Optics and Lasers in Engineering 112 (2019) 162–169

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Modified integral imaging reconstruction and encryption using an improved SR reconstruction algorithm

Xiaowei Li[a], Ying Wang[a], Qiong-Hua Wang[b,*], Yang Liu[c], Xin Zhou[a]

[a] School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
[b] School of Instrumentation Science and Opto-electronics Engineering, Beihang University, Beijing 100083, China
[c] School of Computer and Information Technology, Liaoning Normal University, Dalian 116082, China

A R T I C L E I N F O

Keywords:
Monospectral image encryption
Hyperchaotic system
Cellular automata
Color image encryption

A B S T R A C T

We propose a monospectral image encryption method in which the multispectral color image acquisition by using heterogeneous monospectral cameras. Because the captured monospectral elemental images (EIs) belongs to grayscale image, it is means that the captured EIs can be directly encrypted by the proposed encoding method. Subsequently, the linear cellular automata (CA) and hyperchaotic encoding algorithm are employed to encrypt the captured EIs. Different from previous methods, the proposed method can directly encrypt the multispectral color information rather than having to divide into three color channels (R, G and B), thereby, the proposed method can greatly reduce the encryption calculation.

1. Introduction

Recently, the multimedia security such as color images is drawing more and more attention because of its importance in various applications such as e-education and military that lead to the importance of real-time and sufficiently secure and robust image encryption methods [1–7]. The color image encryption algorithm is quite different from those of textual or binary data, and that is because of its special features of color images such as large size, high redundancy (three color channels) and large computation [8–23].

Chaos for image security have triggered much interest, such as topological transitivity and random-like behaviors. Considering the features and the performance of the chaotic algorithms, Britain mathematician Matthes [24] firstly introduced chaotic theory for image encryption. After that, lots of image encryption methods based on chaos have been presented [25–27].

It is very vital for an effective encryption method to be sensitive to the encryption keys, thus the key space of the encryption method should be large enough to resist brute-force attacks [28–31]. Recently, cellular automata (CA) based image encryption methods have been presented because of the capacity of parallel calculation and high security. CA are dynamical systems on finite state sets [32–34]. Pseudorandom number obtained by CA, which plays a very important role in image encryption. It is necessary to generate pseudorandom numbers in parallel owing to the emergence of massively parallel computation.

In the pickup process of integral imaging, the researchers utilize the Bayer color filter array (CFA) to capture 3D scene. Then 3D scene can be reconstructed by the computing integral imaging (CIIR) algorithm [35–39]. With the Bayer CFA, color image information can be efficiently acquired from single sensor camera. However, color crosstalk between each of color filters, which reduces the quality of the reconstructed 3D image [38].

In this paper, a monospectral image encryption method is proposed. Different from the previous methods, in our work, the color image is first recoded into monospectral elemental images (EIs) by monospectral camera array. Because EIs belongs to the grayscale image, it can be directly encrypted by the proposed encoding algorithm, rather than having to divide into three color channels (R, G and B). Hence, it will greatly enhance the efficiency of color image encryption. Following that, we propose an improved super-resolution (SR) reconstruction technique to improve the image quality.

2. Description of the monospectral image encryption algorithm

The encryption procedure of the proposed method is summarized in Fig. 1. It can be divided into mainly three procedures: firstly, the color image is captured by heterogeneous monospectral cameras. Secondly, the captured monospectral EIs are encrypted by combining the use of the hyper-chaotic system and the CA encoding algorithm. Thirdly, the color image can be reconstructed by the inverse encoding process of encryption method and the improved SR image reconstruction method.

* Corresponding author.
E-mail address: qionghua@buaa.edu.cn (Q.-H. Wang).

https://doi.org/10.1016/j.optlaseng.2018.09.015
Received 27 July 2018; Received in revised form 10 September 2018; Accepted 18 September 2018
Available online 25 September 2018
0143-8166/

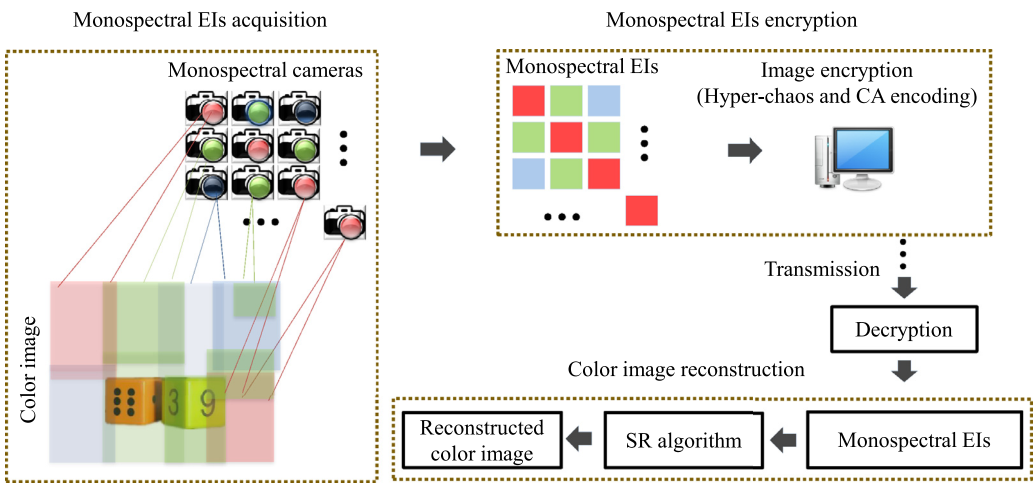

Fig. 1. The implementation principle of the proposed color image encryption. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

The detailed description of the proposed color image encryption is presented below.

2.1. *Monospectral EIs captured by monospectral camera array*

To effectively reduce the color crosstalk, in our work, the monospectral camera is utilized to capture the color image. The left of Fig. 1 shows the monospectral EIs acquisition process through heterogeneous monospectral cameras. In this experiment, we do not use the Bayer color filter pattern of CCD camera; each camera of our proposed image capture method is isolated and only sensitive to just monochromatic color, red, green, or blue. The numbers of luminance sensors (green) of the monospectral camera array are more than the chrominance sensors (red, blue). The reason is that the human eyes are more sensitive to the luminance signals rather than the chrominance signals. For example, in a 4×4 monospectral camera array mode, eight or more sensors are sensitive to green spectrum for the increased image quality requirements. A sub-image array (SIA) is obtained through the monospectral camera array and each sub-image only possesses one of the spectral information (R, G, or B).

2.2. *Monospectral EIs encrypted by linear CA and hyper-chaotic system*

2.2.1. *M-sequence generated by linear CA*

CA can offer significant benefit over existing algorithms [32,33]. In a one-dimensional (1D), two-state, three-site neighbourhood CA, where the next state of a cell is updated according to its neighborhood, the value of each cell is 0 or 1. The value of each cells can be generated by a specified rule. The value of next state is calculated by the Boolean function with three parameters.

$$s_i(t+1) = F(y_{i-1}(t), y_i(t), y_{i+1}(t)), \tag{1}$$

where $s_i(t+1)$ denotes the value of cell i at time $t+1$, $s_i(t)$ denotes the value of the cell i at time t, $y_{i-1}(t)$ is the left neighboring cell value at time t, $s_{i+1}(t)$ is the right neighboring cell value at time t, and $F()$ represents the Boolean function defining a specified rule.

According his theory of Wolfram, for the 2-state, 3-site CA, it has 2^8 rules. The Wolfram rules are defined from 0 to 255. Among the rules, eight Wolfram rules are linear. They are 0, 60, 90, 102, 150, 170, 204, and 240, respectively. The eight Wolfram linear rules are represented as follows:

$$\begin{aligned}
&\texttt{Rule } 0: s_i(t+1) = 0,\\
&\texttt{Rule } 60: s_i(t+1) = s_{i-1}(t) \oplus s_i(t),\\
&\texttt{Rule } 90: s_i(t+1) = s_{i-1}(t) \oplus s_{i+1}(t),\\
&\texttt{Rule } 102: s_i(t+1) = s_i(t) \oplus s_{i+1}(t),\\
&\texttt{Rule } 150: s_i(t+1) = s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t),\\
&\texttt{Rule } 170: s_i(t+1) = s_{i-1}(t),\\
&\texttt{Rule } 204: s_i(t+1) = s_i(t),\\
&\texttt{Rule } 240: s_i(t+1) = s_{t-1}(t).
\end{aligned} \tag{2}$$

Non-uniform CA is a special case of CA where not all cells present the same set of rules and these rules can change and evolve during the time.

The Wolfram rules 0, 60, 102, 170, 204 and 240 cannot produce high quality pseudorandom sequence, due to the combination of these rules cannot generate maximum-length sequences (m-sequences). However, the Wolfram rules 90 and 150 can generate m-sequences. The m-sequence can be generated by a transition matrix, and the transition matrix (T) is written as

$$T(x_n; y_n; z_n) = \begin{bmatrix} y_1 & z_1 & 0 & \cdots & \cdots & 0 & 0 \\ x_2 & y_2 & z_2 & \ddots & & & 0 \\ 0 & x_3 & y_3 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & & y_{n-2} & z_{n-2} & 0 \\ 0 & & & \ddots & x_{n-1} & y_{n-1} & z_{n-1} \\ 0 & 0 & \cdots & \cdots & 0 & x_n & y_n \end{bmatrix} \tag{3}$$

The transition matrix (T) can be re-written according to the rules 90 and 150 as

$$T(d_1, d_2, \ldots, d_{n-1}, d_n) = \begin{bmatrix} d_1 & 1 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & d_2 & 1 & \ddots & & & 0 \\ 0 & 1 & d_3 & \ddots & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & & d_{n-2} & 1 & 0 \\ 0 & & & \ddots & 1 & d_{n-1} & 1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & d_n \end{bmatrix} \tag{4}$$

Each element of the diagonal vector signifies linear rule according to

$$d_i = \begin{cases} 0, & \texttt{rule } 90 \\ 1, & \texttt{rule } 150 \end{cases} \tag{5}$$