TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique

Behrouz Bolourian Haghighi, Amir Hossein Taherinia, Ahad Harati

PII: S1047-3203(17)30187-6
DOI: https://doi.org/10.1016/j.jvcir.2017.09.017
Reference: YJVCI 2066

To appear in: *J. Vis. Commun. Image R.*

Received Date: 24 December 2016
Revised Date: 3 August 2017
Accepted Date: 27 September 2017

Please cite this article as: B.B. Haghighi, A.H. Taherinia, A. Harati, TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique, *J. Vis. Commun. Image R.* (2017), doi: https://doi.org/10.1016/j.jvcir.2017.09.017

TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique

Behrouz Bolourian Haghighi[a], Amir Hossein Taherinia[a,*], Ahad Harati[a]

[a] *Computer Engineering Department, Ferdowsi University of Mashhad, Mashhad, Iran*

Abstract

This paper proposes a fragile and blind dual watermarking method for tamper detection and self-recovery. This method generates two image digests from the host image, based on the lifting wavelet and the halftoning technique. Therefore, for each 2×2 non-overlapping blocks, two chances for recovering tampered blocks is provided. Then, the authentication bit is obtained by using the image digests. Totally, eight bits are embedded in two LSBs for each block of image. To enhance the quality of the digest, a new $\text{LSB}_{\text{Rounding}}$ technique is proposed. Additionally, to determine the mapping blocks and shuffling LSBs, the Arnold Cat Map is utilized. To improve the recovery rate, a Shift-aside operation is proposed. For preventing copy-move, vector-quantization attacks, and any manipulation in LSBs, the information embedded in each block depends on the key which is assigned to it. Experimental results show the efficiency of TRLH compared to the state of the art methods.

Keywords: Data hiding, Watermarking, Tamper detection and self-recovery, Image authentication, Lifting wavelet transform, Halftoning technique.

1. Introduction

By the growth of digital technology over the past decades, and providing the ability to transcribe data in a low cost and easy access, sending and storing electronic media have been increased rapidly. Therefore, the lack of respect for copyright manipulating and using forged documents have been grown dramatically. In other words, the authenticity and accuracy of received media from different communication channels have become a major challenge [1]; Due to powerful tools for creating and editing media that it is serious threat to transfer of digital media. One of the suitable methods to deal with these challenges is watermarking [2]. Watermarking methods are presented for authenticating and verifying the integrity of digital media. Obviously, the most common of these media is image.

Digital image watermarking techniques embed watermark data like copyrights information in the host signal [2]. In other words, the watermark is a pattern of bits that embed in multimedia data such as image, audio or video for various applications. A simple example of a digital watermark can be detected by a signature or seal on an image. Embedded secret information can include text, author serial numbers, company logos, images and so on. Inserted data aims to ensure the security and reliability data, identify the owner and copyright protection in the digital data. Some applications of watermarking are as copyright protection, broadcast monitoring, data authentication, copy protection, and so on.

Watermarking methods can be classified from different aspects like below:

• **Robustness:** From this criteria watermarking techniques can be divided into three categories robust, semi-fragile, and fragile [3]. Robust watermarking [4–6], often used for digital data copyright works, and prevent the destruction of the watermark by applying common variations image, image processing operations, and lossy compression. In these methods, watermark not destroyed and still be detected, against various geometric or non-geometric operations. Semi-fragile watermarking [7, 8], able to tolerate, changing an image such as adding noise due to lossy compression. Finally, the fragile [9–11] method because of the nature of fragility, and lack of strength in the face of these attacks, they used for applications such as authentication and document content protection that should be must very sensitive to signal modification.

• **Perceptible:** If the watermark which embedded in the media can be seen, such as watermarking on paper or TV, called visible watermarking. The methods which can be embedded watermark to host, in a way that not see by the human visual system, but can design the software that can fetch it, it called invisible watermarking [1].

• **Domain:** Watermarking methods are divided into two spatial and frequency domains [1]. In the spatial domain, the watermark is embedded in the least significant bits

*Corresponding author

Email addresses: b.bolourian@stu.um.ac.ir (Behrouz Bolourian Haghighi), taherinia@um.ac.ir (Amir Hossein Taherinia), a.harati@um.ac.ir (Ahad Harati)