Optics and Laser Technology 109 (2019) 370–380

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Review

Review on optical image hiding and watermarking techniques

Shuming Jiao[a,c,*], Changyuan Zhou[a], Yishi Shi[b,*], Wenbin Zou[a,*], Xia Li[a]

[a] Shenzhen Key Lab of Advanced Telecommunication and Information Processing, College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China
[b] College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[c] Tsinghua Berkeley Shenzhen Institute (TBSI), Shenzhen 518000, China

HIGHLIGHTS

- First comprehensive literature review on optical image hiding and watermarking.
- Past existing works are only on optical encryption or digital watermarking.
- Various optical systems and architectures for image hiding are reviewed.
- Processing algorithms related to optical image hiding are summarized.
- Comparison of different optical image hiding schemes is made.

ARTICLE INFO

Keywords:
Watermarking
Image Hiding
Steganography
Optical
Holography
Hologram

ABSTRACT

Information security is a critical issue in modern society and image watermarking can effectively prevent unauthorized information access. Optical image watermarking techniques generally have advantages of parallel high-speed processing and multi-dimensional capabilities compared to digital approaches. This paper provides a comprehensive review of the research works related to optical image hiding and watermarking techniques conducted in the past decade. The past research works have focused on two major aspects: various optical systems for image hiding, and the methods for embedding the optical system output into a host image. A summary of the state-of-the-art works is made from these two perspectives.

1. Introduction

With the rapid development of Internet and information technology, the problem of unauthorized acquisition, transmission, manipulation and distribution of digital content has become increasingly severer in recent years. Research on information security has attracted considerable attention. In addition to digital approaches [1], optical approaches for information security, including optical image encryption, authentication and watermarking, have been extensively investigated [2–5] in the past decade. Optical approaches generally have the advantages of parallel high-speed processing and multidimensional capabilities.

Information hiding, sometimes referred to as watermarking or steganography, is a technique of imperceptibly altering a carrier signal for embedding a hidden message (a watermark signal). Information hiding can be performed for various categories of signals, including, but not limited to, audio, image and video signals. Image watermarking (or hiding) allows the insertion of a watermark image into another carrier image in a way that the watermark image is not accessible and perceptible by unauthorized users. The hidden image is generally referred to as a watermark image and the carrier image is generally referred to as a host (or cover) image. In image watermarking (either implemented digitally or optically), there are usually several necessary criteria: (1) The host image shall not be significantly degraded after the watermark is embedded; (2) The watermark shall be imperceptible from the watermarked host image; (3) The watermark shall be robust and not easily removed or damaged from the host image. The watermark shall be tolerant to different types of attacks such as JPEG compression, cropping, rotation, scaling, noise, filtering and blurring. It shall be noted that this criterion is only applicable to a robust watermark rather than fragile watermark; (4) The watermark shall be sufficiently secure and difficult for an unauthorized user to illegally access.

Some comprehensive reviews on optical image encryption techniques [2,3] and on digital image watermarking techniques [6–10] have been reported in the past. However, little work has been conducted

* Corresponding authors at: Shenzhen Key Lab of Advanced Telecommunication and Information Processing, College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China (S. Jiao).
E-mail addresses: albertjiaoee@126.com (S. Jiao), sysopt@126.com (Y. Shi), wzouszu@sina.com (W. Zou).

https://doi.org/10.1016/j.optlastec.2018.08.011
Received 3 January 2018; Received in revised form 29 May 2018; Accepted 8 August 2018

regarding a survey of optical image watermarking techniques. The difference between encryption and watermarking (either optically or digitally) is briefly described following. Encryption techniques transform the original image into noise-like ciphertext, which is not accessible by unauthorized users without the correct key. However, the existence of ciphertext is usually known to the third party. The aim of watermarking, on the other hand, is to hide the existence of the original image to unauthorized users.

As a comparison, optical image watermarking has some potential advantages over digital image watermarking. First, an optical system can support high-speed parallel optical information processing for mass data. In digital watermarking, however, intensive computational cost is inevitable when the watermark image and host one have a large image size and the watermarking algorithm is complicated. Second, optical watermarking can be implemented directly on a physical two-dimensional or three-dimensional watermark object or host object. The imaging process (from a physical object to a digital image) and watermarking process are realized simultaneously. In addition, the numerous physical parameters, such as wavelength, amplitude, phase, distance, and polarization, in an optical system can be employed as keys for securing the watermark image. Digital watermarking, on the other hand, requires both a digitized watermark image and a digitized host image for further processing. Despite the evident advantages of optical watermarking, it is restricted by the physical principles of a specific optical system, while digital watermarking algorithms can be designed very flexibly. Additionally, digital watermarking possesses easy implementation on widely available computer and digital devices in practice.

Watermarking can be divided into two categories: robust watermarking and fragile watermarking. In the vast majority of works on optical image hiding, watermarking is defined as the former. For robust watermarking, the watermark remains intact when the host image is attacked and distorted. Since a robust watermark is very difficult to remove from a host image, it can be employed for applications such as copyright protection. On the other hand, for a fragile watermark, once the host image is slightly modified, the watermark will be altered. A fragile watermark can be employed for verification applications such as an integrity check of the host image. An intact fragile watermark indicates that the host image is in its original form without editing, damage and alteration.

The proposed optical image hiding or watermarking schemes in the past generally followed the framework illustrated in Fig. 1. In digital watermarking, the original watermark image is usually directly embedded into the host image with certain algorithms. However, in optical image watermarking, the original watermark image is usually employed as an input image to an optical system such as the double random-phase encoding (DRPE) system, off-axis holography system, phase shifting holography system, optimized phase-only mask architecture, joint transform correlator (JTC), ghost imaging system and ptychography system. Then the system output (e.g., a hologram), named “ciphertext” in this review article, is embedded into the host (or cover) image either optically or digitally. The embedding operations range from simple weighted addition to complicated adaptive signal embedding. It shall be noted that the host image may not necessarily be a photograph but also other types of optical images, such as digital holograms. Finally, the original watermark image can be retrieved from the watermarked host image optically (or opto-digitally).

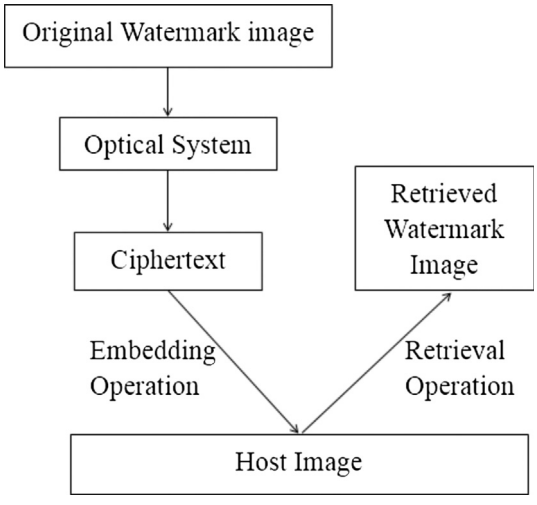

Fig. 1. General framework for optical image hiding (or watermarking) schemes.

This paper presents a comprehensive review of various optical image watermarking systems and schemes proposed in the past decade. In Section 2, a review is conducted on common optical systems employed for image hiding. In Section 3, a review is conducted on the methods to embed optical system output into a host image. In Section 4, a brief conclusion is provided.

2. Various optical systems for image hiding and watermarking

A wide variety of optical systems has been attempted for optical image hiding or watermarking in past works, including DRPE, off-axis holography system, phase shifting holography system, optimized phase-only mask architecture, JTC, ghost imaging system and ptychography.

2.1. Optical watermarking with double random-phase encoding

The DRPE scheme was first proposed by Refregier and Javidi in 1995 [11] and it has been extensively employed in the optical information security area, including optical image hiding. DRPE can be expressed as

$$g(x, y) = IFT\{FT[f(x, y)exp(j2\pi p(x, y))]exp(j2\pi q(u, v))\} \quad (1)$$

where $f(x, y)$ denotes the watermark image, FT denotes Fourier transform, IFT denotes inverse Fourier transform, $exp(j2\pi p(x, y))$ and $exp(j2\pi q(x, y))$ are two random-phase masks in the spatial domain and frequency domain, respectively, and $g(x, y)$ denotes the ciphertext image (a complex signal) generated for the original watermark image.

In [12,13], a straightforward way to apply DRPE in image watermarking is proposed. The original watermark image $f(x, y)$ is first encrypted by DRPE and the cipher-text $g(x, y)$ (a complex signal) is weight added to the host image $h(x, y)$ in the spatial domain:

$$w(x, y) = h(x, y) + m \cdot g(x, y), \quad (2)$$

where m is a weighting coefficient. The watermark can be retrieved when conventional DRPE decryption steps are applied to the watermarked host image $w(x, y)$:

$$f'(x, y) = IFT\{FT[w(x, y)]exp(-j2\pi q(x, y))\}exp(-j2\pi p(x, y)) \quad (3)$$

The host image will contribute a tolerable level of noise in the retrieved watermark image $f'(x, y)$. An example of watermarking results is illustrated in Fig. 2.

The complex amplitude of ciphertext after DRPE encryption can be quantized to a reduced number of discrete real values [14,15]. As a consequence, the data size of ciphertext is highly compressed, and reasonable recovered watermark image quality can still be maintained.

In addition to the Fourier transform domain, the watermark can be encrypted by DRPE in the fractional Fourier transform (FrFT) domain. The fractional order parameter in FrFT offers extra security against attacks. The ciphertext is embedded into a conventional host image [16] or a Fresnel hologram [17]. Multiple watermarks can be encrypted by DRPE with different keys in the FrFT domain and then multiplexed by superposition [18]. Each individual watermark can be retrieved separately from the watermarked host image. The original watermark image can be encrypted by other optical encryption schemes