International Journal of Computer Vision and Image Processing
Volume 10 • Issue 4 • October-December 2020

Digital Image Encryption Based on Chaotic Cellular Automata

Zubair Jeelani, University of Kashmir, India
https://orcid.org/0000-0003-4600-2899

ABSTRACT

Cellular automata are dynamical systems, discrete in terms of both space and time. Many cellular automata are capable of generating chaos and are well suited for applications like digital image encryption and scrambling. Various cellular automata-based digital image scrambling techniques have been proposed in literature. An adversary may have access to a set of images from which the particular image is scrambled. The problem with these techniques in this particular case is that an adversary may be able to find out the true content of the scrambled image just by comparing its histogram with the histograms of a suspected set of images. In this paper, a secure digital image encryption technique based on outer totalistic cellular automata is proposed that modifies the histogram of the scrambled image so that it is difficult to guess the true content carried in the digital image.

KEYWORDS

Cellular Automata, Entropy, Image Encryption, Image Scrambling

INTRODUCTION

Protection of digital images from malicious entities is an important concern in modern digital space (Saranjame and Das, 2018). Digital image scrambling (DIS) refers to changing the spatial arrangement of pixel intensity values to hide the true content of the image. DIS is used as a pre/ post processing step in the digital image encryption process (Jeelani and Qadir, 2018b) because DIS isn't sufficient to provide a foolproof security to the image content. Basically, DIS just permutes the pixels in a digital image and as such the histogram of the complete image is same before and after the pixel scrambling is done. An adversary may obtain the scrambled image from a storage device or a computer network. Moreover, the adversary may have access to a set of images from which the particular image is scrambled. In such a case, the adversary just needs to compare the histogram of the scrambled image with the histogram of each plain image in the set. This poses a serious security problem and as such DIS must be supplemented with digital image encryption to fully secure the digital images.

Some researchers propose conventional cryptosystems (Jiping *et al*., 2008) to directly encrypt images. But this is not advisable due to large data size and real-time constraints of image data. Conventional cryptosystems need a lot of computational time to directly encrypt thousands of image pixel values. "On the other hand, unlike textual data, a decrypted image is usually acceptable even if it contains small levels of distortion" (Soleymani, Nordin, and Sundararajan, 2014). For all the above mentioned reasons, the algorithms that function well for textual data may not be suitable for multimedia data (Soleymani, Ali, and Nordin, 2012). DIS is computationally less expensive compared to image encryption but can't be used on pixel level directly to encrypt images. Therefore, bit level

DOI: 10.4018/IJCVIP.2020100102

image scrambling (Ping, 2015) has been proposed to use DIS to encrypt images by modifying the histogram of the input image.

The main objective of the work presented in this paper is to propose a secure and robust cellular automata-based digital image encryption algorithm that employs DIS to encrypt digital images. The proposed image encryption system uses the principles of digital image scrambling basically, and therefore, the proposed algorithm is very efficient, fast and simple. A brief introduction of cellular automata and the cellular automata rules used in this work are discussed in the following section.

BACKGROUND

The proposed work is based on the two dimensional outer totalistic cellular automata (2D-OTCA) model. Below, we first discuss the concept of cellular automata (CA) in general. Next, the 2D-OTCA model is introduced and the 2D-OTCA rules used in this work are also introduced in this section. Finally, the review of the related literature is presented in this section.

Cellular Automata

Cellular automata (CA) are mathematical models characterized by discrete time and space units. The discrete space units are called cells and each cell has a cell state at any given time. Each CA cell evolves according to a predefined rule (local transition function) denoted by the δ symbol. The CA rule takes the state of the current cell and state of cells in the local neighborhood of this current cell at time *t*. The CA rule assigns a new state to the current cell at time *t+1* as a function of state of the current cell and states of the neighboring cells at time *t*. Mathematically, a cellular automaton C can be expressed as a quintuple (Ye and Li, 2008) as shown in equation 1.

$$C = (\Sigma, N, \delta, A, G_\delta) \tag{1}$$

where, Σ is the finite set of states a CA cell may assume at any given time; N is the local neighborhood of a cell, where $N = \{c_1, \ldots, c_k\}$ is a finite subset of the CA lattice; $\delta: \Sigma^N \rightarrow \Sigma$ is the local transition function which determines the next state of the cell under consideration at next time step; A is the configuration set; and, G_δ is the global mapping.

Cellular automata have been successfully used to solve a wide variety of image processing problems including noise filtration (Jeelani and Qadir (2018a)), digital image forgery (Gani and Qadir (2020)) and digital image scrambling (Jeelani and Qadir (2020)). In the following sub section, we discuss the important CA model that is used in our proposed work; the two-dimensional outer totalistic cellular automata (2D -OTCA).

Two-Dimensional Outer Totalistic Cellular Automata

Two – dimensional outer totalistic cellular automata (2D–OTCA) consists of a rectangular lattice of cells. The cells in the rectangular grid are also rectangular in shape. The local transition function (δ) used to update the state of a cell C(*i*,*j*) in 2D–OTCA is shown in Equation 2.

$$C\left(i,j\right)^{t+1} = (C\left(i,j\right)^{t}, \sum_{i',j'} C\left(i',j'\right)^{t}) \tag{2}$$

The local transition function (δ) calculate the new state of the cell C(*i*,*j*) at time step *t+1* as a function of the states of the cell C(*i*,*j*) and cells in its local neighborhood at time step *t*.δ is applied to each cell in the 2D-OTCA synchronously so that each cell receives an updated state at the next time step. There are many different ways to select the local neighborhood cells for a particular cell

Related Content

Theoretical Concepts and Technical Aspects on Image Segmentation
Anju Pankaj and Sonal Ayyappan (2018). *Computer Vision: Concepts, Methodologies, Tools, and Applications (pp. 2333-2348).*
www.igi-global.com/chapter/theoretical-concepts-and-technical-aspects-on-image-segmentation/197054?camid=4v1a

Three-Dimensional Face Shape by Local Fitting to a Single Reference Model
Rubén García-Zurdo (2014). *International Journal of Computer Vision and Image Processing (pp. 17-29).*
www.igi-global.com/article/three-dimensional-face-shape-by-local-fitting-to-a-single-reference-model/111473?camid=4v1a

Part-Based Lumbar Vertebrae Tracking in Videofluoroscopy Using Particle Filter
Ibrahim Guelzim, Amina Amkoui and Hammadi Nait-Charif (2020). *International Journal of Computer Vision and Image Processing (pp. 29-44).*
www.igi-global.com/article/part-based-lumbar-vertebrae-tracking-in-videofluoroscopy-using-particle-filter/252232?camid=4v1a

Shape Codification Indexing and Retrieval Using the Quad-Tree Structure
Saliha Aouat (2013). *International Journal of Computer Vision and Image Processing (pp. 1-21).*
www.igi-global.com/article/shape-codification-indexing-retrieval-using/78367?camid=4v1a