HOSTED BY
ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jides

Robust watermarking scheme and tamper detection based on threshold versus intensity

Lamri Laouamer[a,b,*], *Muath AlShaikh*[b], *Laurent Nana*[b], *Anca Chrisitine Pascu*[b,c]

[a] *Department of Management Information Systems, College of Business and Economics, Qassim University, P.O. Box 6633, Buraydah, 51452, Saudi Arabia*
[b] *Lab-STICC (UMR CNRS 6285), University of Western Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS 93837, 29238 Brest Cedex, France*
[c] *Faculty of Lettres, University of Western Brittany, Brest CS 93837, 29238 Brest Cedex, France*

ARTICLE INFO

Article history:
Received 24 September 2015
Received in revised form
25 October 2015
Accepted 25 October 2015
Published online 10 November 2015

Keywords:
Image watermarking
Attacks
Robustness
Tamper detection

ABSTRACT

A watermarking field is necessary to prove the copyright, ownership, authenticity and other related security aspects of the electronic data. Semi-Blind watermarking refers to need the watermark image during the extraction process. While, informed watermarking generates the watermark data from the original image itself. Moreover, Tamper detection is useful to discover the tamper zone in the image. In this paper, we propose a semi blind and informed watermarking approach. We build the watermark from the original image using Weber Law. Our approach aims to provide a high robustness and imperceptibility with perfectly tamper detection zone. We divide the original image into blocks and the main pixel is chosen for watermark insertion, where the embedding/extraction operates in the spatial domain. The tamper detection is tested by tampering watermarked image, and then based on the extracted attacked watermark; we can discover the tamper area. Also, the robustness watermarking aspect is proved against different kind of geometric and non-geometric attacks. Based on the experimental results, the imperceptibility and robustness of our watermarking approach are proven and showing perfectly the detection of the tamper zones.

Peer review under responsibility of Qassim University.
* *Corresponding author at*:Department of Management Information Systems, College of Business and Economics, Qassim University, P.O. Box 6633, Buraydah, 51452, Saudi Arabia.
E-mail addresses: laoamr@qu.edu.sa (L. Laouamer), Muath.Al-Shaikh@univ-brest.fr (M. AlShaikh), Laurent.Nana@univ-brest.fr (L. Nana), Anca.Pascu@univ-brest.fr (A.C. Pascu).

http://dx.doi.org/10.1016/j.jides.2015.10.001

1. Introduction

In the recent era, the Internet has become the main hub for data exchanges between users. Meanwhile, new attacks and threats may revoke the security of these electronic data. The security of computer field is provided with possibility techniques to cover these threats, like digital signature and watermarking techniques [1]. Watermarking techniques are applied in many fields in order to protect the content from unauthorized user [2], ensuring data integrity and authenticity [3], copyright proof [4] and data ownership [5]. The electronic data have to achieve security requirements. Those requirements concentrate on confidentiality and reliability. The confidentiality prevents unauthorized user from access to the data. While its reliability achieved by its integrity and its authenticity, where the integrity shows the content intact from illegal manipulation and the authenticity prove the data originality as sent from the source.

Robust watermarking techniques aim to prove the copyright and the owner issues. It has the ability to resist against malicious attacks like compression, noise and rotation [6], etc. However, semi-fragile watermarking techniques aim to prove the integrity and authenticity of the data content, It can accept the non-malicious modification and the watermark will be destroyed against malicious attacks, it called soft authenticate [7]. The fragile watermarking approaches called hard authenticate, which does not allow for any modification even for slight non-malicious modification and the watermark will be destroyed [8].

In regards to tamper detection, this subject is a critical and an important issue. The tampering aims to modify in the content without notice any change at the destination. Normally, fragile watermarking approaches can obtain and discover the manipulation area in the received data [9]. Whereas, watermarking consists of embedding a secret data in the host signal. When sending the watermarked image through unsecure signal, the receiver has to detect if the attacked received image was tampered or not and also protect the watermark [10].

Watermarking requirements are focused into its robustness against several attack scenarios. Capacity requirement is the offered space from the host signal for embedding watermark, while the payload is the amount bit of the embedded watermark. Imperceptibility is the visual quality after embedding, regarding to the human visual system (HVS), where the high imperceptibility provides a good visual quality and high fidelity. Moreover, Complexity is also an important aspect in order to reduce the embedding and extraction processing time and processes [11]. Fig. 1 shows the required factor to take into consideration in watermarking schemes.

Based on the manner of applying the watermarking approach, they are classified into two main domains: spatial and frequency. In the spatial domain, the watermark is embedded into the pixel of the host signal directly without applying any transformation, such as Least Significant Bit (LSB) [12] and Local Binary Pattern (LBP) [13]. It is providing a low complexity and simple watermarking approach, but it has not the ability to resist against attacks. Normally, the spatial watermarking approach can be considered for fragile watermarking application. The frequency domain consists to embed the watermark in the coefficients of the host signal, like Discrete Wavelet Transform (DWT) [14], Discrete Cosine Transform(DCT) [15] and Singular Value Decomposition (SVD) [11]. It is more robust against different attacks, but it is more complex than the spatial domain in term of the process.

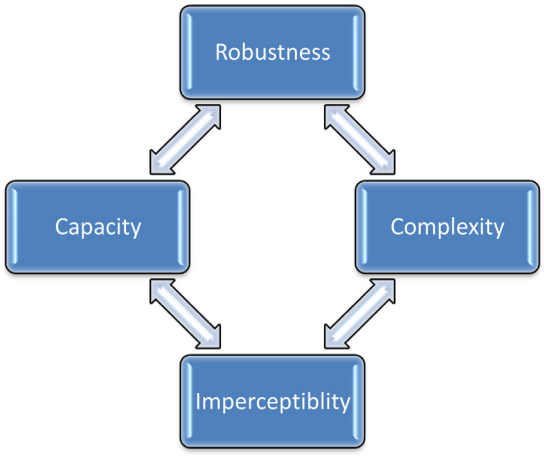

Fig. 1 – Watermarking schemes requirements.

Furthermore, the extraction of the watermark can be viewed as: blind [16], semi-blind [17] and non-blind approaches [18]. Firstly, the blind watermarking approach does not require either watermark or original image during the extraction phase; it is just using the secret key to extract the watermark. Secondly, semi-blind watermarking approach, it does not need the original image, but it still needs the original watermark for the extraction process. Thirdly, the non-blind watermarking approach, it needs the original image in the extraction process. Generally, the non-blind watermarking techniques are robust against image processing attacks.

2. Related works

The work in [19] presented a novel robust watermarking approach in the spatial domain. The technique is based on Imperialistic Competition Algorithm (ICA). The novelty in this paper is using ICA algorithm and the chosen least significant color, where ICA determines the embedding area in the host image. Then, After selecting certain location, the 5×5 neighbors pixel is selected and for each selected neighbor pixel, least significant color is chosen for insertion. The experimental results showed a good quality without attacks, where the PSNR was around 43 dB. But after applying some attacks, we note that the extracted watermark is far from being the same original watermark, especially after compression JPEG attacks.

[20] presented a fragile watermarking approach for image authenticity and integrity. The authors have improved the quality of the watermarked and retrieved images. They divide the original image into blocks of 8×8 pixels size and DCT the decompositions is applied for each block; the obtained coefficients are organized using zigzag order, first ten coefficients are adapted into a binary sequence which called as low frequency bits. The watermark is generated based