Signal Processing ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Signal Processing

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

Chaotic image encryption using pseudo-random masks and pixel mapping

Xiaowei Li [a], Chengqing Li [b], In-Kwon Lee [a,*]

[a] Department of Computer Science, Yonsei University, Seoul, Republic of Korea
[b] College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China

ARTICLE INFO

Article history:
Received 9 April 2015
Received in revised form
13 November 2015
Accepted 15 November 2015

Keywords:
Chaotic encryption
Image encryption
Pixel mapping
Cellular automata

ABSTRACT

Integral imaging-based cryptographic algorithms provide a new way to design secure and robust image encryption systems. In this paper, we introduce a performance-enhanced image encryption scheme based on depth-conversion integral imaging and hybrid cellular automata (CA), aiming to meet the requirements of secure image transmission. First, the input image is decomposed into an elemental image array (EIA) using the depth-converted integral imaging technique. The obtained elemental images then are encrypted by utilizing the CA model and chaotic sequence. The conventional computational integral imaging reconstruction (CIIR) technique is a pixel-superposition technique. The resolution of the reconstructed image is dramatically degraded by the large magnification factor in the superposition process as the pickup distance increases. In the proposed reconstruction process, the pixel mapping technique is introduced to solve these problems. A novel property of the proposed scheme is its depth-conversion property, which reconstructs an elemental image originally recorded at long distances from the pinhole array as one that was recorded near the pinhole array and consequently reduces the magnification factor. The results of numerical simulations demonstrate the effectiveness and security of the proposed scheme.

1. Introduction

With the development of networks and the increasing frequency of image transmissions, image security has become a paramount issue in communication science. All kinds of security problems about image data have emerged, such as unauthorized access and forgery detection [1,2]. Encrypting an image as text data is the most direct way to protect images. Because of the strong correlation in image data, conventional text encryption techniques are not appropriate for image encryption. In the past two decades, a large number of schemes have been proposed for image encryption utilizing all kinds of optical techniques [3–6], which combine the distinct advantages of processing two-dimensional (2D) image data with a parallel conduction mode. Among them, the most widely used transform methods are the fractional Fourier transform (FRT), extended FRT, gyrator transform, and Fresnel transform. As some properties of chaos are very similar to those of a secure encryption scheme, such as high sensitivity to initial values and system parameters, chaotic maps have been used to design image encryption schemes [7–11]. Meanwhile, many approaches to analyzing the security levels of existing encryption schemes have been presented [9,12–18].

In recent years, the integral imaging technique has received intense attention in the study of image encryption [19–21]. This technique divides an input image into many elemental images by utilizing a lenslet array or pinhole array. Each elemental image has nearly

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

http://dx.doi.org/10.1016/j.sigpro.2015.11.017
0165-1684/© 2015 Published by Elsevier B.V.

Please cite this article as: X. Li, et al., Chaotic image encryption using pseudo-random masks and pixel mapping, Signal Processing (2015), http://dx.doi.org/10.1016/j.sigpro.2015.11.017

the full attributes of the input image. As a result, encrypting the elemental images can greatly improve robustness and security during image transmission. The conventional integral imaging system is composed of two parts: pickup and reconstruction. In the integral imaging pickup and reconstruction processes, an optical lenslet array is utilized in both processes to capture and reconstruct the input image. In the pickup process, the light rays coming from the input image pass through the lenslet array and a set of inversely small images are then recorded using a pickup device. The recorded small image array is referred to as an elemental image array (EIA). In the image reconstruction process, light rays of the elemental images are back-propagated through the lenslet array to obtain the original input image. When optical devices are used, the quality of the reconstructed image is poor because of the light diffraction and limitations of the optical devices.

To cope with this problem, some computational reconstruction techniques have been proposed [22–24]. Among them, the most commonly used method is the computational integral imaging reconstruction (CIIR) algorithm, which can digitally reconstruct an image from a recorded EIA. Each of the recorded elemental images are inversely projected onto an output plane and inversely magnified according to a magnification factor. This method can improve the image resolution because there is no diffraction nor limited optical device. The CIIR technique, however, still has some serious problems, such as the fact that the image resolution seriously degrades as the reconstruction distance increases. Because CIIR is a pixel reverse magnified reconstruction technique, the overlapping pixel areas increase as the magnification factor increases. The interference of adjacent pixels degrades the quality of the reconstructed image. Many researchers have focused on how to improve the quality of the reconstructed image in integral imaging systems. However, many techniques still use the CIIR technique [25], and the degradation of the input image resolution for long distances from the lenslet array has not greatly improved.

In this paper, we present a new image security system based on a smart mapping technique to improve the quality of the reconstructed image. Smart mapping is a depth-conversion process in which the original elemental images recorded at long distances can be converted to ones recorded near the pinhole array. This algorithm can improve the quality of the reconstructed image by weakening the interference problem caused by the decreased magnification factor. Meanwhile, the robustness of the encrypted image can be greatly improved because of the data redundancy of 2D EIA. To show effectiveness of the proposed scheme, some experiments were carried out on several typical test images.

The rest of the paper is organized as follows. Section 2 reviews previous related work on image encryption. Next, Section 3 gives some theoretical analysis. The proposed image encryption scheme is proposed in Section 4 and detailed experimental results are presented in Section 5. Finally, the last section concludes the paper.

2. Previous work

In [26], Hwang et al. proposed an image copyright protection scheme based on the computational integral imaging (CII) technique, in which the 3D watermark information is embedded into the DWT domain. The 3D watermark plain-image can be reconstructed using a CIIR technique. This scheme is highly robust because of the data redundancy of the elemental images. However, in the watermark extraction process, CIIR is a pixel superposition reconstruction method. The resolution of the reconstructed 3D plain-image is dramatically degraded as the magnification factor increases. In [19], Piao et al. developed an image encryption scheme based on integral imaging and pixel scrambling techniques. In the scheme, the input image is first recorded using the CII technique and the obtained elemental images are scrambled by a pixel scrambling technique. In the reconstruction process, the image is reconstructed by the CIIR technique. This method is a highly secure and robust encoding system. However, it incurs resolution degradation problems.

In our previous approaches, proposed in [20], we presented a multiple-image encryption scheme based on CII and a back-propagation (BP) neural network. In the multiple-image encryption part, a CII pickup technique is employed to record the multiple-image simultaneously to form an EIA. The EIA is then encrypted using the maximum length cellular automata (CA) and random phase encode algorithm. To improve the low-resolution problem caused by CIIR, a BP neural network is utilized. Numerical simulations were performed to demonstrate the performance of the method. However, reference EIAs are needed to train the BP network. When decrypting multiple images, the sender records all reference EIAs correctly and sends them to the receiver. The encryption process is somewhat complicated and the network load is high. In [21], we proposed a 3D image encryption scheme based on computer-generated integral imaging (CGII) and CA, in which a 2D EIA is digitally recorded by lights coming from the 3D image through a pinhole array according to the ray tracing. The CA transform is then used to encrypt the 2D EIA. This scheme can provide a high level of security because of the hologram-like properties of 2D EIA and large key space provided by CA.

In [27], Maptista presented a message encryption scheme based on chaotic logistic maps, where each alphabet is encrypted into an iteration number of the map that falls in a given interval of the phase space. In the encryption scheme cryptanalyzed in [17], Pareek et al. proposed an image encryption scheme using chaotic logistic maps, where an external secret key of 80 bits and two chaotic logistic maps were used. To make the encryption system more robust against attacks, the scheme updates the secret key after encrypting each block of image pixels.

3. Theoretical analysis

3.1. Review of conventional CGII

A CGII system uses a set of elemental images generated by computer graphics instead of the pickup process

Please cite this article as: X. Li, et al., Chaotic image encryption using pseudo-random masks and pixel mapping, Signal Processing (2015), http://dx.doi.org/10.1016/j.sigpro.2015.11.017