Chapter 37
A Fragile Watermarking Chaotic Authentication Scheme Based on Fuzzy C-Means for Image Tamper Detection

Kamal Hamouda
Mansoura University, Egypt

Mohammed Elmogy
Mansoura University, Egypt

B. S. El-Desouky
Mansoura University, Egypt

ABSTRACT

In the last two decades, several fragile watermarking schemes have been proposed for image authentication. In this paper, a novel fragile watermarking authentication scheme based on Chaotic Maps and Fuzzy C-Means (FCM) clustering technique is proposed. In order to raise the value of the tamper localization, detection accuracy, and security of the watermarking system the hybrid technique between Chaotic maps and FCM are introduced. In addition, this scheme can be applied to any image with different sizes not only in the square or even sized images. The proposed scheme gives high values especially in security because the watermarks pass through two levels to ensure security. Firstly, The FCM clustering technique makes the watermark dependent on the plain image. Secondly, the Chaotic maps are sensitive to initial values. Experimental results show that the proposed scheme achieves superior tamper detection and localization accuracy under different attacks.

DOI: 10.4018/978-1-5225-2229-4.ch037

INTRODUCTION

By the widespread and rapid growth of the Internet technologies, people can exchange information easily and rapidly. Therefore, the protection of intellectual property rights has become increasingly important (Yeung et al., 1997). The Internet has become the place to spread digital media such as text, audio, images, and video for trade. In addition, the main engine for news reporting, intelligence information gathering and criminal investigation are digital multimedia, security surveillance, and health care. Many image processing software are developed. Therefore the digital data can be easily manipulated, tampered, and distributed with the help of the powerful image processing tools. The digital multimedia authentication and copyright have become an important issue. Therefore, we should know the meaning of information hiding (Mintzer et al., 1997).

On the other side, cryptography, steganography, and watermarking are considered the fundamental methods of information hiding and copyright protection (Gaber & Zhang, 2012, Gaber et al., 2013). Cryptography is the study of methods of sending messages (plain text) in a distinct form where only the intended recipients can remove the disguise and read the message (ciphertext) (Simmons, 1998). The Cryptography consists of two processes. The first is enciphering that converting a plaintext to a ciphertext. The second is the deciphering or decryption that is the reverse process. Only a person who possesses appropriate key (or keys) can decrypt the encrypted data (Diffie & Hellman, 1976). Steganography, derived from Greek, literally means "covered writing" is the art of hiding information in other data in ways that prevent the detection of hidden message (Franz et al., 1996). A Stenographic system is typically not required to be robust against the intentional removal of the hidden message (Acken, 1998). Watermarking is the process that embeds data called a watermark into media (Huang and Ye, 2012). After that, the watermark can be detected or extracted later to check if the media is tampered or not. The media may be text or image or audio or video. It provides an indication of ownership of the digital data. Watermarking techniques are particular embodiments of steganography. Any watermarking scheme/algorithm consists of three parts the watermark, the encoder, the decoder and comparator (Tong et al., 2013a).

Therefore, the digital multimedia authentication and copyright have become an important issue, so digital watermarking has been proposed (Madduma and Ramanna, 2011). For instance, 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. The digital multimedia authentication and copyright can be applied to the knowledge called digital watermarking. The Application of watermarking can be divided into two categories visible watermark and invisible watermark. There are many applications for visible watermarks such as Enhanced copyright protection and Indicate ownership originals. Also, The visible watermarks can be used in following cases Enhanced copyright protection and Indicate ownership originals. Also, Invisible watermarks find application in following cases data authentication, data hiding, copyright protection, fingerprinting, copy protection broadcast monitoring, medical safety and indexing (Craver et al., 1998).

Digital watermarking can be classified according to the invisible watermark into three different categories (Chen et al., 2013): robust, fragile, and semi-fragile watermarking. A robust digital watermarking is performed to assure that the encapsulated information cannot be destroyed during any computer attack. A fragile digital watermarking is performed to ensure that detecting the presence of alterations in the image and the encapsulated information can be easily destroyed during any malicious attacks and non-malicious attacks. In other words, a fragile watermarking can detect any modification to the image. A semi-fragile digital watermarking is like the fragile one. It can be destroyed by certain types of at-