Image Steganography Based on DNA Encoding and Bayer Pattern

Elaf Ali Abbood(✉), Rusul Mohammed Neamah, and Qunoot Mustafa Ismail

Computer Department, Science College for Women, University of Babylon, Babylon, Iraq
wsci.elaf.ali@uobabylon.edu.iq

Abstract. Steganography is a method of concealing sensitive data while transmitting it over public networks and it is regarded as one of the invisible security techniques. This paper proposed a new method to encrypt and hide a 24-bit color secret image within a larger 24-bit color cover image using the Bayer pattern principle and LSB algorithm. The secret image goes through a series of special steps of DNA encryption. Then hides to ensure more confidentiality and be more difficult for the attackers' attempts. In this method, each pixel in the secret image is hidden in a 3 × 3 block from the cover image except the center of the block that is used as a public key. These blocks randomly select from the rows and columns of the cover images. The secret image pixels and the center selected block pixels are encrypted in a special method using DNA rules. Then, encoding the resulted encrypted image and encrypted center blocks selected pixels using the DNA-XOR operation. Finally, hiding the resulted image pixels using the Least Significant Bit (LSB) algorithm with locations determined by a modified Bayer pattern. The experimental results show the efficiency of the proposed method to produce a high-quality stego image and the results are acceptable when applying the Structural Similarity Index Metric (SSIM) and Peak Signal to Noise Ratio (PSNR) quality metrics and compared with other method.

Keywords: Information hiding · DNA encoding · Bayer pattern · PSNR · SSIM

1 Introduction

Hiding data is typically related to well-publicized infamous attempts, like secret arranging and coordination of crimes through messages hidden in pictures spread on the general websites [1, 2]. In addition to the many misuse cases, steganography is also utilized in the application of positive operations. For instance, concealed pictures utilized by way of watermarks involve copyright and copyright datum without outwardly disfiguring the picture [3]. In the development of information and communication technology fields, the transmission of confidential information through general channels and websites has become one of the main challenges of our time. Where there are three techniques for concealing information: encryption, concealment, and watermark.

© Springer Nature Switzerland AG 2021
A. M. Al-Bakry et al. (Eds.): NTICT 2021, CCIS 1511, pp. 49–62, 2021.
https://doi.org/10.1007/978-3-030-93417-0_4

The first technique depends on masking the presence of a message. The second technique hides the data as a media format like image, audio, video, and even text in which unauthorized people do not observe the presence of the data in the aforementioned form. The last technology protects copyrights and authorship. Lately, much attention has been given to the science of concealing information [4].

Steganography is a science that aims to include private and confidential data in the cover medium. This process protects copyrights or identifies the identity and securing the data so that the hackers cannot discover the information [5, 6]. Image files are especially popular for medium cover because there is a great deal of redundant space suitable for hiding confidential information. Steganography techniques, by and large, utilize a comparable key to embed confidential messages and create yield information known as stego-image ought to imperceptible of the carrier media to darken the correspondence between the different parties [7].

In this approach, image properties such as a histogram, the SSIM must stay unchanged after the confidential information is covered in it [8]. Encryption is a technique that saves confidential data by encrypting it, so that only an authorized person can read it [9].

The least significant bit (LSB) is the most widely utilized and common image masking technique [10]. Accordingly, the value of the pixel is expanded or reduced by one. If the value of the pixel of the image is changed by "1", it will not alter the appearance of the image. This makes it easier to hide the information, especially when the cover image is larger than the image of the secret message [11].

The Bayer pattern is one of the techniques that used in the proposed method. The Bayer pattern is expressed by a color filter array (CFA). It is considered as an interpolation technique used to find the missed colors in the sensors of the images in digital cameras. As illustrated in Fig. 1, this pattern contains red and blue pixels, which surround green pixels vertically and horizontally. And because the human eye is more sensitive to green, that's why Bayer allocates the largest number of green pixels versus red and blue to produce a better color image [12].

To strength the hiding technique, it has merged with one of the encryptions techniques. DNA encryption is one of the image encryption techniques. DNA encryption uses the DNA molecules to encodes image pixels in a special way that gives big parallelism with little consumption for energy and high storage compactness [13, 14]. Consequently, DNA image encryption methods are considered as one of the straight encryptions methods against the traditional cryptanalysis algorithms [15].

In this work, the secret image is encrypted using a new DNA encryption method. The encrypted color image is hidden within random blocks of the cover image. Every three bands from the secret image pixel are hidden in a block from the cover image. The proposed method depends on the concept of the Bayer pattern in the hiding process after introducing some modifications.

The contributions of this work contain:

1. Increasing the security robustness by encrypting the secret image using a new DNA encryption method. This encoding process increases the safety of the method and it makes the method difficult for hackers to discover confidential information.