Int. J. Electron. Commun. (AEÜ) 69 (2015) 242–245

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

REGULAR PAPER

A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection

Marco Botta[a], Davide Cavagnino[a], Victor Pomponiu[b,*]

[a] Department of Computer Science, Università degli Studi di Torino, 10149 Torino, Italy
[b] Information Systems Technology and Design, Singapore University of Technology and Design, 138682, Singapore

ARTICLE INFO

Article history:
Received 16 September 2013
Accepted 12 September 2014

Keywords:
Fragile watermarking
Content authentication
Arnold cat map
Logistic map
Security

ABSTRACT

In this paper we show that a recently proposed fragile watermarking scheme by Rawat et al. does not detect and localize tampering, therefore cannot be used for authentication applications. The problem lies in that the scheme embeds an authentication code into the LSBs of pixels without taking into consideration the image content. To overcome this issue the authentication should be combined with the first seven bits of the image pixels, and in this paper a revision in this sense is proposed.

1. Introduction

These days witnessed the predominance of digital images thanks to the development of affordable digital cameras and high-speed Internet. Nevertheless, concerns with respect to the origin and integrity of digital images have raised and received increasing attention since their content can be easily manipulated and edited.

The study of *fragile image watermarking* aims at addressing these issues by answering questions about the authenticity of digital images, localization of the tampered areas and, in some cases, the capacity to recover them. In order to achieve these goals, a fragile watermark (which cannot survive to any content alterations) is embedded into the image.

In the last years numerous image authentication techniques have been devised in pixel domain [1,2] and transform domain, e.g., the Karhunen–Loève transform [3,4]. Soft computing techniques [5] have been extensively used to improve the efficiency of the watermarking schemes [6–8].

Security of the watermarking schemes [9–12] is another important feature resulting from applications where there exist adversaries willing to bypass watermarking properties such as copyright and integrity protection.

The outline of this paper is as follows: in the next section, we briefly review several concepts of the chaos theory. In Section 3, we describe the unsecure fragile watermarking scheme proposed by Rawat et al. [8] while in Section 4 we present our attack and other remarks on the scheme. Section 5 concludes this paper.

2. Background

Prior to describing the fragile watermarking algorithm introduced by Rawat et al. [8], we firstly present its main feature, the chaotic maps.

2.1. Chaotic maps

Chaotic maps, such as the Arnold cat map and the logistic map, are widely used for encryption and data hiding applications since they provide a high sensitivity to initial conditions [5].

The Arnold cat map is a two-dimensional invertible map which simply illustrates the principles of chaos. For instance, if the Arnold cat map is applied on an image I of size $m \times n$ then its pixel positions are randomized by the following relation:

$$\begin{bmatrix} p_i(x+1) \\ p_i(y+1) \end{bmatrix} = \begin{bmatrix} 1 & \alpha \\ \beta & \alpha\beta+1 \end{bmatrix} \cdot \begin{bmatrix} p_i(x) \\ p_i(y) \end{bmatrix} \text{mod} n = \Delta \begin{bmatrix} p_i(x) \\ p_i(y) \end{bmatrix} \text{mod} n \tag{1}$$

where $0 \leq i \leq n-1$, $p_i(x)$ and $p_i(y)$ denote the coordinates (x, y) of the pixel p_i, mod is the modulo operator, α and β are two positive integers that characterize the phase space, and $\det(\Delta) = 1$.

[*] Corresponding author.
E-mail addresses: marco.botta@unito.it (M. Botta), davide.cavagnino@unito.it (D. Cavagnino), victor.pomponiu@ieee.org, victor.pomponiu@gmail.com (V. Pomponiu).

http://dx.doi.org/10.1016/j.aeue.2014.09.004
1434-8411/© 2014 Published by Elsevier GmbH.

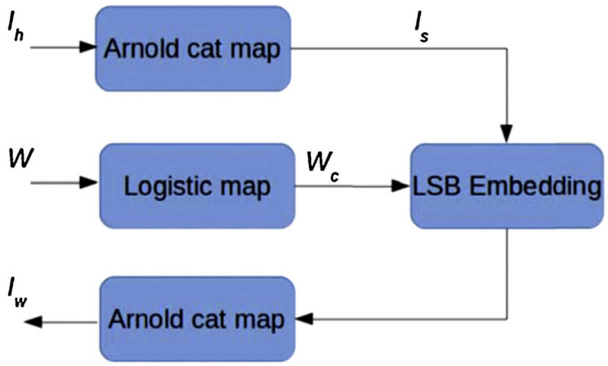

Fig. 1. The embedding procedure.

Due to the restriction imposed to the parameters α and β, the Arnold cat map becomes periodic, i.e., if the pixel p_i at location (x, y) returns to its original position after applying T times the Arnold map, then the chaotic map has period T. It is worth to point out that the period of the map is closely related to parameters α and β, and to the size of the image.

Another instance of the chaotic maps is the logistic map, which is obtained by the following relation:

$$p_i(x+1) = \mu p_i(x)(1 - p_i(x)) \qquad (2)$$

where $0 < \mu \leq 4$. If $3.5699456 < \mu \leq 4$, then the logistic map becomes chaotic. In this state, the sequences generated have a high sensitivity to the initial conditions.

Rawat et al. [8] algorithm makes use of the Arnold cat map to shuffle the pixel positions of the host image, and of the logistic map to encrypt the watermark sequence.

3. A chaotic system based fragile watermarking scheme

The fragile watermarking scheme proposed by Rawat et al. [8] can be summarized as follows:

E1. By employing the Arnold cat map k times, shuffle the host image I_h, of size $m \times n$, to obtain the image I_s.
E2. Split each pixel of I_s into 8-bits planes.
E3. By means of a logistic map create a chaotic sequence C, of the same size as I_h. Further, the values of C are rounded off to obtain an integer chaotic sequence.
E4. Compute the binary chaotic watermark W_c as:

$$W_c = W \oplus C \qquad (3)$$

where W represents the original watermark and $\oplus$ denotes the Boolean exclusive-or operation.
E5. Substitute the LSB of each pixel of I_s with the bits of W_c.
E6. To obtain the watermarked image I_w apply the Arnold cat map $T - k$ times, where T denotes the period of the chaotic map.

A block diagram illustration of the embedding process is presented in Fig. 1.

The process of extracting the watermark is as follows:

D1. Shuffle the watermarked image I_w, via the Arnold cat map p times to obtain I_{ws}.
D2. Split each pixel of I_{ws} into 8-bits planes.
D3. As done in the embedding process, generate the chaotic sequence C and round off each of its values.
D4. To recover the watermark the XOR operation is applied between the LSBs of I_{ws} and the chaotic sequence C.

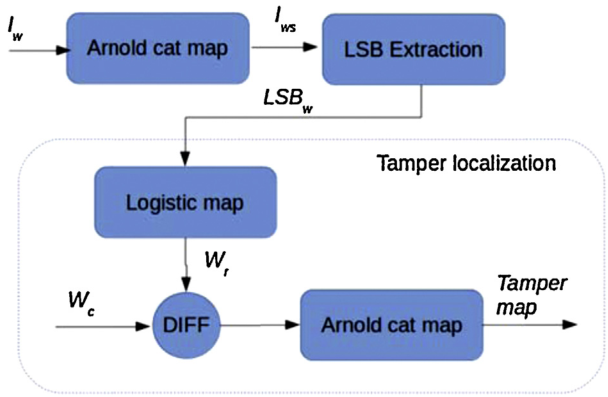

Fig. 2. The watermark extraction and verification procedures.

A block diagram illustration of the extraction and verification procedures is presented in Fig. 2.

To localize the tampered regions, within the watermarked image I_w, perform the absolute difference between the original and the extracted watermark, followed by the Arnold cat map $T - k$ times.

4. The proposed attack

The security analysis adopted follows a cryptanalytic approach: the watermarking algorithm is assumed to be public while the security relies only on the Arnold cat map and the chaotic sequence which are used to watermark the media contents. The adversary, using the devised attack, will aim to tamper the integrity of the watermarked content without leaving any traces and thus circumventing the watermarking verification procedure.

Before describing our attack, we make some observations on this scheme.

Firstly, note that the Arnold cat map, which is employed in step E1, only changes the pixels *position* (i.e., the (x, y) coordinates) of the host image I_h. For instance, the effect of applying the Arnold cat map, with $\alpha = \beta = 1$, $k = 5$, on a 4×4 matrix is shown in Fig. 4. Therefore the 8-bits planes of each pixel remain unchanged, even if the pixel's position is shuffled by the chaotic map.

Secondly, the algorithm does not employ any interdependency between the bit planes of the marked pixels.

The key observation of the attack is to compare steps (E1–E5) and (D1–D4) to reveal the fundamental flaw of the algorithm. In step E5, only the LSBs of the shuffled pixels are *changed independently* with those of the chaotic watermark, without considering the image content [9,11]. In step D4, in order to assess the integrity of the suspicious image, the LSBs are extracted from the shuffled pixels. Therefore, we can tamper the watermarked image, while preserving the integrity of the watermark, using the following mechanism:

A1. In a matrix L, store the LSBs of all the pixels of the watermarked image I_w.
A2. Alter the pixels of the watermarked image I_w as desired.
A3. In order to reinsert the watermark, replace the LSB of each pixel with those stored in the matrix L.

In other words the attack may be restated as: freely alter all the watermarked image bit-planes apart the one of the LSBs.

We have verified the attack experimentally: an 8 bpp gray-scale image of size 256×256 pixels, taken from the OPTIMOL image collection [13], was chosen as the host image. As in [8], the watermark was a binary logo image of size 256×256 pixels. Furthermore, we set up the parameters of the Arnold cat map and logistic map to the