Optics Communications 366 (2016) 314–320

Contents lists available at ScienceDirect

Optics Communications

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

Invited Paper

Optical image hiding based on computational ghost imaging

Le Wang [a], Shengmei Zhao [a,b,*], Weiwen Cheng [a], Longyan Gong [c], Hanwu Chen [d]

[a] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications (NUPT), Nanjing 210003, China*
[b] *Key Lab of Broadband Wireless Communication and Sensor Network Technology (NUPT), Ministry of Education, Nanjing, China*
[c] *Information Physics Research Center and Department of Applied Physics, NUPT, Nanjing, China*
[d] *School of Computer Science and Engineering, Southeast University, Nanjing, China*

ARTICLE INFO

Article history:
Received 23 November 2015
Received in revised form
8 January 2016
Accepted 10 January 2016
Available online 16 January 2016

Keywords:
Digital watermarking
Computational ghost imaging
Imaging reconstruction techniques
Least significant bit

ABSTRACT

Imaging hiding schemes play important roles in now big data times. They provide copyright protections of digital images. In the paper, we propose a novel image hiding scheme based on computational ghost imaging to have strong robustness and high security. The watermark is encrypted with the configuration of a computational ghost imaging system, and the random speckle patterns compose a secret key. Least significant bit algorithm is adopted to embed the watermark and both the second-order correlation algorithm and the compressed sensing (CS) algorithm are used to extract the watermark. The experimental and simulation results show that the authorized users can get the watermark with the secret key. The watermark image could not be retrieved when the eavesdropping ratio is less than 45% with the second-order correlation algorithm, whereas it is less than 20% with the TVAL3 CS reconstructed algorithm. In addition, the proposed scheme is robust against the 'salt and pepper' noise and image cropping degradations.

1. Introduction

Image hiding and watermarking techniques could embed the secret information (or the watermark) in a host image and retain them in their original forms to hide the existence of the secret information [1]. They can achieve secure message storage and transmission to avoid the attention of the eavesdropping. They have attracted increasing interests [2–4] because the enormous data and images have been transmitted through the Internet in now big data times.

In a different context, ghost imaging (GI), also known as correlated imaging [5–16], is an intriguing optical technique to allow the imaging of objects to be located in optically harsh or noisy environments. In a standard two-detectors pseudo-thermal GI configuration, there are two optical beams. One beam, called signal beam, crosses the object and is detected by a bucket detector without any spatial resolution. The other beam, named reference beam, is detected by a spatially resolving detector. The image is retrieved when the bucket detector signals are correlated with that signals in the reference beam [8]. Then, Shapiro [10] proposed a computational ghost imaging (CGI) scheme, which is a modified version of the standard two-detectors pseudo-thermal GI configuration, and the intensity detected in the reference beam is computed offline. The past years have witnessed a rapidly growing interest in applications of ghost imaging ranging from laser radars [17,18], microscopes [19,20], marked ghost imaging [30] and secure key distribution [21,22] to optical encryption schemes [23–26,31].

In this paper, we present an image hiding scheme based on CGI system. In the scheme, each detection result of an original watermark image is created by the bucket detector with the aid of the CGI system, and is transformed to a floating point number with 32-bits. Later, M 32-bits detection results construct a binary-gray-scale encrypted watermark image. Here, the random speckle patterns to create the detection results compose a secret key. The encrypted watermark image is embedded in a host image by least significant bit (LSB) algorithm. With the key, the authorized users can decrypt and reconstruct the original watermark image by the second-order correlation algorithm or the compressed sensing (CS) algorithm.

The advantages of the proposed scheme are the following. Firstly, comparing with LSB algorithm, the encrypted watermark image produced with the aid of the CGI system, instead of the original watermark image, is embedded in a host image in the proposed scheme, which is complete noise even if eavesdropper has known the proper reconstruction mechanism but has no secret keys. Secondly, the proposed scheme is robust against 'salt and pepper' noise and image cropping degradations. Thirdly, the proposed scheme is secure by taking advantage of the optical

[*] Corresponding author at: Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications (NUPT), Nanjing 210003, China.
E-mail address: zhaosm@njupt.edu.cn (S. Zhao).

http://dx.doi.org/10.1016/j.optcom.2016.01.026
0030-4018/© 2016 Elsevier B.V. All rights reserved.

encryption scheme based on CGI.

The organization of the paper is as follows. In Section 2, the image hiding scheme based on CGI system is presented. In Section 3, the performances of the image hiding scheme based on CGI system are discussed. Finally, Section 4 concludes the paper.

2. Optical image hiding based on computational ghost imaging

The schematic configuration of the proposed scheme is illustrated in Fig. 1, where Fig. 1(a) is for getting an encrypted watermark, Fig. 1(b) is for a watermark embedding, and Fig. 1(c) is for the watermark extracting. Fig. 1(a) and (b) comprise the watermark embedding procedure. An encrypted watermark can be obtained with the aid of CGI system, where a random speckle pattern $I_i(x, y)$ illuminates a watermark image, and the total intensity transmitted through the watermark image is collected and detected by a bucket detector, generating a detection result B_i:

$$B_i = \int dx\, dy\, I_i(x, y) T(x, y), \quad (1)$$

where $T(x, y)$ is the distribution function of the watermark image. Here, the detection result B_i is a real decimal number and can be transformed into a floating point number with 32-bits by IEEE 754 standard [27], where the first bit is for the sign, the next eight bits

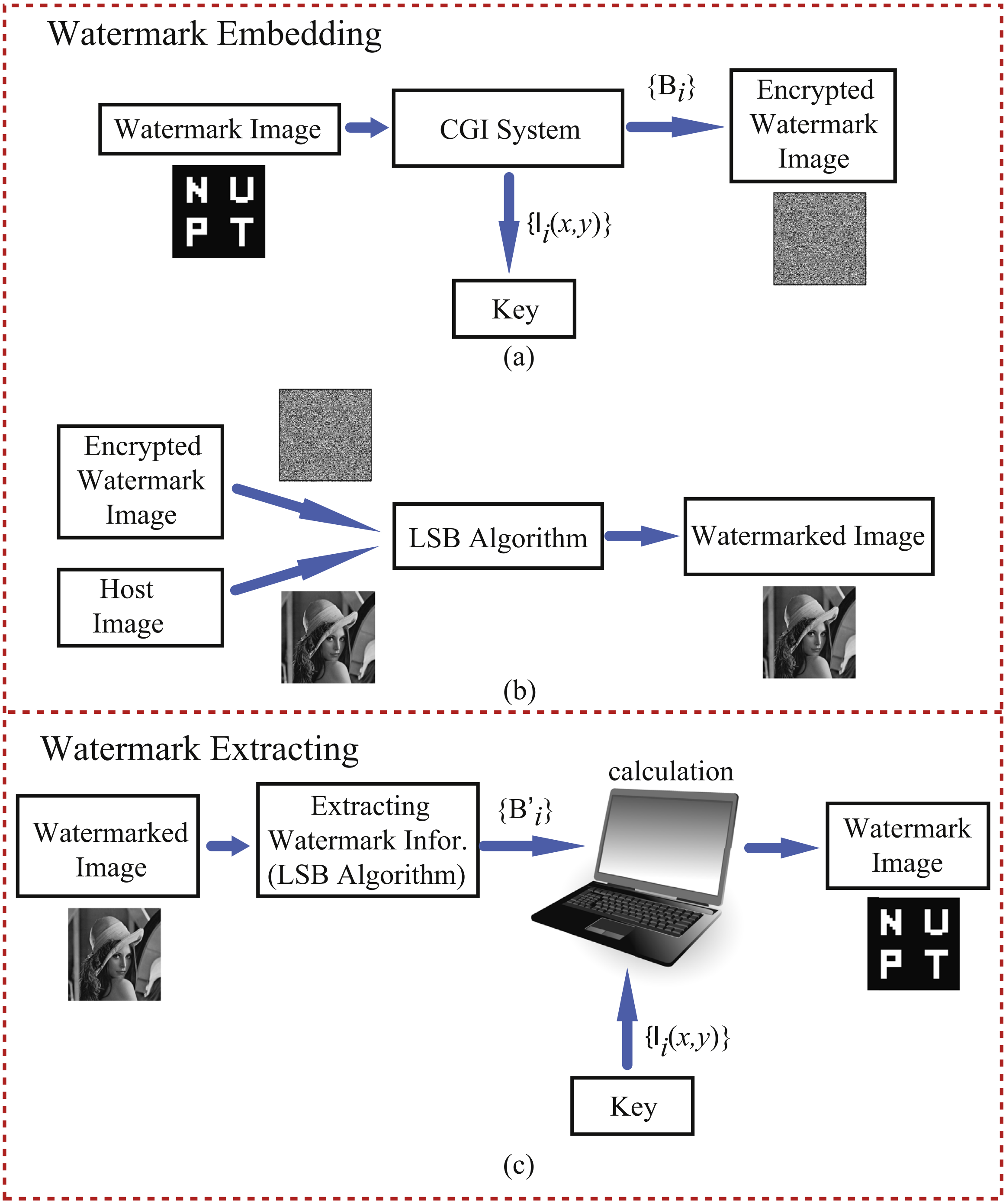

Fig. 1. The schematic configuration of the proposed image hiding scheme. (a) is for getting an encrypted watermark, (b) is for a watermark embedding, and (c) is the watermark extracting procedure. (a) and (b) comprise the watermark embedding procedure.