# Block Based Image Steganography in Spatial and Frequency Domain

D.N.F Awang Iskandar[1], Abdulmalik Bacheer Rahhal[1,2] and Wadood Abdul[2]
[1]*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia.*
[2]*Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia.*
*dnfaiz@unimas.my*

***Abstract*—Steganography is the art of hiding a secret message in different kind of multimedia (image, voice or video), such that the secret message is not detectable. In this paper, we propose two new algorithms, first one uses the spatial domain for steganography, where the host image is converted into blocks of bit-planes to insert the secret information. The algorithm divides the image into 8 bit planes and then the bit planes are further divided in to N x N blocks. The hidden message is inserted based on a chaotic sequence. We intend to find the most optimum bit plane to insert the hidden information, keeping high imperceptibility in terms of the human visual systems. The algorithm shows relatively good Mean Structural Similarity and Peak Signal to Noise Ratio values. The second algorithm is applied in the frequency domain where the host image is converted using the discrete wavelet transform. Then at second and third level of the transform, the secret information is inserted. The proposed algorithm divides wavelet level divide in to M x M blocks. The hidden message is inserted based on chaotic sequence in to the blocks. This algorithm shows better imperceptivity in terms of the human visual system and PSNR.**

***Index Terms*—Bit Plane; Force of Insertion; Spatial Domain Steganography; Wavelet Domain.**

## I. INTRODUCTION

Steganography and encryption are used to transfer secret information. Steganography attempts to hide the transfer of information whereas encryption attempts to make it computationally difficult for an adversary to decrypt the encrypted information [1].

The main purpose of steganography or data hiding is to hide or protect important information for some application. As an example of why two parties wish to have secret communication, it can be used for a political reason as in case of a dissident organization wishing to communicate among themselves. It is also used in the medical field where patients do not want their identity to be linked to their medical records. The multimedia file is only accessible to the doctor and not to anyone else thus preserving the privacy of the patient through steganography.

The main objective of steganography is to ensure communication secrecy and security using different kinds of multimedia, we developed novel imperceptible algorithms for steganography in the spatial and frequency domains. These algorithms are evaluated and compared with other algorithms found in the literature.

The rest of the paper is organized as the follows. In the next section we present the related work. In section III, the proposed block steganography algorithm is described. In Section IV, results are illustrated followed by the capacity analysis and comparison. We conclude our findings in section V.

## II. RELATED WORK

The steganographic algorithms are classified in to the spatial domain algorithms and frequency domain algorithms [2].

### *A. Spatial Domain Steganography*

The Least Significant Bit (LSB) replacing is the most important data hiding method. It is a simple method with high embedding capacity but the hidden data is sensitive to image alteration and vulnerable to attacks [3-8]. In the frequency domain, the image is decomposed into transformed components by using transforms like the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [3] and Discrete Wavelet Transform (DWT) [4],[5], [6]. These components are modified according to the embedding algorithm to insert the secret data. Hiding data in the frequency domain has certain advantages over hiding in the spatial domain; it provides higher robustness against changes and attacks, which means more resistance to loss from image manipulation and increased difficulty for a potential attacker. However, it is relatively costly in terms of complexity [3, 11], also the amount of secret data that can be hidden in frequency domain is less than the LSB scheme [7].

Bandyopadhyay et al. in [8] proposed a 3-3-2 LSB (three, three and two least significant bits from the red, green and blue color components respectively) insertion method in RGB color pixels. This pattern distribution is considered because the human eye is more sensitive to changes in the blue color component compared to the red and green color components. The secret image is inserted into the cover image using chaotic sequence and XOR operation.

In a similar method Amritpal Singh and Harpal Singh proposed 2-2-4 LSB (two, two and four significant bits from red, green and blue color components respectively) insertion method in RGB pixels respectively. Experimental results in [8] and [9] show better PSNR for Lenna image in [9] compared with [8], but on the other hand the algorithm proposed in [4] has less capacity.

In [10] authors proposed spatial domain steganography algorithm based on reversible logic. They use Feynman gate to achieve reversibility for the image with simple LSB technique. A nano-communication circuit for image steganography is shown using proposed encoder/decoder