Commun Nonlinear Sci Numer Simulat 19 (2014) 1898–1907

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A robust chaotic algorithm for digital image steganography

M. Ghebleh *, A. Kanso

Department of Mathematics, Faculty of Science, Kuwait University, Kuwait

ARTICLE INFO

Article history:
Received 24 September 2012
Accepted 17 October 2013
Available online 30 October 2013

Keywords:
Steganography
Discrete wavelet transform
Lifting scheme
Chaos

ABSTRACT

This paper proposes a new robust chaotic algorithm for digital image steganography based on a 3-dimensional chaotic cat map and lifted discrete wavelet transforms. The irregular outputs of the cat map are used to embed a secret message in a digital cover image. Discrete wavelet transforms are used to provide robustness. Sweldens' lifting scheme is applied to ensure integer-to-integer transforms, thus improving the robustness of the algorithm. The suggested scheme is fast, efficient and flexible. Empirical results are presented to showcase the satisfactory performance of our proposed steganographic scheme in terms of its effectiveness (imperceptibility and security) and feasibility. Comparison with some existing transform domain steganographic schemes is also presented.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

With the advancement in Internet technologies, digital media such as images, audio, video and text are shared and transmitted over the Internet more conveniently. However, one of the major challenges in sharing and transmitting any type of information over a public channel is data security. Therefore, some means of protecting the transmitted information against an eavesdropper and an unauthorized party becomes a necessity. Cryptography and steganography are two tools for offering data security. Cryptography provides features such as confidentiality, authenticity, non-repudiation, and integrity of data. For example, confidentiality is achieved via an encryption algorithm which scrambles/mixes the private information so that it becomes unreadable to any party other than the intended recipient. In particular, in a cryptographic application, an eavesdropper/unauthorized party is aware of the existence of the private information, and his challenge is to decipher the encrypted information. On the other hand, steganography provides data security by hiding the information in a cover medium so that even the existence of a hidden message is not known to an intruder. The cover medium, usually referred to as cover, host or carrier, may be any digital medium such as an image, audio, or video file. Digital images are widely used as carriers of hidden information because of the high level of redundancy in them which is caused by the low sensitivity of the human visual system to details. Following the notation proposed in [1], in an image steganography application, we refer to the image used for hiding a secret message as the cover image, and we call an image carrying a hidden message as a stego-image. The hidden message may be of any type such as text, image, audio, or video. The main challenge in steganographic applications is that the message must be hidden in the cover image in such a way that the generated stego-image does not deviate much from the original image, visually and statistically.

A large number of image steganographic techniques have appeared in the literature, for example [2–15]. These techniques can be divided into two main classes: spatial domain and transform domain techniques. In spatial domain techniques, private message is embedded in the intensity of image pixels directly [2,5,6,8]. In transform domain techniques, the private message is embedded in the cover by modifying coefficients in a transform domain. Discrete Fourier Transform (DFT),

* Corresponding author. Tel.: +965 2481 5351.
E-mail addresses: mamad@sci.kuniv.edu.kw (M. Ghebleh), akanso@sci.kuniv.edu.kw (A. Kanso).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.10.014

Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are most commonly used in these applications [3,7,9–15]. Due to their simplicity and speed, spatial domain techniques, and in particular least significant bit (LSB) replacement techniques [2,5,6,8] are widely used for steganographic applications. In LSB-based spatial domain techniques, the information bits are embedded directly in the host image by altering the least significant bits of selected pixels. However, LSB replacement techniques are vulnerable to statistical analysis, as well as slight manipulations of the stego-image. For example, an attacker can destroy the hidden information by simply zeroing out the least significant bits of all pixels in the stego-image. On the other hand, several steganalysis methods against LSB replacement algorithms have been suggested and shown to be effective. Among these techniques are the Chi-squared test [16,17], RS-analysis [18], sample pairs analysis [19], weighted stego analysis [20], and structural steganalysis [21,22]. In contrast, transform domain steganographic techniques possess a higher level of security, and in particular they generally resist the aforementioned steganalytic methods, since they hide the private information more thoroughly [23,24].

A common drawback of using DCT- and DWT-based techniques is the loss of information due to rounding (when the inverse transform is applied). For DWT-based techniques, one may overcome this issue using Sweldens' lifting technique [25]. A lifted wavelet transform (LWT) guarantees integer to integer mapping in forward and inverse transformations. A number of LWT-based steganographic techniques are proposed in [9,14,26–28].

In this paper, we propose an LWT-based steganographic technique that uses a 3D chaotic cat map. A detailed description of the proposed algorithm is given in Section 2. Experimental results showcasing performance and security of the proposed algorithm are presented in Section 3. Some concluding remarks are given in Section 4.

2. The proposed algorithm

The steganographic scheme proposed in this article embeds a binary message in pseudo-randomly selected detail coefficients of a cover image, according to a discrete wavelet transform. This helps imperceptibility since the more significant coefficients of the cover image are not altered. On the other hand, the use of a DWT results in relative robustness against steganalytic attacks as well as some image processing filters such as JPEG2000 compression. For improved imperceptibility and security, the proposed algorithm is designed to be edge adaptive. That is, a larger alteration of values is allowed at the edges of the image where it will be less visible to the human visual system. The general assumption of a binary message results in versatility of the proposed algorithm since the message can be a text file, an image, audio, video, or any other digital content, as long as it is represented as a stream of bits. Moreover, compression filters such as Huffman coding may be applied to the message for higher capacity. Similarly, although when its parameters are chosen properly the proposed algorithm is loss-less, error correcting codes may be used for improved robustness. In the following subsections, we present the proposed algorithm in more detail. A pseudo-code of the algorithm is given in Fig. 1.

2.1. The embedding algorithm

We assume an 8-bit RGB cover image with even dimensions $2m \times 2n$. If one or both dimensions of the cover image are odd, one may simply exclude one row and/or one column of the cover from the embedding process. For imperceptibility, we use a discrete wavelet transform to ensure the embedding of the message in less significant components of the cover. Due to its simplicity, the Haar wavelet is used. Furthermore, to avoid loss of information caused by rounding errors, we employ the

1 Read an RGB cover image C of size $2m \times 2n$, and a binary message $M = M_1 M_2 \cdots M_L$ of length L.
2 Let $C' = \text{round}\left(\lambda + \frac{\mu - \lambda}{255} C\right)$, where $\lambda = 5$ and $\mu = 250$.
3 Apply a 2D LWT to each RGB channel of C' to obtain the coefficients A^R, A^G, A^B and D^R, D^G, D^B.
4 Populate an array P of length $N = 9(m-2)(n-2)$ with all 4–tuples (c, i, j, k) such that
$c \in \{R, G, B\}$, $2 \leqslant i \leqslant m-2$, $2 \leqslant j \leqslant n-2$, and $1 \leqslant k \leqslant 3$.
5 Generate a pseudo-random sequence $\xi_1, \xi_2, \ldots, \xi_N$ according to the pseudo-code in Figure 2.
6 Let π be a permutation which sorts the sequence $\xi_1, \xi_2, \ldots, \xi_N$, and apply π to P to obtain P'.
7 For t from 1 up to L
8 Let (c, i, j, k) denote the t–th entry in P', and let $d = D^c_{ijk}$.
9 Compute q according to the equations 1 and 2.
10 Let d' be obtained from d by setting its q–th bit to $M_t \oplus d_8$.
(Here d_8 is the most significant bit of d, and $\oplus$ denotes xor.)
11 Set D^c_{ijk} equal to d'.
12 End
13 Let $\Delta^R, \Delta^G, \Delta^B$ denote the modified arrays D^R, D^G, D^B.
14 Apply inverse 2D LWTs to A^R, A^G, A^B and $\Delta^R, \Delta^G, \Delta^B$ to obtain the stego-image S.
15 Return S.

Fig. 1. The proposed steganography algorithm.

Download English Version:

https://daneshyari.com/en/article/755790

Download Persian Version:

https://daneshyari.com/article/755790

Daneshyari.com