Computers and Electrical Engineering 000 (2015) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A steganographic method using Bernoulli's chaotic maps☆

Ricardo Francisco Martínez-González [a,*], José Alejandro Díaz-Méndez [b], Leonardo Palacios-Luengas [c], Juan López-Hernández [d], Rubén Vázquez-Medina [c,e]

[a] Electrics and Electronics Department, Instituto Tecnológico de Veracruz, No. 2779, Miguel Ángel de Quevedo, Veracruz, México
[b] Electronics Department, Instituto Nacional de Astrofísica, Óptica y Electrónica, No. 1, Luis Enrique Erro, Puebla, México
[c] ESIME Culhuacan, Instituto Politécnico Nacional, No. 1000, Santa Ana, Distrito Federal, México
[d] Universidad Politécnica de Victoria, No. 5902, Nuevas Tecnologías, Tamaulipas, México
[e] CMP+L, Instituto Politécnico Nacional, Acueducto, Distrito Federal, México

ARTICLE INFO

Article history:
Received 9 June 2015
Revised 29 November 2015
Accepted 1 December 2015
Available online xxx

Keywords:
Steganographic method
Bernoulli map
Pixel substitution
Statistical analysis

ABSTRACT

This paper proposes an alternative for building a data hiding algorithm into digital images. The method is based on chaos theory and the least significant bit technique for embedding a secret message in a image. Specifically the Bernoulli's chaotic maps are used, to perform the following processes: (i) encrypt the bits of the message before embedding them into the cover image, (ii) a random selection of the image's compositions (*R*,*G* or *B*) must be performed and the insertion of the secret message in a random way to (iii) rows and (iv) columns of the image. Several experimental results are shown under different evaluation criteria, such as entropy, autocorrelation, homogeneity, contrast, energy, peak signal-to-noise ratio, mean squared error and maximum absolute squared deviation. Experimental results show a good improvement in the peak-signal-to-noise-ratio and Image Fidelity value of the proposed algorithm in comparison to the results obtained from similar algorithms.

1. Introduction

The internet has caused a substantial increment in data transmission; such data can be important information for social security or bank account numbers, as well as other sensitive information that can be used by swindlers. Many cryptographic [1] and steganographic techniques [2] have been developed to reduce the data vulnerability, these techniques may add the following attributes to the information.

- **Confidentiality,** which refers to the addition of a restriction attribute in the sensitive information that is used to limit the information access only to authorized users.
- **Integrity,** which is the added attribute that allows identifying when sensitive information has been modified.
- **Non-repudiation** is the attribute in the sensitive information that allows verifying when an information sender or receiver denies the information that is communicated.
- **Authentication** allows confirming the identities of the information sender and receiver in the communication proces s.

The modern steganographic techniques are used to provide secrecy in communication by building subliminal channels to hide information into a cover digital media. These techniques are used to satisfy the insecure scenarios defined by the prisoners'

☆ Reviews processed and approved for publication by the Editor-in-Chief Dr. M. Malek.

* Corresponding author. Tel.: +522 221860863.
E-mail address: imag007@hotmail.com, imag@itver.edu.mx (R.F. Martínez-González).

http://dx.doi.org/10.1016/j.compeleceng.2015.12.005
0045-7906/

dilemma established by Simmons in 1983 [3]. On other hand, the cryptographic communication arouses suspicion that there is something important in the communications channel, meanwhile the steganographic communication goes unnoticed. The most important feature that a steganographic scheme should possess is statistical undetectability. In other words, the observer of the communication process should not be able to distinguish between a cover and its respective steganogram. The formal description of this requirement in information-theoretic terms was developed by Cachin in 1998 [4]. The use of steganographic techniques was reconsidered in protection systems in 1996, when the low bit coding, phase coding and spread spectrum techniques were studied by Bender [5] to hide data into digital media with minimal degradation. There is a large variety of techniques to hide secret information in images; some of them are more complex than the others, and all of them have strong and weak aspects. There are several approaches to classify the steganographic techniques [6]. For example, the type of cover used for a subliminal communication can be used, but the cover modifications applied in the embedding process are another possibility. In this work, the last criterion has been used, and then the classification of steganography techniques based on the cover modifications applied by some embedding process can be as follows:

(a) **Least significant bit method (*LSB*).** This approach is simple because the least significant bits of some bytes inside an image are replaced with bits of the message to be hidden. In some cases *LSB* of pixels visited in random areas of image. Some examples of this approach can be reviewed in [7,8]. These techniques are realized in the image spatial domain.
(b) **Transform domain techniques.** This approach embeds secret information in a transformed space of the signal (e. g. in the frequency domain). The significant areas of the cover image are used to hide messages. These techniques are more robust to attacks such as compression, cropping and some image processing compared to *LSB* techniques. A novel technique named DeRand (Data embedding in Random domain) has been used to embed information increment or decrement the value of the pixels randomly selected; DeRand techniques define redundancy in any digital signal by applying the universal parser such that the high entropy random signal can be used for data embedding [9,10].
(c) **Spread spectrum techniques.** This approach adopts ideas and concepts from spread spectrum communication systems [11,12].
(d) **Statistical methods.** This approach embeds information by changing several statistical properties of a cover and use hypothesis testing in the extraction process [13].
(e) **Distortion techniques.** This approach embeds information by distorting a signal and measuring the deviation from the original cover in the extraction step [14,15].
(f) **Cover generation methods.** This approach embeds information in the way a cover for secret communication is created. Some examples of this approach can be reviewed in [16].

The implementation of steganography techniques can include different mathematic concepts and tools. In particular, steganography techniques that use Chaos Theory are emerging [17,18]. Chaotic systems are attractive in security information because they are nonlinear systems characterized by high sensitivity to initial conditions and control, unpredictability, ergodicity and mixing properties, and then they can produce deterministic signals with random appearance suitable in the design of steganographic algorithms. Specifically, this work is focused on the techniques that use one-dimensional chaotic maps [19,20]. In this work, the steganographic method proposed is based on Bernoulli chaotic maps. This chaotic map is simpler than the *TD-ERCS*, and *NCA* chaotic maps used by Anees et al. [20] and the obtained results are similar to the results produced by Anees's algorithm. Additionally, Bernoulli's chaotic map is a piece-wise-linear (*PWL*) chaotic map that has no stability islands inside its chaotic region as it occurs with the logistic map; therefore, its control parameter can be modified into a specific interval in (0,1) of the real numbers. This map can generate pseudorandom sequences with statistical distributions very close to uniform distribution. The proposed algorithm uses the *LSB* technique for data hiding, which is a simple and straightforward technique that also has the advantage of embedding more information than the transform techniques keeping the texture of digital image almost unaffected. The problem with spatial techniques is the low robustness against statistical analysis and differential attacks. In this paper, three Bernoulli chaotic maps are used to propose a chaotic steganography algorithm in the spatial domain that exhibits good statistical features, and it has security conditions against different attacks. Furthermore, the proposed algorithm has a previous stage of chaotic encryption to modify the statistical characteristics of the message that is intended to hide. Also, in this previous stage a Bernoulli's chaotic map is used.

This paper is organized as follow: The mathematical model Bernoulli's chaotic map is given in Section 2, the structure of the proposed method is presented in Section 3, simulations results analysis are provided in Section 4, a comparison with similar algorithms are provided in Section 5 and finally in Section 6 the conclusions are presented.

2. Mathematical model of used Bernoulli's map

The Bernoulli map, also known as dyadic transformation, can be defined as an iterated map of the *PWL* function according to Eq. (1).

$$f(x) = \begin{cases} 2\mu x, & 0 \le x < 0.5 \\ 2\mu x - 1, & 0.5 \le x < 1' \end{cases} \tag{1}$$

where $x \in (0, 1)$ and $\mu \in (0, 1)$.

Please cite this article as: R.F. Martínez-González et al., A steganographic method using Bernoulli's chaotic maps, Computers and Electrical Engineering (2015), http://dx.doi.org/10.1016/j.compeleceng.2015.12.005