International Journal of Information Security and Privacy
Volume 16 • Issue 1

An Imperceptible Watermarking Scheme for Medical Image Tamper Detection

Abdallah Soualmi, LRSD Lab, Computer Science Department, Faculty of Sciences, University of Setif 1, Algeria
https://orcid.org/0000-0003-2107-8598

Adel Alti, LRSD Lab, Computer Science Department, Faculty of Sciences, University of Setif 1, Algeria
https://orcid.org/0000-0001-8348-1679

Lamri Laouamer, Department of Management Information Systems, College of Business and Economics, Qassim University, Saudi Arabia

ABSTRACT

One of the important issues in the telemedicine field refers to an advanced secure communication. Digital image watermarking is an ideal solution since it protects the electronic patient's information from unauthorized access. This paper presents a novel blind fragile-based image watermarking scheme in spatial domain that merges speed up robust features (SURF) descriptor with the well-known Weber descriptors (WDs) and Arnold algorithm. It provides a good way for enhancing the image quality and time complexity for medical data integrity. Firstly, the watermark image is shuffled using Arnold chaotic map. Secondly, the SURF technique is practiced to region of interest (ROI) of the medical image and then the blocks around the SURF points are selected to insert the watermark. Finally, the watermark is encrusted and extracted using WDs. Experimental results show good image fidelity with the shortest execution time to ensure medical image integrity.

KEYWORDS

Blind Watermarking, Fragile, Image Authenticity, Image Integrity, Medical, Spatial Domain

1. INTRODUCTION

The world has witnessed an improvement in human healthcare conditions in recent years, due to continuous technological advances to improve patient safety by identifying early patient risks. However, healthcare organizations are aware of technologies when it comes to unauthorized access across unsecured networks. Disruption of health status may violate the confidentiality of sensitive secret information.

Digital watermarking techniques have emerged in recent years to contribute on security issues regarding confidentiality and integrity of medical images. A watermark can be embedded into a host image (Singh et al., 2019) to ensure image protection, content authentication, and integrity (Molina-Garcia et al., 2020; Akhtarkavan et al., 2020). Image watermarking can be classified as robust, semi-

DOI: 10.4018/IJISP.2022010102

fragile, or fragile (Liu et al., 2019; Hsu et al., 2020; Ortiz et al., 2019). The robust approaches are often used for ownership proofing where the embedded watermark should be super tough against any attempt to delete it (Nejati et al., 2019; Wang et al., 2017). In semi-fragile approaches, the watermark must deal with at least minor attacks (Hurrah et al., 2020), unlike fragile approaches where the watermark is braked after undergoing any operation (Prasad et al., 2020). Fragile and semi-fragile techniques can be used for data integrity and authenticity (Yu et al., 2019; Borah et al., 2020). Additionally, the image watermarking techniques could be classified as blind (Li et al., 2020), where the receiver could extract the embedded watermark without requiring the original watermark or the host image, Semi-blind (Horng et al., 2014) and non-blind (Li et al., 2020) where respectively the embedded watermark, host image are required to extract the watermark.

Several watermarking methods have been proposed (Haghighi et al., 2019; Molina-Garcia et al., 2020; Akhtarkavan et al., 2020; Hurrah et al., 2020; Gull et al., 2020; Bhalerao et al., 2020). Each one has its advantages and drawbacks. The study and analysis of several methods have indicated that they should be used in a secure and imperceptible manner with low computational complexity. At the same time, the receiver could check if the embedded watermarked image was altered during transmission. In healthcare, any alteration on the image content presents a serious concern due to the sensitive information in medical images; even a smooth alteration will incite incorrect interpretation from the physician. Medical images have specific features compared to other kind of images such as: *less texture*. We need to constantly consider the importance of each pixel in medical interpretation to achieve correct medical interpretation.

To overcome the challenges mentioned above, fragile watermarking techniques are widely adopted to secure medical images. In this paper, we propose a new secure and fast watermarking technique with enhanced imperceptibility for tamper detection issue. The approach combines Speed Up Robust Features (SURF) Descriptors, Weber Descriptors (WDs) and Arnold Chaotic Map (ACM), to enhance medical image quality when embedding a watermark by improving data's authenticity and providing sufficient watermark security. We benefit from multiple advantages of the powerful SURF descriptors to achieve less computational complexity while ensuring watermark recovery. The proposed approach applied WDs to both embedding and extracting processes for tamper detection, while Arnold's chaotic map is used to secure the watermark.

The rest of the paper is organized as follows: Related works are presented in section 2. The fundamental theories of the proposed approach are explained in section 3. The proposed algorithm is discussed in Section 4. Results and performance analysis are described in Section 5. Section 6 presents our conclusion and future works.

2. RELATED WORKS

Over the last years, there have been many fragile watermarking methods (Haghighi et al., 2019; Sinhal et al., 2019; Tohidi et al., 2019; Molina-Garcia et al., 2020; Akhtarkavan et al., 2020; Bhalerao et al., 2020; Hurrah et al., 2020; Gull et al., 2020). The proposed methods cover the image authentication issue and preserve the confidentiality and privacy of health data. In (Haghighi et al., 2019), the authors presented a fragile blind watermarking scheme using Lifting Wavelet Transform (LWT), Chebyshev System, and Genetic Algorithm (GA). The LWT and image blocks differencing are used for generating four compact digests. Four chances are obtained to recover 2×2 destroyed blocks. Finally, the GA is used to optimize the embedded bits for better imperceptibility. The experimental results indicated that the proposed method provides a significant improvement in terms of safeguard, tamper detection, and recovery accuracy compared to existing methods. However, the method requires high execution time.

In (Sinhal et al., 2019) authors presented a tampering detection and recovery watermarking method based on multiple LSB bit substitutions. The fragile watermark bits are embedded using random insertion. This technique shows good result in terms of altering detection accuracy and recovery, but suffering from low imperceptibility degree (i.e. less than 40 dB).