Int. J. Electron. Commun. (AEÜ) 65 (2011) 840–847

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.de/aeue

A chaotic system based fragile watermarking scheme for image tamper detection

Sanjay Rawat*, Balasubramanian Raman[1]

Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247 667, India

ARTICLE INFO

Article history:
Received 23 September 2010
Accepted 24 January 2011

Keywords:
Tamper detection
Chaotic map
Authentication
Digital watermarking

ABSTRACT

In the past few years, various fragile watermarking techniques have been proposed for image authentication and tamper detection. In this paper, a novel chaos based watermarking scheme for image authentication and tamper detection is proposed. Tamper localization and detection accuracy are two important aspects of the authentication watermarking schemes. Our scheme can detect any modification made to the image and can also indicate the specific locations that have been modified. To improve the security of the proposed scheme two chaotic maps are employed. Since chaotic maps are sensitive to initial values, the corresponding position relation between pixels in the watermarked image and the watermark get disturbed, which helps the watermarking scheme to withstand counterfeiting attacks. Initial values of the chaotic maps are used as secret keys in our scheme. The effectiveness of the proposed scheme is checked through a series of attacks. Experimental results demonstrate that the proposed scheme is not only secure but also achieves superior tamper detection and localization accuracy under different attacks. For instance in copy-and-paste attack and collage attack.

1. Introduction

With the rapid growth of internet technologies, a large amount of digital data is easily accessible to everyone these days. This digital data can be easily manipulated, tampered and distributed with the help of powerful image processing tools. The ease and extent of such manipulations emphasize the need for image authentication techniques in applications where verification of integrity and authenticity of the image content is essential. Therefore, various authentication schemes have recently been proposed for verifying the integrity and authenticity of the image content. The authentication schemes can be divided into two categories: digital signature based schemes and digital watermark based schemes. A digital signature can be either an encrypted or a signed hash value of image contents and/or image characteristics. The major drawback of signature based schemes is that they can detect if an image has been modified, but they cannot locate the regions where the image has been modified [1–3]. To solve this problem, many researchers have proposed watermarking based schemes for image authentication [4–7]. One of the first watermarking-based authentication schemes was proposed by Walton [9]. He divided the image into 8×8 blocks and embedded the checksum in the LSB of each block. The main drawback of Walton's scheme is that there is a possibility of exchanging the blocks with the same position in two different authenticated images without affecting the checksum of the image. Yeung and Mintzer [10] proposed a watermarking scheme for image authentication that uses a pseudo random sequence and a modified error diffusion method to embed a binary watermark into an image, so that any change in pixel values of the image can be detected. Fridrich et al. [11] analyzed the security issue in the scheme proposed by Yeung and Mintzer [10] and proposed an improved scheme with localization capability, where a block cipher defined on a local neighborhood rather than on a single pixel is used to replace the binary look-up tables. Thus, attacker could not deduce the binary look-up table. At the same time, authors embedded an image index into all non-overlapping sub-blocks of each image to prevent the collage attack proposed in [12,13]. Wong [14] proposed a public key fragile watermarking scheme for image authentication. He divided the image into non-overlapping blocks and inserted a digital signature for authentication. In his scheme, a key is used to generate a signature using the seven most significant bits of the pixels in each image block together with a logo to form a watermark, and embed the watermark into the least significant bits of the corresponding blocks. The blockwise independence of the authentication schemes, proposed in the literature was exploited by Holliman and Memon [15]. They proved that these scheme are vulnerable to vector quantization attack. According to them, a counterfeit image can be constructed using a vector quantization codebook generated from a set of watermarked images. Since each block is authenticated by itself, the counterfeit image appears authentic to the watermarking scheme. To withstand the vector quantization attack, a number of schemes has been proposed. Wong and Memon [16] proposed an improved blockwise authentication scheme by

* Corresponding author. Tel.: +91 01332 285852; fax: +91 01332 285852.
E-mail addresses: sanjudma@gmail.com (S. Rawat), balaiitr@ieee.org (B. Raman).
[1] Tel.: +91 1332 285852.

1434-8411/$ – see front matter © 2011 Elsevier GmbH. All rights reserved.
doi:10.1016/j.aeue.2011.01.016

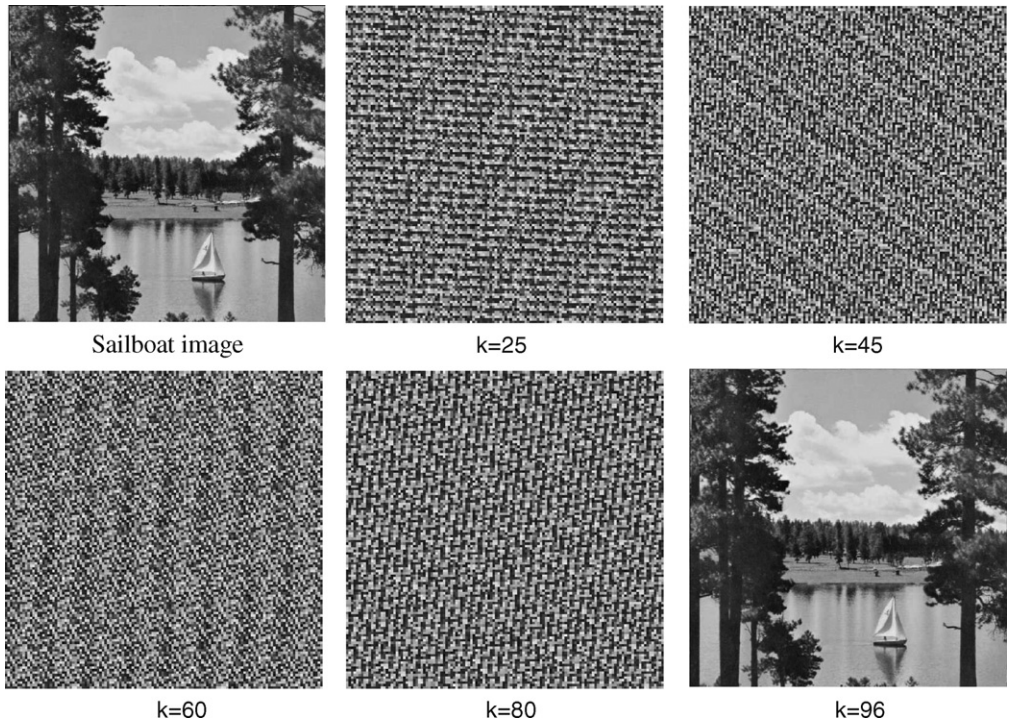

Fig. 1. Periodic phenomenon in cat map.

adding an image index and a block index to the inputs of the hash function. However, this idea works at the expense of requiring the verifier to have a priori knowledge about the image index, which limits its applicability to some extent. Celik et al. [17] proposed a hierarchically structured watermarking scheme based on Wong's scheme [14] which provides a blockwise authentication with highly overlapping blocks. In Celik et al.'s scheme, the original image is partitioned into blocks in a multi-level hierarchy and then block signatures in this hierarchy are calculated. Based on this hierarchy structure, the scheme can effectively thwart vector quantization attack. Suthaharan [18] proposed a fragile watermarking scheme in which the security against vector quantization attack is achieved using a gradient image and its bits distribution properties to generate a large key space. Chang et al. [19] proposed a block-based image authentication scheme which can withstand counterfeiting attacks by combining the local and global features to obtain the authentication data. Chen et al. [20] proposed a fuzzy c-means clustering based watermarking scheme to resist counterfeiting attacks. To break the block wise independency, they applied the fuzzy c-means clustering technique to cluster all the image blocks, so that the relationship between blocks can be created. The authentication data is embedded into two least significant bits of each image block.

In this paper, a novel watermarking scheme based on chaotic maps is proposed. The pixels of the cover image are disturbed with the help of Arnold's cat map. The image is further divided into 8-bit planes and the least significant bit (LSB) plane is used for watermark embedding. A binary logo is used as watermark in our scheme. A chaotic image pattern is generated by using logistic map. A scrambled watermark is obtained by using exclusive-or (XOR) operation between chaotic image pattern obtained by using logistic map and the binary watermark. The scrambled watermark is then embedded in the least significant bit (LSB) plane of the image. Watermarked image is obtained by performing an inverse cat map.

The rest of the paper is organized as follows. In Section 2, Arnold's cat map and logistic map are briefly described. In Section 3, the proposed watermarking scheme is explained. Experimental results are given in Section 4. Conclusions are drawn in Section 5.

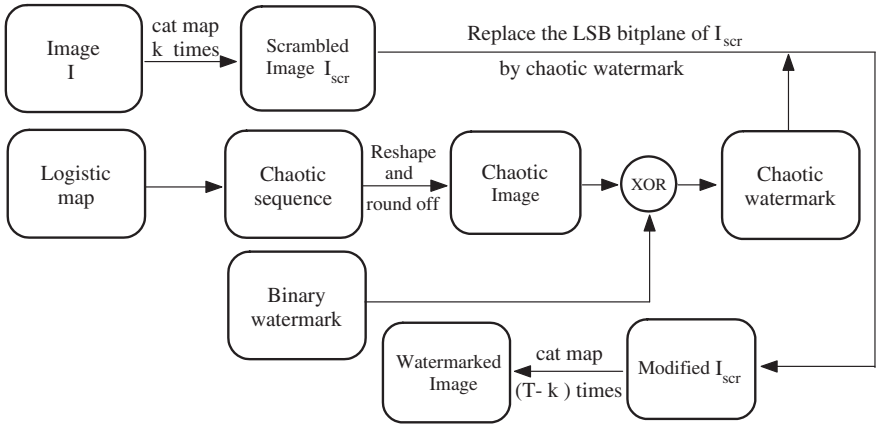

Fig. 2. Block diagram of embedding process.