Robust Image Watermarking Theories and Techniques: A Review

Hai Tao[*1], Li Chongmin*[2],Jasni Mohamad Zain[1], Ahmed N. Abdalla[3]

[1]Faculty of Computer System and Software Engineering,
University Malaysia Pahang , Malaysia
[2]Department of mathematics and information,
Qinghai Normal University, China
[3]Faculty of Electrical and Electronic Engineering,
University Malaysia Pahang, Malaysia

ABSTRACT
Over the past several decades, digital information science has emerged to seek answers to the question: can any technique ensure tamper-resistance and protect the copyright of digital contents by storing, transmitting and processing information encoded in systems where digital content can easily be disseminated through communication channels? Today it is understood that the answer is yes. This paper reviews the theoretical analysis and performance investigation of representative watermarking systems in transform domains and geometric invariant regions. Digital watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios, and other multimedia data by a certain algorithm. The basic characteristics of digital watermark are imperceptibility, capacity, robustness and false positive of watermarking algorithm and security of the hiding place. Moreover, it is concluded that various attacks operators are used for the assessment of watermarking systems, which supplies an automated and fair analysis of substantial watermarking methods for chosen application areas.

Keywords: watermarking, robust, attacks, security.

1. Introduction

Because of the fast and extensive growth of network technology, digital information can be distributed with no quality loss, low cost and nearly instantaneous delivery. Protection of multimedia content has recently become an important issue because of the consumers' insufficient cognizance of the ownership of intellectual property. Thus, over the past several decades, digital information science has emerged to seek answers to the question: can researchers ensure tamper-resistance and protect the copyright of digital contents by storing, transmitting, and processing information encoded in systems where digital content can easily be disseminated through communication channels? Today it is understood that the answer is yes, and many research groups around the world are working towards the highly ambitious technological goal of protecting the ownership of digital contents, which would dramatically protect inventions represented in digital form for being vulnerable to illegal possession, duplication and dissemination [83]. Digital watermarking [16] is the process of embedding or hiding digital information called watermark into a multimedia product, and then the embedded data can later be extracted or detected from the watermarked product, for protecting digital content copyright and ensuring tamper-resistance, which is indiscernible and hard to remove by unauthorized persons.

Digital watermarking is seen as a partial solution to the problem of securing copyright ownership [80]. Essentially, watermarking is defined as the process of embedding sideband data directly into the samples of a digital audio, image, or video signal. Sideband data is typically "extra" information that must be transmitted along with a digital signal, such as block headers or time synchronization markers. It is important to realize that a watermark is not transmitted in addition to a digital signal, but rather as an integral part of the signal samples. The value of watermarking comes from the fact that regular sideband data may be lost or modified when the digital signal is converted between formats, but the samples of the digital signal are (typically) unchanged[72].

To clarify this concept further, it is useful to consider an analogy between digital watermarks

and paper watermarks. Watermarks have traditionally been used as a form of authentication for legal documents and paper currency. A watermark is embedded within the fibers of paper when it is first constructed, and it is essentially invisible unless held up to a light or viewed at a particular angle. More importantly, a watermark is very difficult to remove without destroying the paper itself, and it is not transferred if the paper is photocopied. The goals of digital watermarking are similar; in the next section, it will be shown that digital watermarks require similar properties.

Before the concept of watermarking can be explored further, three important definitions must first be established. A host signal is a raw digital audio, image, or video signal that will be used to contain a watermark. A watermark itself is loosely defined as a set of data, usually in binary form, that will be stored or transmitted through a host signal. The watermark may be as small as a single bit, or as large as the number of samples in the host signal itself. It may be a copyright notice, a secret message, or any other information. Watermarking is the process of embedding the watermark within the host signal. Finally, a key may be necessary to embed a watermark into a host signal, and it may be needed to extract the watermark data afterwards[16].

Up to now, two traditionally-used strategies, spatial-domain [68] and transform domain [28][80] techniques have been developed for digital image watermarking. The former category is designed to insert directly a watermark into the original image by a factor, which would lead to fair-quality watermarked images. The latter approach, for taking advantage of perceptual properties, is devised to embed a watermark into the frequency-domain of the original images. These types of watermarking schemes have good performances of robustness in comparison to the most common signal processing manipulations such as JPEG compression, filtering, and addition of noise [16][14][40][49][59]. Signal processing operators are applied to watermarked images for removing the watermark or decreasing its energy so that the extracted watermark is unrecognizable or insufficient as the validate evidence. Unfortunately, the ineffectiveness of existing traditional watermarking algorithms is described by the robustness against unintentional or malicious geometric attacks [37]. Geometric attacks induce synchronization errors between the original and the extracted watermark during the detection process. In other words, the watermark still exists in the watermarked image, but its positions have been changed. Therefore, while traditional watermarking systems require the creation of a framework of the resilience to watermarked data geometrical modifications, creation and enforcement of synchronization errors correction of such frameworks is now possible. Besides facilitating more efficient copyrighted protection and robustness against desynchronization, adaptation of geometrically invariant image features can potentially offer a greater robust capacity to detect watermarks without synchronization errors, especially when applied to survive local distortions such as random bending attacks. Development of such a framework is an essential starting point for organizations that wish to improve or replace currently existing watermarking algorithm-based pixel frequency or other transform coefficients for watermark embedding, and develop a set of means to establish and maintain feature-based watermarking of geometric distortions correction.

In the first section, the properties of the general watermarking frameworks that are exploited in the process of encoding and detecting watermarking are shortly reviewed. A survey of the key digital image watermarking algorithms and techniques is presented subsequently. The characteristics of watermarking systems are described for evaluating the performance of watermarking systems. There are five important issues that are usually considered in the most practical application; they are highlighted in the following subsections. In addition, digital watermarking is described as an efficient method for the protection of ownership rights of digital audio, image, video and other data types. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control, and secret communication. Watermarking attacks can be classified into two broad categories: destruction attacks: including image compression, image cropping, spatial filtering, among others; and synchronization attacks: including image rotation, image shifting and pixelhine deletion. The chapter lists and describes some of these conventional attacks in the following sections.

For constructing geometric invariant watermarking, four mainstream schemes are introduced by literature reviews on watermarking algorithms robust to the