Cryptanalysis and Improvement of a Digital Watermarking Scheme Using Chaotic Map

Musheer Ahmad, Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India
Hamed D. AlSharari, AlJouf University, AlJouf, Kingdom of Saudi Arabia

ABSTRACT

In the recent past, a new statistically efficient digital image watermarking scheme based on chaotic map was proposed. The authors of this watermarking scheme claimed under study that their scheme is efficient, secure, and highly robust against various attacks. However, the security analysis of the scheme unveils that it has serious inherent flaws. In this article, the shortcomings of the proposed watermarking scheme and cryptanalysis are presented to demonstrate that the scheme is not secure against the proposed attacks. Specifically, with the chosen host image and chosen watermarks, we can successfully recover the watermark from received watermarked image without having any knowledge of the secret key. The simulation analysis of the proposed cryptanalysis is provided to exemplify the proposed attack and lack of security of the anticipated watermarking scheme. In addition, an improved version is proposed to enhance the security performance of the watermarking scheme against possible attacks. The improved scheme tends to hold against attacks and statistical efficiency.

KEYWORDS

Chaotic Logistic Map, Cryptanalysis, Image Watermarking, Security, Statistical Efficiency

1. INTRODUCTION

Digital watermarking is a method of embedding an imperceptible watermark into a host digital media, like still images, audio signals, and video streams, such that it doesn’t perceptually degrade its quality. The goal of digital watermarking is to provide practical platforms for designing security systems to accomplish copyright protection, broadcast monitoring, tamper detection, digital fingerprinting, intellectual property protection etc. (Potdar, 2005; Bas, 2016; Lei, 2004). Watermarking systems for digital media involve two stages: namely (i) watermark embedding- to indicate copyright and (ii) watermark detection- to identify the owner (Swanson, 1998). Depending on the requirements and purpose, a practical and bonafide watermarking scheme is characterized by four properties (Cox, 2008) such as: robustness- the watermarking scheme must be capable to resist different kinds of attacks; imperceptibility- watermark is embedded in a way such that the degradation in the quality of digital media is imperceptible; capacity- it refers to the number of bits a watermark encodes within a unit of time or within a work, for an image, it would refer to the number of bits embedded within the image; and security- it refers to the fact that an un-authorized person should neither detect nor read the watermark. The watermark is viewed as a sort of a mark that uncovers the proprietor of authoritative

DOI: 10.4018/IJRSDA.2018100104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
data. The data needs to be implanted with watermarks in their media objects for copyright security, content confirmation, tamper detection and so on. A watermarking scheme securely implants an imperceptible watermark in host media information. The embedding procedure is guided by utilization of a key which chose the portions inside the data where the watermark would be implanted. Once the watermark is implanted, it may encounter a few cryptanalytic analyses by the assailants. The watermarked data needs to be prepared carefully. The assaults can be accidental (like transmission errors) or purposeful (like malicious editing). Subsequently, the watermark must be exceptionally robust against all cryptanalytic attacks from the unintended parties. When the proprietor needs to check the authenticity of watermarks in the potentially assaulted watermarked data, then it does depend on the secret key that was utilized to embed the watermark at sender side. By using key, the embedded watermark can be obtained for ensuring the authenticity, copyright and malicious activities on the multimedia data. The digital watermarking schemes are broadly divided into fragile watermarking and robust watermarking. Fragile watermarking is aimed to detect the integrity, authenticity and modifications of digital media (Zhang & Shuozhong, 2009). Whereas, the robust watermarking prevents someone to remove the watermark to determine the owner of digital media even if it is altered (Wang, 2008). Most of the multimedia applications require imperceptible, secure and robust watermarking to protect the ownership of digital media (Cox, 1996). In the last decade, a lot of digital image watermarking schemes have been proposed in the literature for content authentication, rightful ownership, copyright protection etc. (Liu, 2006; Shieh, 2006; Tao & Eskicioglu, 2004; Wang & Chen, 2007; Mohammd, 2008; Bhatnagar & Raman, 2009; Rawat & Raman, 2011; Chang, 2011; Jamal, 2013; Aslantas & Dogru, 2014; Ansari, 2016; Zhang, 2017). Contemporarily, the attempts have been also made by the researchers to analyze and assess the security of individual watermarking schemes. It has been performed with intent to arrive and design more robust, secure and efficient schemes. Consequently, the customized attacks are framed by the cryptanalysts to unveil the inherent flaws and weaknesses. It has been found that some watermarking schemes are not secure and incompetent to withstand possible attacks, as exposed by the cryptanalysts in (Das, 2005; Chou, 2007; Ting, 2008; Ting, 2009; He & Zhang, 2012; Teng, 2013; Ling, 2011; Benrhouma, 2016; Caragata, 2016; Ahmad, 2011; Sharma, 2014; Ahmad, 2015a; Ahmad, 2015b; Sharma, 2016).

(Jamal, 2013) recently proposed a chaos-based digital image watermarking scheme, here onwards we call it CBDWS. They employed the chaotic map to locate random embedding positions in host image. The statistical analyses measures illustrate the high security performance of their scheme and it was hoped that scheme can resist all possible attacks. However, a careful security analysis of the scheme reveals its inherent weaknesses, which facilitates unauthorized recovery of watermark. The main flaw of the scheme is the generation of random embedding positions is independent to the host image. It only depends on the secret key, namely the initial conditions of chaotic logistic map. As a result, the scheme will always yields the same embedding positions with same secret key, regardless of the distinct host images. In this paper, we exploit the advantage of this flaw and proposed an attack to successfully cryptanalyze the watermarking scheme under study by recovering the watermark. Moreover, the efforts are made to improve the security of CBDWS scheme. The proposed enhancements are designed to develop an improved scheme. Our improved version is creditenial enough to overcome the proposed attack and also have comparable statistical measures. This paper mainly focuses on the following contributions by the authors:

1. Firstly, a chaos based digital image watermarking scheme is scrutinized and its loopholes are highlighted;
2. A chosen-watermark attack is proposed to break the watermarking scheme to show the ineffectiveness of scheme for security applications;
3. An improved watermarking scheme is proposed with same statistical performance which has the power to thwart the above attack and other chosen-plaintext attacks.
Challenges of Meta Access Control Model Enforcement to an Increased Interoperability
www.igi-global.com/chapter/challenges-of-meta-access-control-model-enforcement-to-an-increased-interoperability/183778?camid=4v1a

Multimodality Medical Image Fusion using M-Band Wavelet and Daubechies Complex Wavelet Transform for Radiation Therapy
www.igi-global.com/article/multimodality-medical-image-fusion-using-m-band-wavelet-and-daubechies-complex-wavelet-transform-for-radiation-therapy/133530?camid=4v1a