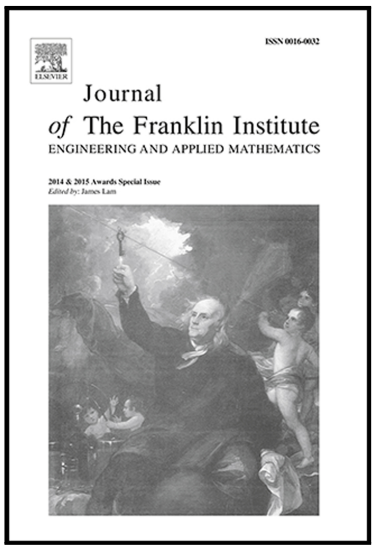

LWT-DSR based new robust framework for watermark extraction under intentional attack conditions

Vivek Singh Verma, Rajib Kumar Jha

PII: S0016-0032(17)30346-0
DOI: 10.1016/j.jfranklin.2017.07.032
Reference: FI 3071

To appear in: *Journal of the Franklin Institute*

Received date: 23 March 2016
Revised date: 27 May 2017
Accepted date: 7 July 2017

Please cite this article as: Vivek Singh Verma, Rajib Kumar Jha, LWT-DSR based new robust framework for watermark extraction under intentional attack conditions, *Journal of the Franklin Institute* (2017), doi: 10.1016/j.jfranklin.2017.07.032

LWT-DSR based new robust framework for watermark extraction under intentional attack conditions

Vivek Singh Verma[a], Rajib Kumar Jha[b]

[a]*Ajay Kumar Garg Engineering College, Ghaziabad 201009, India.*
[b]*Indian Institute of Technology Patna, Bihar, 800013, India.*

Abstract

This paper proposes a new watermarking approach using dynamic stochastic resonance (DSR) based tuning operation to extract the watermark logo from the watermarked image that has undergone different intentional and signal processing attacks. This method is intended to provide remedies from the shortcomings of the technique proposed by Lin *et al*. in 2008, and invalidates the effect of intentional attacks recently designed by Meerwald *et al*. in 2009. The algorithm incorporates three level image decomposition using lifting wavelet transform (LWT) and low-pass subband is utilized for data hiding purpose. Watermark bits are embedded into the blocks of non-overlapped wavelet coefficients of the cover image by quantizing the two maximum coefficients of the corresponding block. In watermark extraction process, the DSR is applied by performing the tuning operation on coefficient blocks of attacked watermarked image. It is a parameter dependent approach that enhances the performance of watermark extraction, where the parameters of DSR inherently depend on the image properties such as standard deviation or variance. As far as security is concerned, the randomization of wavelet coefficients, blocks, and watermark bits helps the framework to be more secure. The proposed technique is also examined against multiple watermarking attack and successfully proves its authenticity and ownership. Comparison of the proposed technique with recent techniques shows remarkable improvement in terms of robustness and security against various intentional, signal processing, and geometrical attacks.

Keywords: Blind watermarking, Lifting wavelet transform, Dynamic stochastic resonance, Significant coefficient difference, Intentional attacks.

1. Introduction

Currently, the quick advancements of the Internet and digital advances have shrewdly expanded the simplicity of the creation and distribution of digital multimedia. The most serious issue with multimedia information is to give copyright assurance on the grounds that this might be effectively copied and circulated. Digital watermarking is the most conspicuous answer for making the information exchange secure from the unlawful interference. Digital watermarking is a process of embedding unremarkable data (or signal) called as watermark into the digital content. This embedded data (or signal) is typically imperceptible (invisible) that can later be detected or extracted to prove ownership of digital content. Numerous watermarking techniques exist providing copyright protection from the contaminated environment. A review of the literature reveals that the transform domain techniques are typically more robust to various signal processing attacks as compared with spatial domain techniques [1].

Numerous watermarking techniques have also been proposed using transform domain and most of these methods analyze watermark perceptibility against various signal processing attacks (see for example, [2, 3, 4, 5, 6, 7, 8, 9]). Byun *et al*. [2] proposed a watermarking scheme based on the statistical characteristics of wavelet subbands of an input image. In this scheme, the watermark is embedded into the middle-frequency subband. However, the technique fails to achieve effective robustness against JPEG compression. Li *et al*. [3] discussed the improved blind watermarking scheme based on wavelet tree quantization. The wavelet coefficients of the original image are grouped into wavelet super trees and each watermark bit is embedded using two wavelet super trees. But, this technique is less effective against few attacks such as low-pass filtering, JPEG compression with quality factor less than 20. Later, Lin *et al*. [4] proposed a blind watermarking scheme based on quantization of the significant difference between wavelet coefficients. The two maximum wavelet coefficients in a block of size 7 are quantized using average significant difference value of all blocks, and adaptive threshold value is designed to extract the watermark. Though, this method provides more robustness against various signal processing operations, but fails to achieve robustness against intentional attacks. Recently, Meerwald *et al*. [10] presented various intentional attacks targeted to the technique designed by [4]. These attacks are designed on the basis of plentiful knowledge of the implementation details of the watermarking technique proposed by [4]. In this paper, radically three types of attacks are proposed aiming to remove the watermark from the watermarked image. And, all these attacks have successfully achieved their objective without degrading

Email addresses: viveksv10@gmail.com (Vivek Singh Verma), jharajib@gmail.com (Rajib Kumar Jha)