Optics Communications 356 (2015) 186–194

Contents lists available at ScienceDirect

Optics Communications

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

Robustness enhancement for image hiding algorithm in cellular automata domain

Xiaowei Li [a], Seok-Tae Kim [b], In-Kwon Lee [a,*]

[a] Department of Computer Science, Yonsei University, Seoul, Republic of Korea
[b] Department of Information and Communications, Pukyong National University, Busan, Republic of Korea

ARTICLE INFO

Article history:
Received 20 May 2015
Received in revised form
18 July 2015
Accepted 23 July 2015

Keywords:
Cellular automata
Distributed memory
Elemental images
Lensless integral imaging

ABSTRACT

In this paper, we present a cellular automata (CA)-domain image hiding scheme that embedding a secret image into a gray-level image, in which an effective image preprocessor technique is introduced to improve the robustness of the secret image. The image preprocessor works by transforming a secret image into many elemental images based on the lensless integral imaging technique. The properties of data redundancy and distributed memory of the elemental images reinforce the ability to resist some data loss attacks. Besides, we study an improved pixel-wise masking model to optimize the imperceptibility of the stego-image. Experiments verify that the imperceptibility and robustness requirements of the image hiding are both satisfied excellently in the proposed image hiding system.

1. Introduction

With the development of multimedia and network, the problem of information security is becoming more and more important [1–8]. Image hiding technique has become an important tool to realize image protection. Image hiding is a technique of transferring the secret image without attracting the attention of third parties. An image embedded with a secret image is called a stego-image. The irrelevant recipients of a stego-image are unaware of the existence of the hidden image. Numerous image hiding techniques have been presented in recent years, some based on transform domain [9,10], some in spatial domain [11], and some based on quantization [12]. From the literature survey we find that many researchers are studying the field of image hiding in their own methods, and most methods for image hiding have their own identity, strength and weakness.

A fundamental issue in image hiding is to achieve a trade-off between imperceptibility and robustness. Recent years, a study field whose results could undoubtedly help in the design of an image hiding algorithm is human visual system (HVS)-based image compression. HVS model in transform subbands of discrete wavelet transform (DWT) is originally developed for image compression based on DWT, where there is a need of a good quantization matrix that provides better quality of compressed images with higher compression ratio. A pixel-wise masking based image hiding technique has been proposed in [13]. According to the characteristics of the HVS, this method provides good image quality, and is robust against common signal processing attacks. However, because embedding is made only in the highest resolution level, the watermark information can be easily removed by a potential attacker. After that, many image hiding techniques based on modified improved pixel-wise masking techniques have been presented in [14–17]. In order to improve the robustness, the moment-based watermarking methods have been proposed in [18,19], the researchers incorporated the orthogonal image moments into their own methods. The invariant properties of the moments to remain unchanged under common geometric transformations significantly improve the robustness of the watermarks in such kind of attack. Recently, the singular value decomposition (SVD) based image watermarking has been proposed for solving the ownership problem [20,21]. The key point of the SVD-based image watermarking is the stability property of the singular value matrix. Most of the SVD watermarking techniques, only the singular values of watermark are embedded into the host image. This strategy causes the false positive problem. A false positive problem may also occur when a specific watermark is detected from a content in which a different watermark was embedded, causing an ambiguous situation. The attackers can easily prove the ownership of the arbitrary watermarked image without knowing the original watermark embedded in the host image [22].

Most of pervious works on image hiding aimed at valuing the embedding weight-function to improve the robustness of the extracted secret image. In most cases, these methods provide good robustness for secret image extracting. However, the robustness of these methods could seriously degrade or disappear when a stego-

[*] Corresponding author.
E-mail address: iklee@yonsei.ac.kr (I.-K. Lee).

http://dx.doi.org/10.1016/j.optcom.2015.07.073
0030-4018/© 2015 Elsevier B.V. All rights reserved.

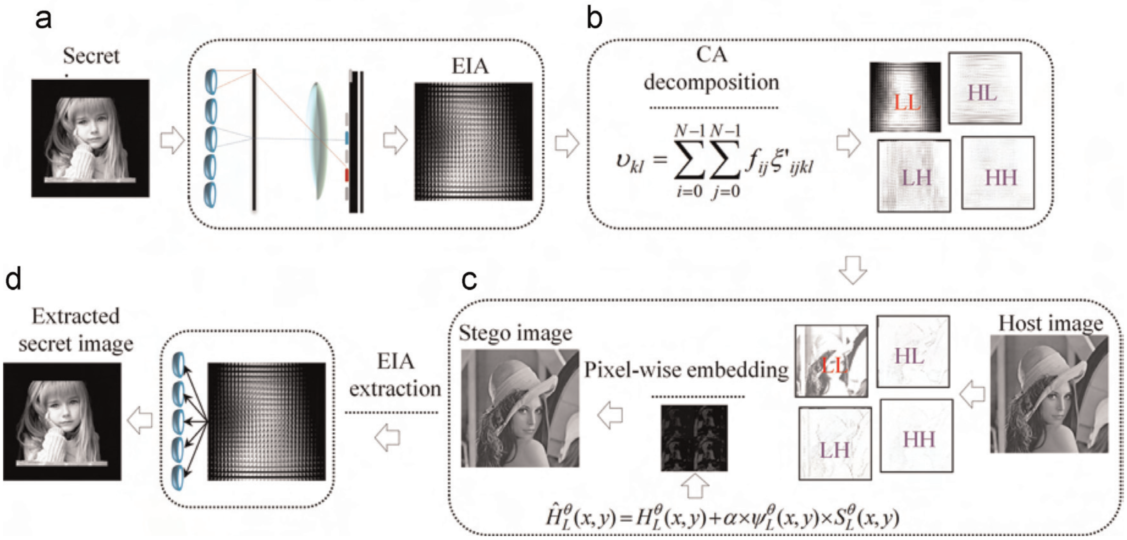
a
Secret
EIA
b
CA decomposition
$\upsilon_{kl}=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f_{ij}\xi'_{ijkl}$
LL
HL
LH
HH
d
Extracted secret image
EIA extraction
c
Stego image
Pixel-wise embedding
Host image
LL
HL
LH
HH
$\hat{H}_L^{\theta}(x,y)=H_L^{\theta}(x,y)+\alpha\times\psi_L^{\theta}(x,y)\times S_L^{\theta}(x,y)$

Fig. 1. Structure of the proposed image hiding technique: (a) pickup process, (b) CA decomposition process, (c) pixel-wise embedding process, (d) secret image reconstruction process.

image against some serious data loss attacks. That is because of most useful information of the secret image is lost when the stego-image is damaged by the high-strength attacks. The secret image is hardly reconstructed from the incomplete information.

Cellular automata (CA) have been of theoretical interest since the pioneering work of Von Neumann in the 1940s. CA are dynamical systems in which space and time are discrete [23,24]. The cells are arranged in the form of regular lattice structure and each must have a finite number of states. These states are updated synchronously according to a specified local rule of interaction. Using CA with various rule numbers, it can offer many channels for embedding. Thus CA-based watermarking scheme can recover the weak point having only one transform plane in the DWT method. It can greatly improve the security of the watermarking system due to large key space. Also, CA transform as an orthogonal transformation which offers considerable simplicity in the calculation of the transform coefficients, in other words, it can improve the quality of watermarked image by reducing energy loss compared with the traditional complicated transform process.

We study an image hiding technique that operates in the CA domain. Before embedding, the secret image needs to be preprocessed by the lensless integral imaging technique [25–28]. In this processing stage, many small elemental images are produced by a virtual pinhole array, and each of the elemental images possesses the inherent property of the secret image. Although most of the elemental images are damaged or lost, the secret image can be successfully reconstructed from the remaining elemental images.

In this paper, a new lensless integral imaging based image hiding algorithm that allows embedding of a secret image in all CA subbands is designed. To achieve a trade-off between imperceptibility and robustness, we first design an improved pixel-wise masking model to value the embedding strength. The lensless integral imaging technique is used to improve the robustness of the secret image. Besides, compared with conventional transform-based image hiding schemes only provide one spectrum for data embedding, CA can provide many transform planes for data embedding according to various CA rules, which help improve the security. The performance is checked in terms of peak signal-to-noise ratio (PSNR) and bit correct ratio (BCR) to check the effectiveness of the proposed scheme.

The rest of this paper is organized as follows. Characteristics of the proposed algorithm and its details are described in Section 2. Experimental results and discussion in Section 3. Finally we draw our conclusions in Section 4.

2. Proposed method

To achieve better image quality and high robustness on both the stego-image and the extracted secret image, the pixel-wise masking and lensless integral imaging techniques are adopted in this scheme. CA transform is very suitable to identify that the secret image can be more easily hidden because of its excellent spatial-frequency localization properties. A pixel-wise masking technique, which was originally presented in [13], is able to adjust the pixel by pixel embedding strength to more efficiently fulfil the high resolution requirement of the stego-image. As for the high robustness, in this study, the secret image needs to be picked-up in the form of many elemental images before being embedded into the CA coefficients.

2.1. Secret image pickup

To improve the robustness requirement of the image hiding system, in this paper, we introduce the lensless integral imaging technique. The detailed description of the integral imaging technique can be found in [29–31]. In this section, we at first describe image preprocessing stage by using lensless integral imaging technique. The optical structure of the preprocessing stage is shown in Fig. 1(a), a secret image is set to the front of a lenslet array, an elemental image array is recorded through this lenslet array and an image sensor. For convenience, the lensless integral imaging replaces the optical devices is used in this scheme. The benefit of using this lensless system is to improve the quality of the reconstructed image. The recorded elemental images $E(x,y)$ can be calculated by the following equation:

$$E(x,y)=\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} f\left(-x\frac{d}{l}+i\delta,\,-y\frac{d}{l}+j\delta\right) \tag{1}$$

where $M\times N$ denotes the number of the elemental images, d is the gap between the computer synthesized pinhole array and recorded pickup plane, l is the distance between the secret image and the pinhole array, and δ is the size of each of pinholes.