Signal Processing 93 (2013) 1268–1294

Contents lists available at SciVerse ScienceDirect

Signal Processing

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

A novel approach to digital watermarking, exploiting colour spaces

Frédéric Lusson [a], Karen Bailey [a], Mark Leeney [a], Kevin Curran [b,*]

[a] Computing Department, Institute of Technology, Letterkenny, Co. Donegal, Ireland
[b] Intelligent Systems Research Centre, University of Ulster, Derry, N. Ireland, UK

ARTICLE INFO

Article history:
Received 16 December 2011
Received in revised form
8 October 2012
Accepted 14 October 2012
Available online 13 November 2012

Keywords:
Watermarking
Steganography
Image processing
Security
Information hiding

ABSTRACT

Watermarking is the process of embedding information in a carrier in order to protect the ownership of text, music, video and images, while steganography is the art of hiding information. Normally watermarks are embedded in images but remain visible in the majority of commercial image databases, such as Getty (gettyimages.ie) or iStock Photo (istockphoto.com). However this leaves traditional watermarking techniques vulnerable to tampering. Thus the advantage of using steganographic techniques for watermarking is that the watermark is resistant to detection and consequently to tampering. Robustness is a characteristic of critical importance, in order that a watermark is to survive image manipulation and enhancement processes, as well as intentional attacks, to ensure piracy is prevented.

The aim of this work is to produce a novel hybrid digital watermarking technique, based on the exploitation of both the RGB and the YCbCr colour spaces, using spatial domain techniques. Results demonstrate that the proposed hybrid technique can withstand levels of geometric attacks and processing attacks up to a point where the commercial value of the images tested would be lost. Results also demonstrate technical and performance improvements over existing methods, in terms of security and algorithm efficiency, while taking inspiration from steganography, to avoid drawing attention to the fact that an image contains hidden information.

1. Introduction

The unprecedented increase in piracy and digital criminality over the past 10 years has stimulated interest in the field of watermarking to enhance protection against violations of copyrighted digital material, such as digital images. According to a recent study carried out by TERA Consultants for the International Chamber of Commerce and made public in March 2010, the European creative industries lost around 9.9 billion euros and over 186,000 jobs in 2008 because of piracy, mainly digital piracy [48].

Over the last 15 years, many watermarking methods have been developed and tested with the aim of providing reliable ways of proving image ownership. Surveys detailing the most popular watermarking techniques can be found in the literature [3,5,39,28]. This document does not attempt to give a comprehensive review of all the watermarking and steganographic techniques developed over the past 15 years, as there is an impressive amount of research in this area. Rather, this paper discusses the most significant steps and techniques developed in the context of watermark invisibility and robustness in hiding information in digital images, in order to propose a novel watermarking technique approach. There are multiple data hiding methodologies and algorithms, each solving a particular facet of the watermarking problem, while no technique outperforms the others from all points of view. Most of the watermarking and steganography schemes are applied to grey-scale images, or colour images first transformed into

* Corresponding author.
E-mail address: flusson@utvinternet.com (K. Curran).

0165-1684/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2012.10.018

grey-scale images before the embedding phase would occur. However their application to colour images might not be completely adequate since they do not take into consideration the implication of the Human Visual System and in particular its sensitivity to colour brightness and perception.

More recent watermarking studies [38,32] have turned their attention to colour images rather than grey-scale images. Effectively, colour may be more than just an extension of grey scale. It is considered as a key element for a number of image processing systems. In particular, colour space transforms have played a central role in coding, compression and transmission applications, in television, video and image processing. While RGB channel format is a natural scheme for representing real-world colour, each of the three channels is highly correlated with the other two. YCbCr is a component colour space used by digital video. Unlike the RGB model, YCbCr breaks the visual information into black and white (luma) signal and two colour components. It separates luminance from chrominance (lightness from colour). With many more rods than cones, the human eye is more attuned to brightness and less to colour differences. Hence the YCbCr colour system allows more attention to be paid to Y, and less to Cb and Cr. As a result, using Cb and Cr values to embed the watermark, rather than the Y channel, should achieve watermark invisibility. Results show that watermarks hidden in the YCbCr and XYZ colour spaces in particular, are better recovered after JPEG compression attacks. Similar results are noticed with Gaussian noise attacks. These results demonstrate that the YCbCr and XYZ colour spaces have large amount of perceptual redundancy for colour pixels in this colour space. The larger the extent of perceptual redundancy, the greater the strength of the watermark signal that can be embedded, and the higher the robustness of the embedded watermark. Although the variety of attacks is quite limited, the YCbCr colour space shows better overall robustness to attacks while preserving the watermark invisibility. Robustness tests done against geometric attacks appear limited. Previous studies suggest that DWT algorithms perform well against compression and filtering.

2. Related work

Very early research focused on LSB insertion in the spatial domain (pixel level) of images for its simplicity and its potentially large capacity. Later scientific research considered the frequency domain and the quantisation of coefficients. Research conducted for the purpose of this work would indicate that watermarking and steganography techniques can be classified into Spatial Domain, Frequency Domain and Adaptive methods. Adaptive methods are treated as a special case here, because they can either be applied to the spatial domain or to the frequency domain. The following sections examine each domain methodology and analyse their impact on achieving the optimum watermarking requirements.

2.1. Spatial domain methods

Histogram equalisation is used in image processing to adjust contrasts [22]. The aim of this technique is to better distribute intensity values on the histogram. This allows for image areas of lower local contrast to gain a higher contrast. Histogram equalisation accomplishes this by effectively spreading out the most frequent intensity values. Histogram-based data-hiding is a commonly used watermarking scheme. In its simplest form, pre-defined histogram values are used to embed the watermark. Chrysochos et al. [8] chose a blind algorithm with an asymmetric key to embed the watermark into histogram values. They show that after embedding, the histogram shape is mainly preserved. They also demonstrate their algorithm to be robust against geometrical attacks such as rotation, flipping, translation, aspect ratio changes and resizing, warping, shifting, drawing and scattered tiles, as well as their combinations. They did not test their algorithm against compression nor against filtering attacks. In addition, the data hiding capacity is very much restricted to 127 bits (for grey-scale images) and 384 bits for colour images.

Such a scheme has the advantage of recovering the original cover image from the combined image. In addition, a modified histogram does not affect the visual perception of the image. The main drawback of this technique is that the embedding strategy can be detected more easily, just by comparing the histogram shape of the original image versus the watermarked image. Chrysochos et al. [8] and Bayley [4] suggest that the main advantage of histogram based data hiding is its robustness to rotations and other geometric transformations. On the other hand, the main difficulty associated with this technique is that there is a non-linear relationship between its representation and the pixel representation. Spatial domain methods concern the modification of a pixel value directly on the spatial domain of an image [36]. All studies referred to in this section are applied to either JPG or BMP images. One of the simpler approaches to hiding data within an image file is LSB insertion. Using this method, the binary representation of the hidden data is computed and LSB of each byte within the cover image is overwritten. There is a trade-off between preserving the image quality versus information hiding (watermark or secret message) payload, although it is generally accepted that modifying the LSB of each pixel does not visually alter image quality. A reasonable capacity is a third the size of the host image original size [47] (p. 34). This algorithm, presented by Shih and Wu [46] and Celik et al. [9], is easy to break, by flipping the least significant bit of every pixel of the image, or by embedding a new watermark on top of the current one. On the other hand, it is easy to implement and it requires less processing power. To alleviate this concern, other algorithms [17] have been introduced whereby a private key is used to define where the bit value should be embedded (LSB, LSB2 or LSB3). Varying the bit position used, makes it a lot more difficult to find which bit is used to embed the watermark bit. One potential problem with any of the LSB methods is that they can be discovered visually by an adversary who is looking for unusual patterns, or by using steganalysis tools. LSB manipulation is a fast and relatively inexpensive way of hiding information