Expert Systems with Applications 42 (2015) 2224–2233

Contents lists available at ScienceDirect

Expert Systems with Applications

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

A highly secure oblivious sparse coding-based watermarking system for ownership verification

Afaf Tareef [a,*], Ahmed Al-Ani [b]

[a] School of Information Technologies, University of Sydney, NSW 2006, Australia
[b] Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia

ARTICLE INFO

Article history:
Available online 25 October 2014

Keywords:
False positive detection problem
Multiple claims of ownership
Sparse coding
Watermarking security

ABSTRACT

In the last few decades, the watermarking security issue has become one of the main challenges facing the design of watermarking techniques. In this paper, a secure oblivious watermarking system, based on Sparse Coding (SC) is proposed in order to tackle the three most critical watermarking security problems, i.e., unauthorized reading, false positive detection, and multiple claims of ownership problems, as well as optimize the fidelity, imperceptibility, and robustness characteristics. The reason for incorporating SC in the proposed system is to encode the watermark image before embedding it in the host image. This process is implemented using the well-known Stagewise Orthogonal Matching Pursuit (StOMP) method and an orthogonal dictionary that is derived from the host image itself. The watermark embedding is implemented in the transform domain of the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) of the host image. The proposed system is oblivious, as it does not need the original host image when extracting the embedded watermark. In addition, it is suitable for both bi-level and gray-level watermarks, and can accommodate large watermarks that are up to half the size of the host image. The proposed SC–DWT–SVD based watermarking scheme is tested for various malicious and un-malicious attacks and the experimental results show that it realizes the security requirement as it tackles the false positive detection and multiple claims of ownership problems on one hand and generates an encryption form of the watermark on the other hand. In addition, the added security does not compromise the imperceptibility and robustness aspects of the proposed technique and hence can be considered to be comparable or superior to other up-to-date watermarking techniques.

1. Introduction

Digital watermarking can be defined as the process of hiding secrete imperceptible piece of information, called watermark, into the multimedia data (i.e., images, videos and audios), called host or cover signal. For different purposes, digital watermarking is categorized into two classes based on the watermarks' resistance to attacks: robust watermarking and fragile watermarking. The main purpose of the robust watermarking is protecting ownership of the digital media, whereas the fragile watermarking is used to ensure the integrity of the digital media (Bianchi & Piva, 2013). In the last decade, robust digital watermarking has received a great attention.

In general, watermarking techniques have been evaluated according to the robustness, invisibility and capacity measures. The watermarking security has not been properly considered in most of the current literature despite of being an essential issue in many critical watermarking applications, such as those related to legal environments (e.g., authentication of legal documents, data monitoring, fingerprinting and medical image watermarking). In such applications, accepting fake information as legal is more detrimental than rejecting a legal one (Pérez-Freire, Comesana, Troncoso-Pastoriza, & Pérez-González, 2006). One of the most important problems related to the security issue of watermarking technology is the false positive detection problem, which is referred to as the ability to extract an un-embedded watermark from the digital host image. Many of the existing watermarking techniques, especially SVD-based watermarking ones, suffer from this problem. Fig. 1 illustrates the problem of false positive detection.

Another critical problem related to the security issue of watermarking technology is the problem of multiple claims of ownership. As known, protecting ownership rights is one of the earliest purposes of digital watermarking. However, extracting the embedded watermark from the watermarked multimedia is

* Corresponding author.
E-mail addresses: atar8654@uni.sydney.edu.au (A. Tareef), ahmed@eng.uts.edu.au (A. Al-Ani).

http://dx.doi.org/10.1016/j.eswa.2014.09.055
0957-4174/

not enough to confirm ownership unless certain requirements are imposed (Al-Nu'aimi and Qahwaji, 2009; Mohammad, Alhaj, & Shaltaf, 2008). If an attacker embeds another un-legal watermark to the already watermarked image, proofing the ownership becomes a serious problem. According to Craver, Memon, Yeo, & Yeung, (1998), rightful ownership cannot be resolved by most of the existing watermarking schemes. The false positive detection problem is largely arisen in the SVD-based watermarking techniques (Ali, Ahn, & Pant, 2014; Aslantas, 2009; Bhatnagar & Raman, 2009; Ganic & Eskicioglu, 2004; Huang & Guan, 2004; Lai, 2011; Lai & Tsai, 2010; Liu & Tan, 2002; Makbol & Khoo, 2013; Mishra, Agarwal, Sharma, & Bedi, 2014; Ouhsain & Hamza, 2009; Rastegar, Namazi, Yaghmaie, & Aliabadian, 2011; Shieh, Lou, & Chang, 2006). As a solution, (Mohammad et al., 2008) suggested dealing with this problem by ensuring to reach the maximum allowable amount of embedded information to prevent the attacker from adding any extra information to the image. However, this solution discourages some of the applications in watermarking technology that require embedding more than one watermark. The false positive detection in SVD-based watermarking techniques is still an open problem. In this paper, an effective solution for this challenging problem is proposed and evaluated using bi-level and gray-level watermarks. The false positive detection problem is tackled by using the host image itself as an evidence to prove the right watermark through the utilization of sparse coding, at the same time, the proposed approach can embed multiple high quality watermarks.

Another common security challenge that face watermarking techniques is keeping the secrete message unreadable and un-understood for unauthorized persons. Many algorithms deal with this challenge by using cryptography techniques, such as the Arnold transformation (Zhang, Wang, & Wang, 2008; Lu, Sun, & Cai, 2010; Ali, Ahn, & Pant, 2014) and chaotic encryption (Keyvanpour & Bayat, 2013; Song, Hou, Li, & Huang, 2011). This paper introduces a new version of encryption using the sparse coding theory.

An important issue related to the efficiency and practicability of watermarking schemes is blind watermarking. Based on whether or not the original image/signal is needed in the time of extraction, digital watermarking algorithms are divided into two main categories; blind and non-blind. Non-blind techniques are those that require the original image/signal for watermark extraction, which is not the case with the blind techniques. Blind watermarking (so-called oblivious or public watermarking) has a great significance and practical value in many applications where keeping a copy of the original signal without security is not practical.

All these issues, along with high robustness, invisibility and payload are maintained in our proposed watermarking system. Our SC–DWT–SVD based watermarking technique enables the legal owner to prove his/her ownership of the digital image even if an attacker embeds a fake watermark in it. To the best of our knowledge, this research represents the first attempt to encode the watermark as a function of its carrier using sparse coding. The incorporation of sparse coding in our proposed technique is based on generating a private dictionary from the host image itself to encode and decode the watermark image, which will inherently solve the watermarking security problems, as well as, enhance the robustness and imperceptibility. We believe this research will open the door for further researches in this area.

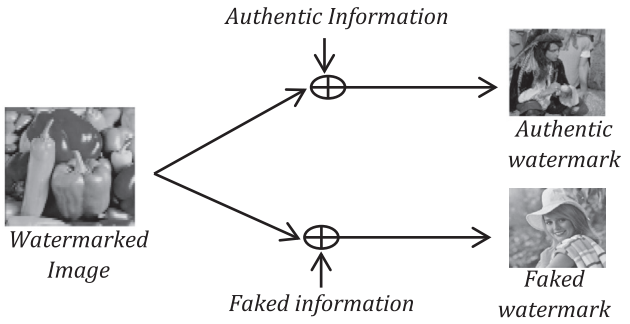

Fig. 1. Illustrates the problem of false positive detection.

The rest of this paper is organized as follows: in Section 2, a brief background about watermarking is given. Section 3 presents the basic theoretical concepts of the sparse coding. Section 4 describes the details of the proposed watermarking system. Simulations and analysis of the performance of the algorithm are presented in Section 5. The conclusion is drawn in Section 6.

2. Background

Digital image watermarking techniques can be categorized based on their applications, embedding domain and characteristics. With respect to the embedding domain, watermarking methods are divided into spatial domain techniques and frequency domain techniques. In the spatial domain watermarking algorithms, the watermark is embedded directly into image pixels while transform domain watermarking algorithms embed the watermark by altering the transformed coefficients after applying one or more transforms e.g., Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposing (SVD), Discrete Walsh Hadmard Transform (WHT), Discrete Fourier Transform (DFT) (Cox, Miller, Bloom, & Honsinger, 2002), or moment-based transformation, such as Tchebichef, Wavelet, Krawtchouk, and Zernike moments (Tsougenis, Papakostas, Koulouriotis, & Tourassis, 2012). Generally, embedding the watermark into the transform domain makes it more robust and invisible than embedding in the spatial domain, and the performance of frequency domain techniques can be further improved by combining two or more transforms.

In this section, the concepts of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are briefly described.

2.1. Discrete Wavelet Transform (DWT)

One of the most common used transforms is the Discrete Wavelet Transform (DWT). The idea behind DWT is dividing an image into four sub-bands in a single level: Low–Low (LL). Low–High (LH), High–Low (HL) and High–High (HH) frequency sub-bands. This process can be iterated many times to compute multiple scale wavelet decomposition as shown in Fig. 2. DWT is widely used in watermarking as it has found to enhance imperceptibility in the watermarked image. Some examples of DWT based watermarking techniques can be found in (Barni, Bartolini, & Piva, 2001; Lin, Wang, Horng, Kao, & Pan, 2009; Ouhsain & Hamza, 2009; Run et al., 2011).

One of the blind watermarking algorithms that utilized DWT was proposed by Lin et al. (2009) using maximum wavelet coefficient quantization. For embedding the watermark bits, the local maximum coefficients of various sized blocks, which are randomly selected from two sub-bands, are quantized. Another blind wavelet-tree based watermarking algorithm based on quantizing the maximum wavelet coefficient in a wavelet tree is proposed in Run et al. (2011). However, the two main limitations of the algorithm are its sensitivity to the rotating and cropping attacks and its inability to resolve the rightful ownership of an image when embedded with multiple signatures (Run et al., 2011).

2.2. Singular Value Decomposition (SVD)

Singular Value Decomposing (SVD) is an effective mathematical tool for extracting algebraic features from images. It has been used in signal processing for multiple purposes, such as image