Journal of Information Security and Applications 000 (2017) 1–10

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A new transform domain steganography based on modified logistic chaotic map for color images

Milad Yousefi Valandar[a,*], Peyman Ayubi[b], Milad Jafari Barani[a]

[a] Young Researchers and Elite Club, Urmia Branch, Islamic Azad University, Urmia, Iran
[b] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Digital image steganography
Modified logistic map
Integer wavelet transform

ABSTRACT

The art and science of hiding information by embedding messages in various type of digital media is called steganography. This method performs by replacing bits of multimedia files (such as graphics, sounds and texts) with bits of secret message. The information that embeds in the cover media can be plain text, cipher text and even images. Steganography sometimes is used when encryption is not permitted or more commonly, steganography is supplement for encryption. By using steganography, if the encrypted file is deciphered, the encrypted file may still hide information. This paper is proposed a new transform domain steganography method based on integer wavelet transform (IWT) for digital images and also it used a chaotic map. This map is a modified logistic map which it increases the key length and security of proposed method. Experimental results shows that the proposed method has high capability in hiding information in any images which used as a cover media. Visual quality of image after embedding process is desirable due to Peak Signal-to-Noise Ratio (PSNR) measures. Also the NIST, DIEHARD and ENT tests suite show the proposed chaotic map randomness and sensitivity to smallest changes.

1. Introduction

With development of communication science, the quick and easy access to most communication networks are accessible. Today, anyone can be connected to these networks with many devices in any locations. This progress has also brought problems such as imperil the owners rights of property. Hence, we need to provide the new secure ways to ensure the security of digital documents. Generally, there are three ways to secure digital data: Cryptography, Watermarking and Steganography [1,2]. In cryptography, digital data scrambled with a key and it can be restored with the same key [3]. This method does not guarantee the security of data after decryption [4]. In the watermarking methods, the limited and specific information embeds into digital data to prevent unauthorized tampering [5,6]. Steganography is the art and science of embedding a secret message inside the cover media [7]. This method is mostly used for private and secure communication and it is a necessity in security applications [8].

Most steganography methods uses a shared key to hide secret message and generate a stego [9]. To conceal the communication between two side, stego should be statistically undetectable from the cover media. Increasing the size of the cover media after embedding secret message, undetectability and the amount of distortion are three important points that should be consider in the proposed steganography methods because these points show the capability of the algorithm in embedding process and diagnosis the histogram changes resistance against the histogram based attacks [10–14].

Generally, steganography is divided into four domains: *1. Spatial domain:* In this type of technique, secret message bits embeds directly into the cover media bits and usually they have simple algorithms. LSB (least significant bits) is one of the most well-known algorithms in this domain that replaces secret message bits with cover media's LSB. This change is undetectable by the human eye but it can be recognize with statistical tests [15–17]. The LSB methods are very fast and simple but they have some disadvantages: a) The secure message size is small. b) The secure message bits destroys in cover media compression. c) With smallest changes in media cover the embedded information can be disappears [18]. *2. Transform domain:* This category uses transformation for embedding secure message in cover media [19]. These transforms are included: DCT (Discrete Cosine Transform): In this type, cover media divides into 8 × 8 blocks. These blocks quantize with quantization table and then the cover media's sensitive bits determine in each block [20]. The embedding process performs in all parts of each blocks especially in the high sensitive part of me-

* Corresponding author.
E-mail address: milad_yousefi@hotmail.com (M.Y. Valandar).

http://dx.doi.org/10.1016/j.jisa.2017.04.004
2214-2126/

dia cover [21]. DWT (Discrete Wavelet Transform): In this kind, the cover media divides to 4 main sub bands (LL, HL, LH, and HH). The main features of the cover media are in LL, and if secret message embeds in this part, it isn't destroyed with various compression [22,23]. DFT (Discrete Fourier Transform): This transform changes each points of the input signal into two point at the output. The input signal in DFT is a combination of samples which obtained at regular intervals of time [24]. *3. Spread spectrum*: This method embeds the secret message in cover media's noises which created in image acquisition process. This method is a blind scheme and there is payload capacity in this type [25,26]. *4. Model based*: This method divides cover media to two parts. First part will not use during the embedding process. The secret message embeds in second part without changing the cover media's statistical properties. High embedding capacity is one of this method advantages [27].

Increase the size of the secret message in embedding process and high resistance against various known attacks, are some benefits of transform domain. Rise of embedding and extraction process time by the increasing size of cover media or the secret message, can also be considered this method disadvantage [28]. With increasing data security, types of steganography methods have been proposed. Generally, Some of these methods are based on chaotic maps and some of them based on transformation [29]. Briefly, we introduce several proposed methods in following: Lou Der-chyuan and Chen Hao hu proposed a spatial domain steganography. This method selects the group of pixels from cover image and generates a unique key for each group. These keys are used in embedding and extracting process. The proposed algorithm embeds each bits of secret message in cover image directly. Statistical results show that algorithm had high resistance against χ^2 and *RS* attacks [30].

In [31] Reza Jafari, et al.are introduced a transform domain steganography. The proposed method uses DWT in embedding and extracting process. This algorithm first applies DWT on cover image and then chooses the LL part of transform. After that, the LL part divides to 2×2 blocks and embedding process starts on these blocks. The experimental results shows the algorithm has good resistance against compressing.

Kanso and Own, in 2012 proposed a variable-sized steganography algorithm based on a single chaotic map. In this method, Chaotic map generates the sensitive bits and embeds secret message in them. This chaotic map also uses for finding secret message bits in extraction process. The simulation results show the algorithm high resistance against some steganalysis attacks and chaotic map randomness [32].

The present paper is organized as follow: Section 2 describes chaotic map. Section 3 introduces integer wavelet transform. The new algorithm for transform domain steganography is proposed in Section 4. The simulation results are discussed in Sections 5. Section 6 contains the comparison with similar methods and Finally Section 7 concludes the paper.

2. Chaotic map

Chaos is the behavior of the dynamical system in time. This demeanor usually occurs in discrete-time systems and it can be seen in weather, electrical circuits, fluid dynamics, mechanical systems etc [33]. The main characteristic of chaos is sensitivity to initial conditions and very small changes in the input can cause large changes in the output. This feature has caused that chaotic methods to be used in the most information hiding techniques. Chaotic maps are used for exhibit chaotic behavior, and these maps can be parameterized by initial variables [34].

2.1. Modified logistic map

Logistic map is one of the well known map which used in many data hiding methods. This map is simple and very fast but it has short key space [35]. This map is defined by:

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

where x_n is initial condition and r is control parameter. Variable x_n is a number in interval [0,1] and variable r is in interval [0,4]. The following map introduces for increasing key space in logistic map. Key space is very important factor in proposed methods security and in most papers authors try to increase key space [36]. The present paper uses logistic map in steganography and improves the key space problem in logistic map. First, we generate three equation form logistic map and introduce them by:

$$f(x_n) = x_{n+1} = rx_n(1 - x_n) \tag{2}$$

$$f(y_n) = y_{n+1} = ry_n(1 - y_n) \tag{3}$$

$$f(z_n) = z_{n+1} = rz_n(1 - z_n) \tag{4}$$

we add three variables (α, β, γ) to increase the key space and mix these three equation with each other in the following:

$$\begin{cases} x_{n+1} \equiv \left[\dfrac{\alpha \times f(x_n)}{f(y_n)}\right] \mod 1 \\ y_{n+1} \equiv \left[\dfrac{\beta \times f(y_n)}{f(z_n)}\right] \mod 1 \\ z_{n+1} \equiv \left[\dfrac{\gamma \times f(z_n)}{f(x_n)}\right] \mod 1 \end{cases} \tag{5}$$

By performing final changes, the equation that used in this paper is:

$$\phi(x_0, y_0, z_0, \alpha, \beta, \gamma) = \begin{cases} x_{n+1} \equiv \left[\dfrac{\alpha \times x_n(1 - x_n)}{y_n(1 - y_n)}\right] \mod 1 \\ y_{n+1} \equiv \left[\dfrac{\beta \times y_n(1 - y_n)}{z_n(1 - z_n)}\right] \mod 1 \\ z_{n+1} \equiv \left[\dfrac{\gamma \times z_n(1 - z_n)}{(x_n(1 - x_n)}\right] \mod 1 \end{cases} \tag{6}$$

where x_n, y_n, z_n are initial conditions and α, β, γ are control parameters. Initial conditions are between [0, 1] and control parameters are in the interval [0.5, 4]. These variables are links to each other and any changes in one of them influences entire map. In this equation, x and y are the coordination of pixel and z is pixel color channel. The statistical tests suite (NIST, DIEHARD, ENT) results showed that proposed method is fully random and very sensitive to changes. These tests results are providing in section experimental result.

3. Integer wavelet transform

During the last few years, wavelet transform has become to the powerful tool in image noise reduction, compression and encoding. Haar wavelet transform is one of the most well-known transform in this field [37]. Compatibility with real signals, ease of use and low computational complexity are this transform features. The Haar wavelet transform problem is non-smooth signals that they generated when this transform applied on digital images. In this case, extraction of secure message bits cannot be done properly but image processing schemes have used lifting scheme to solve this problem.

Please cite this article as: M.Y. Valandar et al., A new transform domain steganography based on modified logistic chaotic map for color images, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.04.004