaining low BER at the expense of reduced capacity.

The results highlight the inherent trade-offs between spatial and frequency domain steganography and demonstrate that transform-domain embedding is more suitable for practical applications where robustness against signal processing operations is required.

***Index Terms*—DSP, DCT, Steganography, Image processing**

I. Introduction

With the rapid growth of digital communication and multimedia sharing, protecting the confidentiality of transmitted information has become increasingly important. Cryptography is widely used to secure sensitive data by transforming it into an unreadable form. However, encrypted data often attracts attention due to its apparent randomness. In contrast, steganography aims to conceal the very existence of a message by embedding it within a carrier, such as an image, audio signal, or video stream.

Digital image steganography exploits redundancies in image representations and limitations of the human visual system to embed secret information without introducing perceptible distortion. The primary objectives of an effective steganographic system are high imperceptibility, sufficient embedding capacity, and robustness against common signal processing operations. Achieving all three simultaneously is challenging, and improving one aspect often degrades the others.

Existing image steganography techniques are commonly categorized into spatial domain and frequency domain methods. Spatial domain techniques, such as least significant bit (LSB) replacement, directly modify pixel values to embed data. These methods are simple to implement and provide high embedding capacity, but they are extremely sensitive to noise, filtering, and lossy compression. Even minor image processing operations can significantly corrupt the hidden data.

To address the fragility of spatial methods, frequency domain approaches embed information into transform coefficients obtained using techniques such as the discrete cosine transform (DCT). Since modern image compression standards like JPEG operate in the frequency domain, embedding data in selected frequency components can improve robustness against compression and filtering. However, this robustness is typically achieved at the cost of reduced payload capacity and increased computational complexity.

In this paper, a systematic comparison between LSB-based spatial domain steganography and DCT-based frequency domain steganography is presented. The study focuses on evaluating their robustness against Gaussian low-pass filtering, a common image processing operation. Performance is quantitatively assessed using bit error rate (BER) to measure robustness and peak signal-to-noise ratio (PSNR) to evaluate imperceptibility. Through experimental analysis, this work aims to highlight the practical trade-offs between the two approaches and provide insights into selecting appropriate steganographic techniques for real-world applications.

II. Methodology

The process of image steganography can be divided into two sections as shown in Fig. 1. We need to encode the secret message into binary string, such as ASCII code. The binary data can be embedded in the cover image we choose by different approaches. The ”stego image” is yielded by combining different type of data into another. In general, we can embed image into audio, text in audio, audio in image, etc.

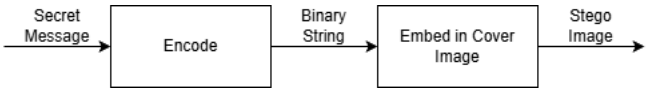

Fig. 1. The general process of generating image steganography.

A. Message Encoding

We map every character to 8 bits binary sequence. The header of output binary string consists of 8 bits pilot signal and 16 bits data representing the length of the message. The pilot signal is a known sequence, e.g., 11110000, which is used to determine the threshold for the detector.

B. Spatial Domain Implementation (LSB)

The spatial domain approach utilizes least significant bit (LSB) Replacement. This technique operates directly on the pixel RGB values of the cover image.

The decoding process is also simple, we retrieve the bit stream directly from the LSB of the stego image.

C. Frequency Domain Implementation (DCT)

The implementation begins by converting the image from RGB to YCbCr. In steganography, the Y (Luminance) channel is the preferred carrier. Although the variation of brightness is more sensitive for human eyes than chrominance, it provides greater robustness against compression and common image processing operations.

Each 8×8 block is transformed from the spatial domain to the frequency domain using the 2D-DCT.

$$C_n(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) \times \cos\left[\frac{(2x+1)u\pi}{16}\right] \cos\left[\frac{(2y+1)v\pi}{16}\right] \tag{1}$$

where

$$\alpha(u) = \begin{cases} \frac{1}{2\sqrt{2}}, & u = 0, \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

$$\alpha(v) = \begin{cases} \frac{1}{2\sqrt{2}}, & u = 0, \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

To simulate the effects of JPEG compression and to provide a stable embedding surface, the coefficients are divided by the luminance quantization table (Q). We round the coefficients to compress the data.

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}. \tag{2}$$

For robustness against compression, we target the mid-frequency range, e.g. $(u, v) = (3, 3)$. Since the low frequencies are too visually sensitive, and high frequencies are often discarded in the compression. After quantization and rounding, the mid-frequency components are very likely to be 0. We modify the mid-band frequency as shown in Eq. 3.

$$\begin{cases} C_n(u_s, v_s) = \beta, \text{ if } bit = 1, \\ C_n(u_s, v_s) = -\beta, \text{ if } bit = 0, \end{cases} \tag{3}$$

where (u_s, v_s) denote the modulated frequencies. For large β, the message is more robust, but the imperceptibility is worse. It is a tradeoff between robustness and imperceptibility. After embedding the message, we multiply the quantization table and perform the inverse discrete cosine transform (IDCT) to reconstruct the image. The overall encode process is shown in Fig. 2. [1]

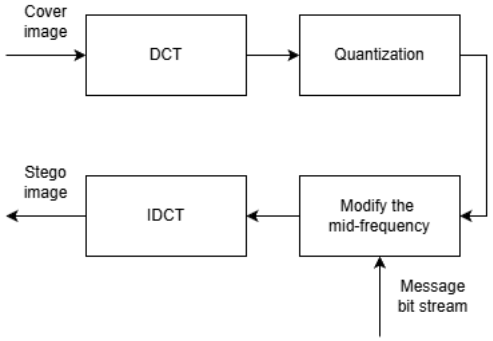

Fig. 2. Embedding method for DCT steganography.

The decode part is similar to encode part. The mid-frequency component is obtained by performing DCT and quantization with respect to the stego-image. For noise-free and unfiltered scenarios, the message retrieval is trivial. However, the decision rule is necessary for filtered image. The decision rule is given by

$$b[n] = \begin{cases} 1, \text{ if } C_n(u_s, v_s) > T[n], \\ 0, \text{ if } C_n(u_s, v_s) < T[n], \end{cases} \tag{4}$$

where T denotes the threshold. The threshold is adaptive, which is obtained by a IIR filer given by

$$T[n] = \begin{cases} \alpha T[n-1] + (1-\alpha)b[n], \text{ if } 8 \le n, \\ T[n-1] + \frac{1}{8}b[n], \text{ if } 0 \le n \le 7, \\ 0, \text{ if } n < 0, \end{cases} \tag{5}$$

where α is a tunable parameter. It is worth nothing that the begin threshold is acquired by the pilot signal. The overall structure of the decode process is fully illustrated by Fig. 3

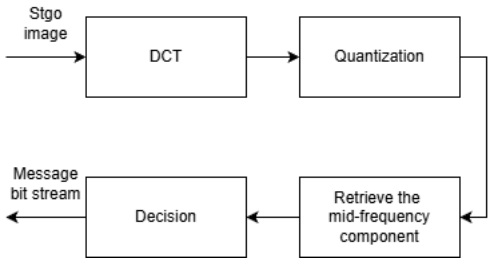

Fig. 3. Embedding method for DCT steganography.

D. Evaluation

The bit error rate (BER) and peak signal to noise ratio (PSNR) are used to evaluate the robustness and imperceptibility, respectively. [2] For BER calculation,

$$BER = \frac{N_e}{min(L_m, L_{en})} \le P_{symbol}, \tag{6}$$

where N_e denotes the number of error bits, L_m denotes the length of the message bits, L_{en} denotes the length of the encode bits, and P_{symbol} denotes the symbol error probability.

The method is more robust if the BER is smaller. The PSNR is given by

$$PSNR = \frac{\left[\max_{x,y} I(x,y)\right]^2}{\frac{1}{mn}\sum_{y=0}^{m-1}\sum_{x=0}^{n-1}\left[I(x,y) - K(x,y)\right]^2}, \quad (7)$$

where $I(x,y)$ denotes the luminance original image, $K(x,y)$ denotes the luminance of the stego image. We usually use dB to represent the PSNR. For larger PSNR, the stego image is more similar to the original one. The PSNR measures the visual imperceptibility of the method. In this paper, we define the energy of the image as

$$E = \left|\frac{\partial I}{\partial x}\right| + \left|\frac{\partial I}{\partial y}\right|. \quad (8)$$

III. Result and Discussion

A. Visual Artifact Comparison for Unfiltered Images

In this section, we compare the visual artifacts qualitatively. In the following section, we will discuss them quantitatively.

Fig. 4. The stego image for LSB and DCT method.

Fig. 5. The detail of stego image (Hotel California) for LSB and DCT method.

Fig. 6. The detail of stego image (Water Lilies) for LSB and DCT method.

As shown in Fig. 4, the outcomes of both the LSB and DCT methods exhibit very few visual artifacts. However, detailed inspection reveals that small dots appear in the upper-left region of the image when zooming in on the DCT stego image as shown in Fig. 5. If we change the cover image, the small dots may be visual imperceptible, as we shown in Fig. 6. Since the energy of the cover image is high, the small variation we make does not cause severe artifacts.

B. Performance for Filtered Image

The performance is evaluated by three indexes, BER for robustness, PSNR for imperceptibility, and capacity. From Table I, we observe that the LSB has much more capacity than DCT. Nevertheless, the BER of LSB is about 54%. From the aspect of information theory, this implies that the decoded data is nearly useless. Conversely, the DCT approach has BER of 0.18%. For audio signal, this BER may be good enough, but we may need to add error correction bits for text data.

TABLE I
Comparison of LSB and DCT-based methods

	LSB	DCT ($\beta = 2$)
BER	54%	0.18%
PSNR	34.11 dB	31.41 dB
Capacity	$3 \times$ image size	$\left\lfloor \frac{\text{width}}{8} \right\rfloor \times \left\lfloor \frac{\text{length}}{8} \right\rfloor$

C. Robustness and Imperceptibility Trade-off

The performance of the DCT method is significantly influenced by the embedding strength parameter, β. In this section, we use the stego image filtered by 5×5 Gaussian filter since the BER is always zero for unfiltered image.

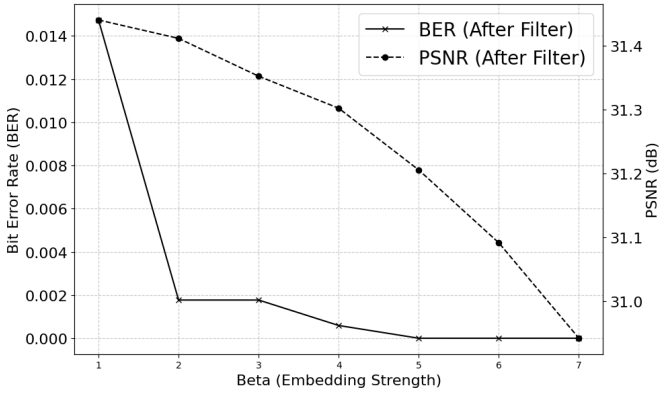

Fig. 7. Impact of β on filtered image (Hotel California) robustness and quality.

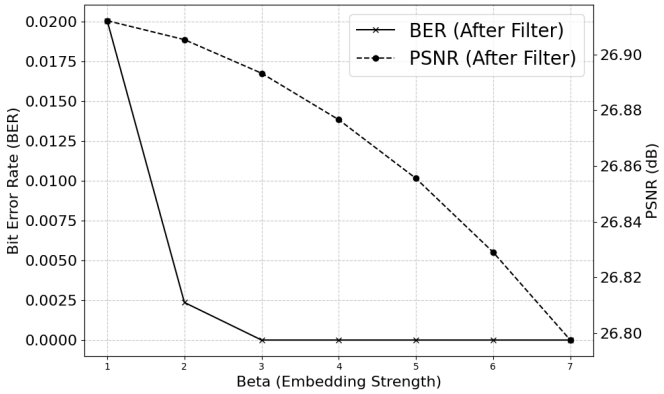

Fig. 8. Impact of β on filtered image (Water Lilies) robustness and quality.

From Fig. 7 and Fig. 8, we observe that an increase in β improves robustness by decreasing BER after filtering, but simultaneously degrades imperceptibility by decreasing PSNR. In addition, we may consider $\beta = 2$ as the optimal embedding strength since the BER drops significantly and the PSNR degrades little. Furthermore, experimental data shows that the PSNR drop for "Water Lilies" is smaller than that for "Hotel California", implying that the resulting artifacts are lower for high energy part. This can explain the difference in Fig. 5 and Fig. 6. Thus, we should avoid embedding the message in low energy part, e.g., sky, plain wall, ocean, etc.

D. Limitations

In this paper, we only test the robustness against the image filtering. There are lots of image processing technique that will lead the DCT method to fail, e.g., cropping, resizing, rotation, etc. Even though DCT methods have little visual artifacts, certain modifications can be detected as "dots" in specific areas, such as the upper left region of the image, when inspected close enough.

IV. Conclusions

Digital image steganography presents a critical trade-off between imperceptibility, embedding capacity, and robustness. This comparative study demonstrates the distinct performance profiles of spatial and frequency domain techniques.

- Spatial Domain (LSB): While LSB replacement offers superior embedding capacity and high computational efficiency, it is inherently fragile. Experimental results indicate that spatial domain methods suffer from significant bit error rates (approximately 54%) when subjected to common filtering attacks, rendering the decoded data nearly useless.
- Frequency Domain (DCT): Frequency domain methods exhibit higher resilience to intentional signal smoothing and filtering. By targeting the mid-frequency range, such as $(u_s, v_s) = (3, 3)$, these methods successfully preserve message integrity, achieving BER as low as 0.18%, albeit at the cost of reduced payload capacity.
- Optimal Embedding Strength: The performance of the DCT method is significantly influenced by the embedding strength parameter, β. The study identifies $\beta = 2$ as an optimal balance point where the bit error rate (BER) drops significantly while visual imperceptibility, measured via PSNR, degrades minimally.
- Energy Aware Embedding: Embedding secret messages in high-energy regions of an image results in fewer detectable visual artifacts than embedding in low-energy areas like clear skies, plain walls, or the ocean.

Future work could extend this study by incorporating error correction coding, testing robustness against additional attacks such as compression and geometric transformations, or exploring adaptive embedding schemes to further enhance performance.

V. Reflection

This project provided valuable hands-on experience in both the theoretical and practical aspects of image steganography. By implementing and evaluating steganographic techniques in the spatial and frequency domains, I gained a deeper understanding of the fundamental trade-offs between imperceptibility, robustness, and embedding capacity.

One important takeaway from this work is that visual quality alone is not a sufficient metric for evaluating steganographic performance. Although the LSB method produced stego images with high PSNR and minimal visible artifacts under noise-free conditions, it proved extremely vulnerable to even mild image filtering. This highlighted the importance of robustness testing and reinforced the idea that real-world communication channels are rarely ideal.

The frequency domain implementation, particularly the DCT-based method, offered insight into how transform domain techniques leverage properties of common compression standards to improve resilience.

Overall, this project strengthened my understanding of digital signal processing concepts such as DCT, quantization, and filtering, while also illustrating how theoretical knowledge translates into practical system design challenges.

References

[1] E. Walia *et al.*, "An analysis of LSB and DCT based steganography," *Global Journal of Computer Science and Technology*, vol. 10, no. 1, Apr. 2010.

[2] N. Hamid *et al.*, "Image steganography techniques: An overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, 2012.

Appendix

The implementation of the algorithms and the experimental framework used in this study are available at the following repository:

https://github.com/lucyanyuyang/Image-Steganography