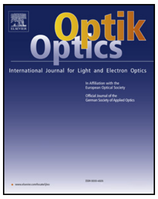
Optik - International Journal for Light and Electron Optics 170 (2018) 106–124

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.com/locate/ijleo



Original research article

Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map

Gurjit Singh Walia[a,*], Shikhar Makhija[b], Kunwar Singh[b], Kapil Sharma[c]

[a] *Scientific Analysis Group, Defence Research and Development Organization, Ministry of Defence, India*
[b] *Netaji Subhas Institute of Technology, Department of Electronics and Communication, University of Delhi, India*
[c] *Department of Information Technology, Delhi Technological University, Delhi, India*

ARTICLE INFO

Keywords:
High capacity
Steganography
Image data hiding
Image scanning

ABSTRACT

High capacity image steganography using Least Significant Bit (LSB) substitution greatly impaires visual quality of the stego image. In addition, most of steganographic schemes consider direct embedding of secret message without considering its security concern over public channel transmission. To address this problem, we have introduced a novel stego-key directed LSB substitution scheme which not only offers high embedding capacity but also resilient against stego image distortion. The aim of this work is to consider this problem as search and optimization. High embedding capacity is achieved through optimal utilization of search domain using proposed LUDO scan scheme. Optimal Stego-key is determined through cuckoo search optimization where *Le´vy* flight is used for obtaining new Stego-key. In addition, secret message is encrypted before embedding using chaotic map generated through random key. Large key space of Stego-key offer high resistance against various crypt analytic attacks. Proposed steganography scheme is evaluated over nine standard test images and competitive results are obtained. On an average, we achieved a Peak Signal-to-Noise Ratio (PSNR) of 44.09 and Structural Similarity Matrix (SSIM) of 0.97. Results demonstrate that the proposed steganography scheme not only outperforms state-of-the-art high embedding steganography schemes but also offers high payload capabilities with immunity against visual degradation.

1. Introduction

Steganography is imperative for coherent ways of digital security in the age of global digitisation. It offers a ‘covert’ transmission of information between two nodes on a network, whose existence is unknown to the attacker or any eavesdropper. This process involves embedding secret data in an innocuous message which acts as a host or cover (e.g. text, image, video etc.). This modified host or cover is called a stego – object. Thus, it forms a subliminal channel between the transmitter and receiver [1]. The fundamental and foremost aim of any steganography method is to achieve impenetrable security, visual imperceptibility and high payload capabilities. Many types of host media can be used but digital images are the most common host media because of their high frequency of usage on Internet [2]. Steganography is widely utilized in defence applications, as it promises transmission of data in a reliable and efficient manner with minimal vulnerability to an illicit access.

In recent past, many state-of-the-art steganographic methods have been reported. These steganographic methods can be divided mainly into two classes, namely spatial domain and frequency domain. Frequency domain method involves alteration of the transfiguration of the host image by various transforms such as Discrete Cosine Transform (DCT) [3], Adaptive Wavelet Transform

[*] Corresponding author.
E-mail address: gurjit.walia@gmail.com (G.S. Walia).

https://doi.org/10.1016/j.ijleo.2018.04.135
Received 2 August 2017; Received in revised form 27 April 2018; Accepted 29 April 2018

[4] and Discrete Wavelet Transform (DWT) [5] etc. This class of steganography offers a higher resistance against steganalysis attacks but has a limited payload capability. It is extensively employed in digital watermarking and fingerprinting [6]. On the other hand, spatial domain steganography involves alteration of the host pixel intensities to hide the secret message. LSB substitution is one of the most popular spatial domain steganographic method. In this scheme, data is hidden by the replacement of the LSB of the host image by the secret message. Optimal Least Significant Bit Substitution techniques have been devised in the past employing genetic algorithm [7] or dynamic programming strategies [8] to achieve better stego - image quality. These techniques provide an appreciable image quality but are prone to many steganalysis attacks [9] and a higher distortion for greater payloads. Many, other spatial domain techniques have also been devised which exploits the limitations of the Human Visual System (HVS) to gain visual imperceptibility. HVS is more sensitive to distortions in a smooth area as compared to the area of sharper contrast. On this observation, Pixel Value Differencing (PVD), a spatial domain steganography method was devised to hide secret information according to the difference in intensity between two consecutive pixels [10]. Further, improvement was made to payload capabilities by limiting the application of PVD to edge areas and corresponding application of LSB substitution in smoother areas [11]. However, PVD utilizes range table, leading to a more computational complexity than simple LSB substitution.

In addition to this, many other techniques have reported to achieve appreciable stego – image quality. Data compression [12,13] and vector quantisation [14] based approach are also some of the widely used steganographic techniques. In most of these techniques the recovery of host image is not feasible. In order to cater for this limitation, work on reversible steganography has also been reported in recent past. Reversible steganography was achieved through various techniques such as image interpolation [15], zero and minimum value of histogram of image [16], difference expansion of vectors [17] and image inpainting technique [18].

Generally, steganographic methods are motivated with a common objective to exploit cover image in an efficient and reliable manner. However, limited research work has been reported which considers steganography as a search and optimization problem. In sum, problem of robust steganography with optimal and sustainable utilization of the host image through state-of-the-art optimisation technique is limitedly solved. To solve this problem, we have proposed an optimal stego-key based LSB substitution scheme based on Cuckoo search optimisation technique that offers high embedding capacity.

The main contributions of the proposed work are listed as follows:

- Proposed a robust ninety bit Stego-key directed LSB substitution scheme that offers high embedding capacity with immunity against visual degradation.
- Resilience against distortions caused by high embedding is achieved through optimal embedding using Cuckoo Search optimisation and maximisation of search domain using the proposed LUDO scanning.
- Substitution scheme is controlled by the optimiser and thus, optimum stego image quality is achieved regardless of message size.
- Immunity against various cryptanalytic attacks is obtained through shuffling the secret message through logistic maps and chaotic sequences.
- Global optimisation regardless of domain parameters is obtained with low computational requirement.
- Extensive experimental validation on benchmarked images to demonstrate real-time implementation.

The rest of the paper is structured in the following manner. In Section 2, various works related to the field of LSB based steganography have been presented. We have introduced core design of proposed steganographic method in Section 3. In addition, flow chart and pseudo code are illustrated. Various implementation intricacies and data set challenges for experimental simulation are highlighted in Section 4. Proposed method is compared both qualitatively and quantitatively with various state-of-the-art steganographic techniques in Section 5. Finally, summary and future directions are sketched out in Section 6.

2. Related work: LSB based steganography

Many state-of-the-art steganographic techniques were reported in literature over the last decade. In this section, we have discussed various technological developments in LSB substitution in order to gauge the gap in reported research work. Detailed comparison of various state-of-the-art methods is tabulated in Table 1 and discussed as follows. In general, LSB substitution provides appreciable visual quality with minimal computational complexity. However, it involves a trade-off between stego image quality and dimensions of secret data that can be embedded. To resolve this, Chan et al. [19] proposed an approach which involved application of Optimal Pixel Adjustment Process (OPAP) after LSB substitution to improve image quality. However, this approach is highly susceptible to various data corruption and extraction attacks. In [7], an optimal k – bit LSB substitution technique based on Genetic Algorithm was introduced. k – bit decomposed secret image pixels was randomised by a bijective map function. Due to randomisation, resultant secret image was immune to various data scraping attacks. PSNR was maximised by selecting optimal substitution matrix using genetic algorithm. This approach was highly exhaustive and computational expensive. To address this problem, Chang et al. [8] proposed a LSB substitution method which derived its optimal solution using a dynamic programming strategy. In similar lines, Wang et al. [20] proposed a Meta – heuristic approach based on Cat Swarm Optimisation (CSO) strategy to derive optimal substitution matrix. These techniques provide appreciable visual quality but fail in utilizing the cover image effectively and obtain globally optimal image quality.

LSB substitution along with Pixel Value Differencing (PVD) was used to achieve high payload capabilities [11]. Host image is partitioned into non – overlapping blocks of adjacent pixel intensities. If difference between subsequent pixels is a subset of lower division of range table, simple LSB substitution technique was adopted. While for areas of sharper contrast, PVD embedding technique was employed. Furthermore, Khodaei et al. [21] improved the payload capabilities of this technique and also preserved the