Computers and Electrical Engineering 000 (2018) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Chaotic system-based secure data hiding scheme with high embedding capacity☆

Gyan Singh Yadav*, Aparajita Ojha

Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing Jabalpur, Jabalpur, Madhya Pradesh 482005, India

ARTICLE INFO

Article history:
Received 5 March 2017
Revised 13 February 2018
Accepted 13 February 2018
Available online xxx

Keywords:
Steganographic method
Chaotic map
Data security
Imperceptibility

ABSTRACT

In recent years, data hiding has emerged as one of the main research areas in digital security. There are plenty of schemes to hide the secret data into the least significant bit planes of an image. Most of them either traverse the image pixels according to the scanning methods or using some structural fixed patterns. Researchers have proposed data hiding techniques with an orientation of hiding the content of the information, but algorithms are known publicly. Hence, the secret data is prone to be revealed easily. To provide higher security, several methods have been proposed that determine data hiding locations using certain patterns/formula. Chaotic systems have also been effectively utilized to devise secret key based data hiding algorithms. This alleviates the problem of easy retrieval even if the embedding algorithm is known. The present paper proposes a chaotic system based data hiding scheme that provides high payload as well as imperceptibility. In addition, the scheme exhibits excellent performance in terms of data security.

1. Introduction

Growing complexities in networks and sophistication in communication technologies have led to the development of data hiding in multimedia contents. Data hiding in images has been one of the most common techniques over the last two decades with applications in copyright protection, authentication etc. The image that is used to hide the data is called the cover image and the image after data embedding is called the stego image. Embedding the secret data results in distortion of the cover image, hence the data becomes susceptible to attacks. Therefore, quality of the stego image is given due importance in applying such techniques, inter-alia other aspects such as security and payload. Many data hiding schemes have been introduced keeping a good balance between imperceptibility, data security and embedding capacity. Some schemes focus on data embedding capacity and others pay more attention to image quality and security of embedded data. Researchers have used different mathematical methods, image properties and operations on secret data to accomplish their objectives. Inspite of enormous growth in the field, maintaining a balance between payload, imperceptibility and security remains a challenge.

Most of the existing algorithms concentrate on the basic trade of data hiding and retrieval algorithms. Analysis of such schemes revolves around imperceptibility and payload and such schemes are known publicly. Therefore use of such

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez-Perez.

* Corresponding author.
E-mail address: gyanu2005@gmail.com (G.S. Yadav).

https://doi.org/10.1016/j.compeleceng.2018.02.022
0045-7906/

schemes keeps the secret data secure as long as the algorithm is not known to eavesdroppers. Once the information is revealed as to which algorithm is being used, such schemes remain no longer secure. Keeping this in mind several schemes based on secret keys have been proposed in recent years (see for example, [1–6,18,19] and references therein). One such scheme is recently proposed by Wu et al. [3]. The key is employed to generate data embedding patterns. The larger the size of the secret data, higher is the overhead of sharing the pattern. To overcome this problem of sharing the pattern map, an improved scheme is proposed in the present paper, in which embedding pattern is generated using a secret key based on chaos. Instead of generating location with the help of fixed pattern map as in the magic cube based scheme [3], data embedding locations are generated with the help of a logistic map. The whole process is elaborated in Algorithms 1 and 2. Key sensitivity analysis shows that the scheme provides higher security and resists most of the conventional attacks. Further, a comparison of payload, imperceptibility and RS-analysis shows that the scheme is comparable to the existing schemes.

The paper is organized as follows. In Section 2 we give a brief overview of some of the related works. In addition, a logistic map is introduced that is used in the present work. Section 3 presents a detailed account of the proposed scheme. Section 4 is devoted to analysis of results in term of payload, imperceptibility and security of the algorithm. Section 5 presents the concluding remarks.

2. Related work

In this section, we give a brief description of some of the related data hiding schemes that form a background for the present work. In addition, we present the definition of a logistic map that will be used in the present work for data embedding. We begin with the scheme proposed by Zhang and Wang [7].

2.1. Exploiting modification direction [7]

Zhang and Wang [7] have proposed a data hiding scheme by exploiting modification direction (EMD) [7]. The scheme exploits all the possible directions of pixel modifications in the cover image for data embedding. Cover image pixels are randomly permuted using a secret key, and then are grouped into n-pixels to form a sequence. Data embedding and extraction is performed using the following extraction function.

$$f(c_1, c_2, c_3, \ldots, c_n) = \sum_{i=1}^{n} (c_i.i), \tag{1}$$

where c_i is the intensity value of the ith pixel in a pixel group of $c_1, c_2, \ldots, c_n$. To illustrate the method, let us consider the following example.

If we take $n = 2$ (group of two pixels), $5 - ary$ secret data will be embedded in two adjacent pixels out of which one pixel will be modified. To further enhance the embedding capacity, Kuo et al. [8] have introduced a generalized exploiting modification direction method (GEMD) to embed $(n + 1)$ binary bits into n adjacent pixels directly. But the method can embed atmost two bits of secret data per pixel. Very recently, Kuo et al. [9] have introduced a multi-bit encoding function that helps embed upto 4.5 bpp with acceptable stego image quality showing PSNR greater than 30 dB. The method works well in two different ways, first the data embedding process is relatively less complex, and second, the method does not need any additional external information to retrieve the secret data. But the method uses a brute force approach to solve the problem of overflow/underflow.

2.2. Dynamic embedding [10]

The earlier embedding techniques based on LSB replacement were static, i.e., secret bits were embedded in predetermined fixed size blocks of a cover image. Also, the secret data was not evenly distributed in the whole cover image. So the image quality of the secret image was prone to be affected more. Keeping this in view, Eslami and Ahmadabadi [10] proposed a scheme to improve the visual quality by introducing the concept of dynamic embedding. The process of dynamic embedding is as follows.

Suppose there are fixed size chunks of data $D_1, D_2, D_3, \ldots, D_l$. Consider l blocks from the cover image C with the block size BS given by $BS = \lfloor |C|/l \rfloor$ where $|C|$ represents the number of pixels in C. Now embed the ith chunk of data D_i in the LSB planes of the corresponding ith block of the cover image.

The method proposed by Eslami and Ahmdabadi [10] is able to distribute the payload in the entire image, and hence provides better visual quality of the stego image. However, there is no connection between the secret data block size and pixel block size which may lead to inconsistency in data distribution over the image. For example, if the data block size is small, and pixel block size is relative large, the secret data will be distributed in small chunks of pixel blocks throughout the image space, without any proper embedding rule. So the image space is not efficiently utilized for optimum data embedding.

2.3. Gene based embedding [2]

The traditional data hiding techniques were intended to hide the content only, if somehow an eavesdropper comes to know that some information is being transferred through the media then it can be easily detected. So, to overcome this

Please cite this article as: G.S. Yadav, A. Ojha, Chaotic system-based secure data hiding scheme with high embedding capacity, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.02.022