mathematics

MDPI

Article

Reversibility of Symmetric Linear Cellular Automata with Radius $r = 3$

A. Martín del Rey [1,*,†], R. Casado Vara [2,†] and D. Hernández Serrano [3,†]

1 Department of Applied Mathematics, IUFFyM, University of Salamanca, 37008-Salamanca, Spain
2 BISITE Research Group, University of Salamanca, 37008-Salamanca, Spain; rober@usal.es
3 Department of Mathematics, IUFFyM, University of Salamanca, 37008-Salamanca, Spain; dani@usal.es
* Correspondence: delrey@usal.es
† Authors contributed equally to this work.

Received: 31 July 2019; Accepted: 31 August 2019; Published: 3 September 2019

Abstract: The aim of this work is to completely solve the reversibility problem for symmetric linear cellular automata with radius $r = 3$ and null boundary conditions. The main result obtained is the explicit computation of the local transition functions of the inverse cellular automata. This allows introduction of possible and interesting applications in digital image encryption.

Keywords: linear cellular automata; reversibility; symmetric rules

1. Introduction and Preliminaries

The notion of cellular automaton was originated by Von Neumann and S. Ulam [1], and it can be defined as a simple computational model capable of simulating complex phenomena. This concept was popularized in the seventies by M. Gardner with John Conway's Game of Life [2], and was brought into academic fashion by S. Wolfram [3] in the eighties. Since then, cellular automata have been extensively analyzed, and not only from a theoretical perspective [4,5]; they have also been used to simulate different phenomena [6–8].

One can find different definitions of cellular automaton depending on the perspective [9]. J. Kari defines them as ultradiscrete dynamical systems that consist of a finite collection of state automata (called cells) that are endowed with a state at every time step and these states change according to a local transition function. The variables of this function are the states at the previous step of time of the cell itself and its neighborhood.

More precisely, a cellular automaton over the finite field $\mathbb{F}_2 = \{0,1\}$ is given by a 3-uplet $\mathcal{A} = (\mathcal{C}, f, \mathcal{N})$, such that $\mathcal{C}$ is the cellular space, f is the local transition function, and $\mathcal{N}$ is the neighborhood. Specifically, $\mathcal{C}$ is formed by n cells that are arranged uniformly in a one-dimensional lattice. Each of them is endowed with a state from $\mathbb{F}_2$ that changes at every step of time according to a local transition function f. Specifically, if s_i^t stands for the state of the i-th cell at time t, then

$$s_i^{t+1} = f\left(s_{i-k^-}^t, \ldots, s_{i-1}^t, s_i^t, s_{i+1}^t, \ldots, s_{i+k^+}^t\right), \quad 1 \leq i \leq n, \tag{1}$$

where $k^-, k^+ \in \mathbb{N}$, and $\mathcal{N}(i) = \{i-k^-, \ldots, i-1, i, i+1, \ldots, i+k^+\}$ represent the neighborhood of the i-th cell. As the cellular space is constituted by n cells (the cellular space is finite), some type of boundary conditions must be stated in order to define the dynamics of the system in a proper way. This work deals with null boundary conditions, that is, $s_i^t = 0$ for each t when $i \notin \{1, 2, \ldots, n\}$.

The cellular automaton is linear when its local transition function f is linear. Moreover, a linear cellular automaton is said to be symmetric of radius r if $k^- = k^+ = r$. Consequently, its local transition function is

$$s_i^{t+1} = \bigoplus_{k=-r}^{r} \lambda_k s_{i+k}^t, \quad \lambda_k \in \mathbb{F}_2, \quad 1 \leq i \leq n. \tag{2}$$

This cellular automaton will be denoted by $\mathcal{A}_{n,r}$. Note that we are dealing with 1D boolean cellular automata.

If $C^t = \left(s_1^t, s_2^t, \ldots, s_n^t\right) \in \mathbb{F}_2^n$ is the global configuration of $\mathcal{A}_{n,r}$ at step of time t, the local transition function leads to global transition function F, such that

$$\begin{array}{rcl} F\colon \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ C^t & \mapsto & C^{t+1} = F\left(C^t\right) \end{array} \tag{3}$$

The graphical illustration of the global evolution of a CA can be obtained using the simple evolution diagram and the global state transition diagram. The evolution diagram is a two-dimensional grid, where the rows represent the configurations of the cellular automaton (that are sequentially computed from the initial configuration) such that the color of each site is black for state 1 or white for state 0. On the other hand, the global state transition diagram can be defined as a directed graph whose nodes represent the configurations of the cellular automaton and whose edges represent transformations $C^t \mapsto C^{t+1}$.

If the global transition function F is bijective, the cellular automaton is said to be reversible. Thus, the evolution backwards can be computed by means of the inverse cellular automaton whose global transition function is F^{-1} [10,11]. Reversibility is probably the most studied property of cellular automata; not only have several theoretical works appeared (see, for example, works by the authors of [12–16]), but different applications based on this property have also been proposed (see, for example, work by the authors of [17–20]).

The reversibility problem for symmetric linear cellular automata endowed with periodic boundary conditions has been tackled in several works [21–24] and completely solved by I. Siap, H. Akin, and M.E. Koroglu [25] and the explicit expressions for the inverse of a reversible cellular automaton with $(2r+1)$-cyclic rule are given in the work by the authors of [23]. On the other hand, in the case of null boundary conditions, the cases $r = 1$ and $r = 2$ have been tackled in works by the authors of [26,27]; moreover, in the work by the authors of [28], it is shown that the symmetric linear cellular automaton of radius r, whose cellular space is formed by $n = 2r + 1$ cells, is reversible.

The main objective of this work is to completely solve the reversibility problem for the symmetric linear cellular automaton with n cells and radius $r = 3$, which is denoted by $\mathcal{A}_{n,3}$. Specifically, the explicit expressions of the local transition matrices of the inverse cellular automata are computed, and an illustrative application of this result to the encryption of digital images is proposed.

The rest of the paper is organized as follows. Section 2 is devoted to introduce the particular characteristics of symmetric cellular automata with radius $r = 3$ and endowed with null boundary conditions; the reversibility problem is tackled in Section 3. In Section 4, some potential applications in the field of digital image encryption are shown. Finally, the conclusions are presented in Section 5.

2. The Symmetric Linear Cellular Automata with $r = 3$

The explicit expression of the local transition function of the symmetric cellular automaton with radius $r = 3$ and n cells, $\mathcal{A}_{n,r}$, is as follows.

$$s_i^{t+1} = s_{i-3}^t \oplus s_{i-2}^t \oplus s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t \oplus s_{i+2}^t \oplus s_{i+3}^t = s_i^t \oplus \bigoplus_{k=1}^{3} \left(s_{i-k}^t \oplus s_{i+k}^t\right), \; 1 \leq i \leq n. \tag{4}$$

If $C^t = \left(s_1^t, s_2^t, \ldots, s_n^t\right)$, $\in \mathbb{F}_2^n$ is the global configuration of the cellular automaton at step of time t, then its global evolution is given by

$$C^{t+1} = F\left(C^t\right) = M_n \cdot C^t, \tag{5}$$

where M_n is the local transition matrix. If null boundary conditions are considered, then M_n is a band matrix of order n with bandwidth $r = 3$ whose coefficients inside the band are all equal to 1, that is,

$$M_n = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \ddots & \ddots & & & & \vdots \\ 1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & & & \vdots \\ 1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\ \vdots & & & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\ \vdots & & & & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_n\left(\mathbb{Z}_2\right). \tag{6}$$

In Figure 1a, the evolution state diagram of the cellular automaton $\mathcal{A}_{201,3}$ is shown when the initial configuration is given by $C^0 = \left(0, \overset{(100)}{\cdots}, 0, 1, 0, \overset{(100)}{\cdots}, 0\right)$. Furthermore, in Figure 1b, the evolution state diagram associated to $\mathcal{A}_{201,3}$ is introduced when the initial configuration C^0 is randomly defined.

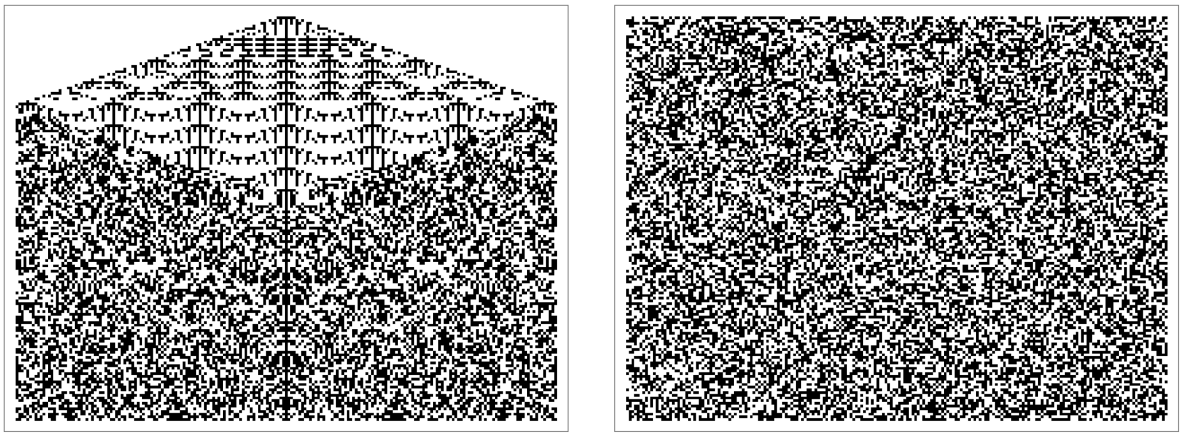

Figure 1. (**a**) Evolution diagram of $\mathcal{A}_{201,3}$ when $C^0 = \left(0, \overset{(100)}{\cdots}, 0, 1, 0, \overset{(100)}{\cdots}, 0\right)$. (**b**) Evolution diagram of $\mathcal{A}_{201,3}$ when the initial configuration is selected at random.

3. The Reversibility Problem

Taking into account the notion of reversibility and the interpretation of the dynamics of $\mathcal{A}_{n,r}$ in terms of linear algebra, this cellular automaton is said to be reversible when its local transition matrix is nonsingular, and consequently its inverse is the local transition matrix of the inverse cellular automaton. Consequently, in this case, the order and characteristics of the transition matrix determine the reversibility of the cellular automata. For example, $\mathcal{A}_{7,3}$ and $\mathcal{A}_{8,3}$ are reversible, whereas $\mathcal{A}_{9,3}$ is not. In Figures 2 and 3, the global state transition diagrams of $\mathcal{A}_{7,3}$ and $\mathcal{A}_{8,3}$ are shown; note that

as they are reversible, each configuration $C = (s_1, s_2, \ldots, s_n) \in \mathbb{F}_2^n$ is represented by the number $\sum_1^n s_i 2^i$. Conversely, $\mathcal{A}_{9,3}$ is not reversible, and some configurations in the global state transition diagram have more than one predecessor (see Figure 4).

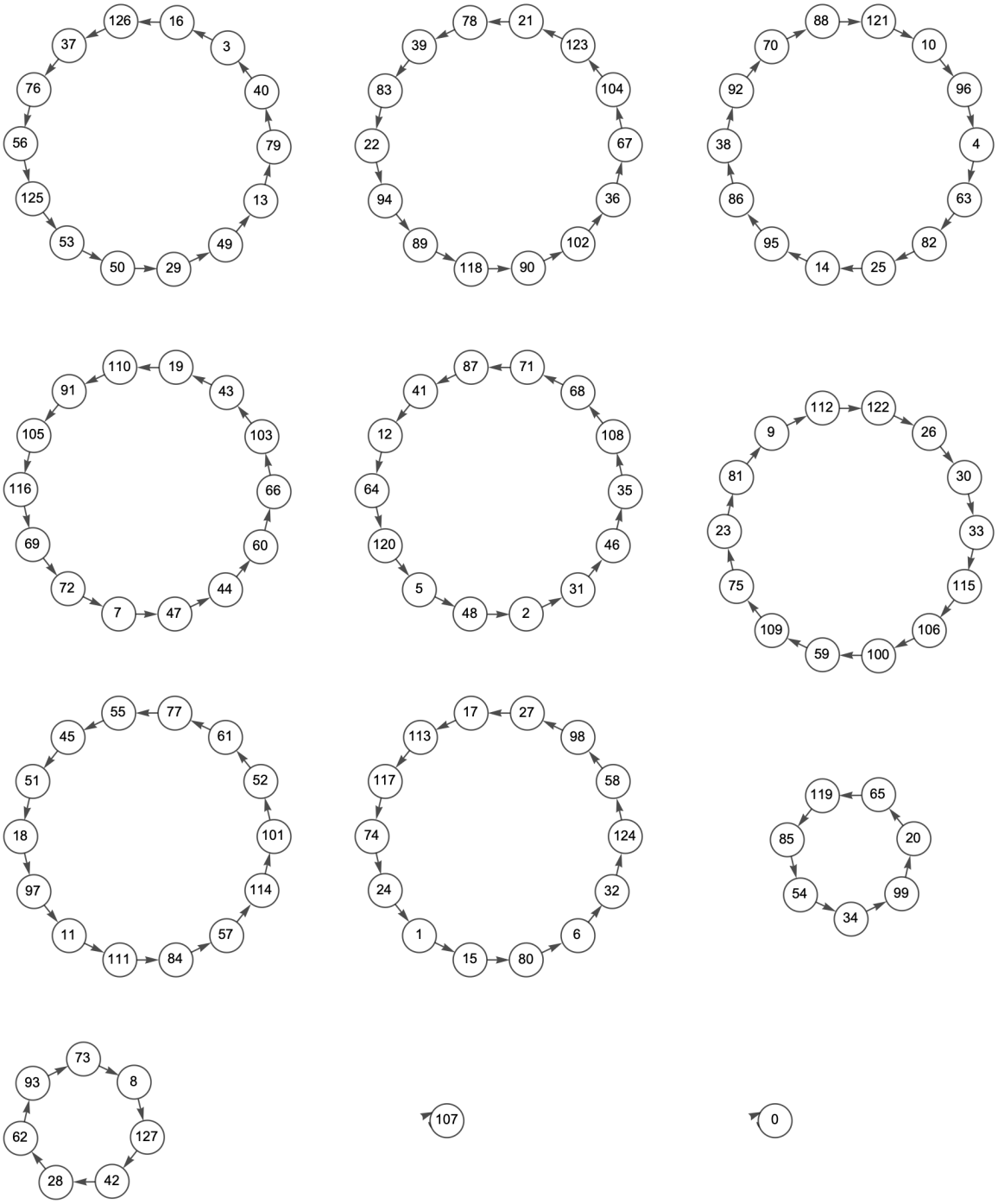

Figure 2. Global state transition diagram of $\mathcal{A}_{7,3}$.

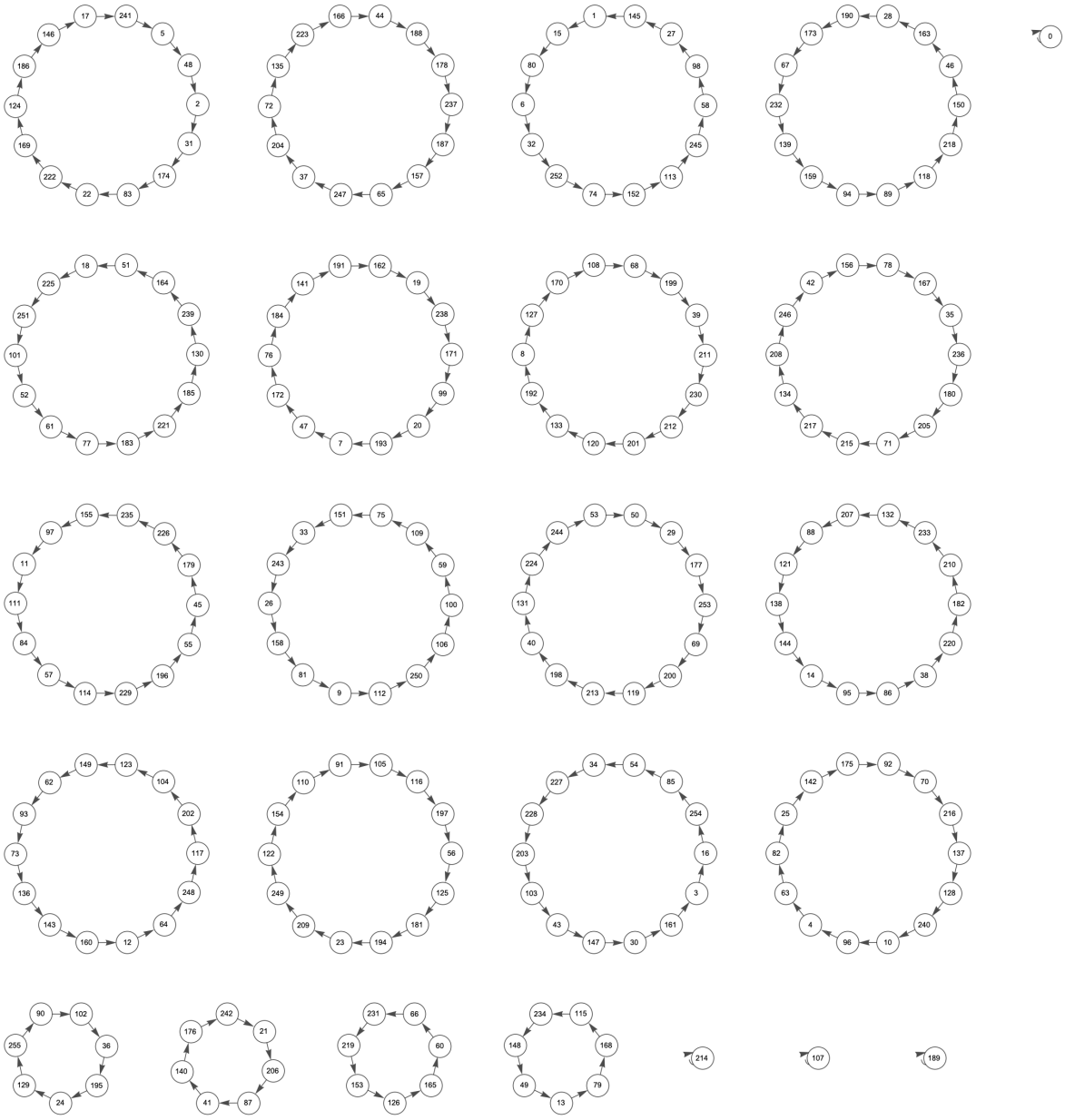

Figure 3. Global state transition diagram of $\mathcal{A}_{8,3}$.

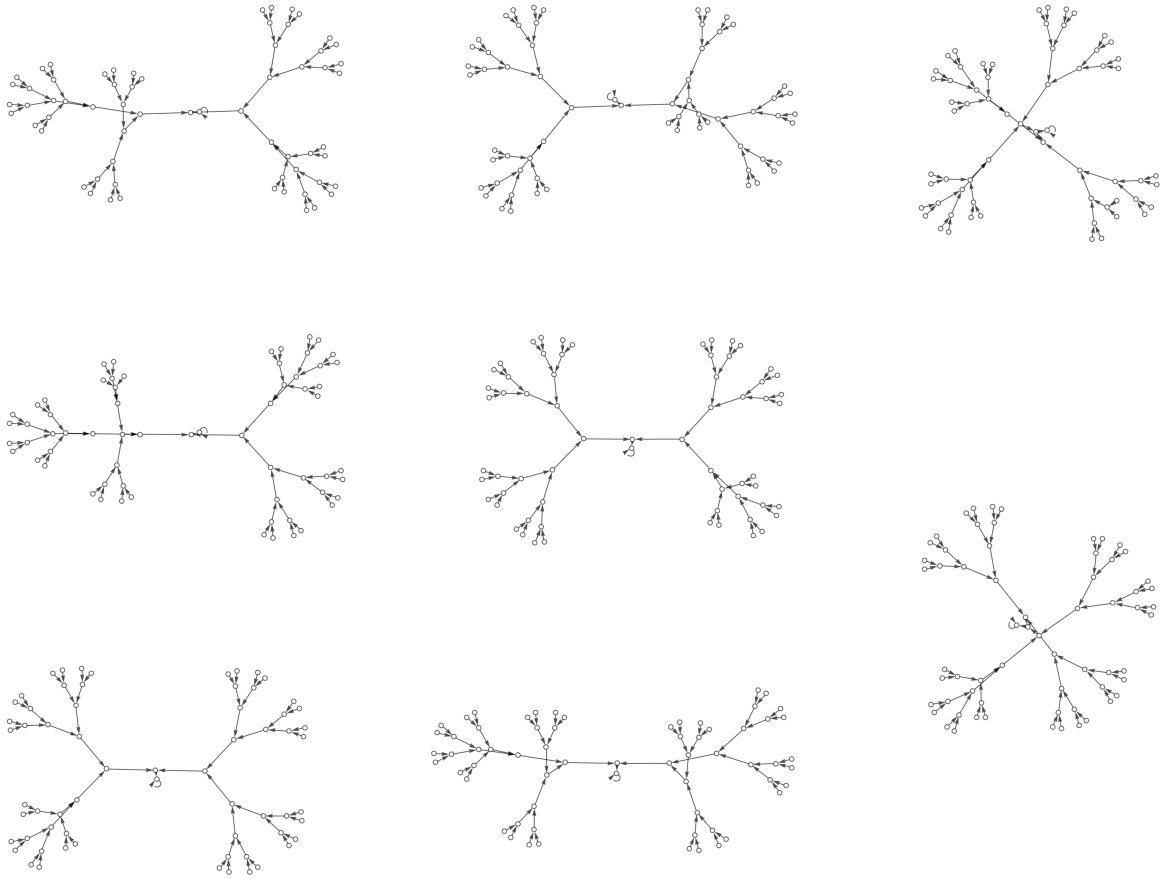

Figure 4. Global state transition diagram of $\mathcal{A}_{9,3}$.

Specifically, the following result holds.

Theorem 1. *The symmetric linear cellular automaton with $r = 3$, $\mathcal{A}_{n,3}$, is reversible if and only if $n = 7k$ or $n = 7k + 1$, with $k \in \mathbb{Z}^+$.*

Proof. Assume that the arithmetic is performed in $\mathbb{F}_2$ and set M_n the transition matrix of $\mathcal{A}_{n,r}$. From Lemma (2) of the work by the authors of [28], it is $\det(M_n) = \det\left(M_{n-(2r+1)}\right)$. Consequently, if $n = (2r+1)m + p$ with $m \in \mathbb{N}$ and $0 \leq p \leq 2r$, then $\det(M_n) = \det\left(M_{(2r+1)+p}\right)$. A simple computation shows that

$$\det(M_n) = \det\left(M_{(2r+1)+p}\right) = \begin{cases} 1, & \text{if } p = 0, 1 \\ 0, & \text{if } 2 \leq p \leq 2r \end{cases} \tag{7}$$

Consequently,

$$\det(M_n) = \begin{cases} 1, & \text{if } n = (2r+1)m \text{ or } n = (2r+1)m + 1 \text{ with } m \in \mathbb{Z}^+ \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

thus finishing, taking $r = 3$. □

Furthermore, it is possible to compute in an explicit way the expression of the inverse cellular automata as follows.

Theorem 2. *(1) The local transition matrix of the inverse cellular automaton when $n = 7k$, $k \in \mathbb{Z}^+$ is*

$$I_{7k} = \begin{pmatrix} I_7 & H & \overset{(k-1)}{\cdots} & H \\ H^T & I_7 & \ddots & \vdots \\ \vdots & \ddots & \ddots & H \\ H^T & \underset{(k-1)}{\cdots} & H^T & I_7 \end{pmatrix} \in \mathcal{M}_{7k}(\mathbb{Z}_2), \tag{9}$$

where

$$I_7 = \begin{pmatrix} 0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&0&1&1 \\ 1&0&0&1&0&0&1 \\ 1&1&0&0&0&0&0 \\ 0&1&1&0&0&0&0 \\ 0&0&1&1&0&0&0 \end{pmatrix} \in \mathcal{M}_7(\mathbb{Z}_2), \quad H = \begin{pmatrix} 0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \end{pmatrix} \in \mathcal{M}_7(\mathbb{Z}_2). \tag{10}$$

(2) The local transition matrix of the inverse cellular automaton when $n = 7k+1$, $k \in \mathbb{Z}^+$ is

$$I_{7k+1} = \begin{pmatrix} I_8 & J & J & \overset{(k-2)}{\cdots} & J \\ J^T & K_7 & L & \cdots & L \\ J^T & L^T & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & L \\ J^T & L^T & \underset{(k-2)}{\cdots} & L^T & K_7 \end{pmatrix} \in \mathcal{M}_{7k+1}(\mathbb{Z}_2), \tag{11}$$

where

$$I_8 = \begin{pmatrix} 1&0&0&0&1&0&0&1 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&1 \\ 1&1&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&0&0&1&0&0&0&1 \end{pmatrix} \in \mathcal{M}_8(\mathbb{Z}_2), \tag{12}$$

$$J = \begin{pmatrix} 0&0&0&1&0&0&1 \\ 0&0&0&1&1&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&1&0&0&1 \end{pmatrix} \in \mathcal{M}_{8\times 7}(\mathbb{Z}_2), \tag{13}$$

$$K_7 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathcal{M}_7(\mathbb{Z}_2), \tag{14}$$

$$L = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in \mathcal{M}_7(\mathbb{Z}_2). \tag{15}$$

Proof. (1) For the sake of simplicity, we can suppose that $I_{7k} = \left(\Omega_{ij}\right)_{1\leq i,j\leq k}$ where $\Omega_{ij} \in \mathcal{M}_7(\mathbb{Z}_2)$ is defined as follows.

$$\Omega_{ij} = \begin{cases} I_7, & \text{if } i = j \\ H, & \text{if } i < j \\ H^T, & \text{if } i > j \end{cases} \tag{16}$$

On the other hand, set

$$M_{7k} = \left(\Delta_{ij}\right)_{1\leq i,j\leq k} = \begin{pmatrix} M_7 & N & \mathbf{0} & \overset{(k-2)}{\cdots} & \mathbf{0} \\ N^T & M_7 & N & \ddots & \vdots \\ \mathbf{0} & N^T & \ddots & \ddots & \mathbf{0} \\ \vdots & \ddots & \ddots & \ddots & N \\ \mathbf{0} & \underset{(k-2)}{\cdots} & \mathbf{0} & N^T & M_7 \end{pmatrix} \in \mathcal{M}_{7k}(\mathbb{Z}_2), \tag{17}$$

the local transition matrix of the CA $\mathcal{A}_{7k,3}$, such that

$$\Delta_{ij} = \begin{cases} M_7, & \text{if } i = j \\ N, & \text{if } j = i+1 \\ N^T, & \text{if } j = i-1 \\ 0, & \text{otherwise} \end{cases} \tag{18}$$

with

$$N = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_7(\mathbb{Z}_2). \tag{19}$$

Then we have to proof that $I_{7k} \cdot M_{7k} = M_{7k} \cdot I_{7k} = Id \in \mathcal{M}_{7k}(\mathbb{Z}_2)$.

First of all, suppose that $I_{7k} \cdot M_{7k} = \left(\Phi_{ij}\right)_{1\leq i,j\leq k}$ such that $\Phi_{ij} \in \mathcal{M}_7\left(\mathbb{Z}_2\right)$, then

$$\Phi_{ij} = \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{lj}. \tag{20}$$

Now, we can distinguish five cases depending on the values of subindices i and j:

(a) Assume $i = j$, then

$$\Phi_{ii} = \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{li} = \Omega_{i,i-1} \cdot \Delta_{i-1,i} + \Omega_{ii} \cdot \Delta_{ii} + \Omega_{i,i+1} \cdot \Delta_{i+1,i}, \tag{21}$$

since $\Delta_{ij} = 0$ when $|i - j| > 1$. Then, taking into account Equations (16) and (18), it is

$$\Phi_{ii} = H^T \cdot N + I_7 \cdot M_7 + H \cdot N^T = Id \in \mathcal{M}_7\left(\mathbb{Z}_2\right). \tag{22}$$

(b) Suppose that $j = i + 1$ (the coefficients of the first upper diagonal of $I_{7k} \cdot M_{7k}$), then from Equations (16) and (18) we obtain

$$\begin{aligned} \Phi_{i,i+1} &= \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{l,i+1} = \Omega_{ii} \cdot \Delta_{i,i+1} + \Omega_{i,i+1} \cdot \Delta_{i+1,i+1} + \Omega_{i,i+2} \cdot \Delta_{i+2,i+1} \\ &= I_7 \cdot N + H \cdot M_7 + H \cdot N^T = \mathbf{0} \in \mathcal{M}_7\left(\mathbb{Z}_2\right). \end{aligned} \tag{23}$$

(c) If $j = i - 1$ (the coefficients of the first lower diagonal of $I_{7k} \cdot M_{7k}$), then, using Equations (16) and (18), the following result holds.

$$\begin{aligned} \Phi_{i,i-1} &= \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{l,i-1} = \Omega_{i,i-2} \cdot \Delta_{i-2,i-1} + \Omega_{i,i-1} \cdot \Delta_{i-1,i-1} + \Omega_{ii} \cdot \Delta_{i,i-1} \\ &= H^T \cdot N^T + H^T \cdot M_7 + I_7 \cdot N^T = \mathbf{0} \in \mathcal{M}_7\left(\mathbb{Z}_2\right). \end{aligned} \tag{24}$$

(d) Now we will compute the coefficients Φ_{ij} with $3 \leq i \leq k$ and $1 \leq j \leq i - 2$ corresponding to the entries below the first lower diagonal. In this case

$$\begin{aligned} \Phi_{ij} &= \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{l,j} = \Omega_{i,j-1} \cdot \Delta_{j-1,j} + \Omega_{ij} \cdot \Delta_{jj} + \Omega_{i,j+1} \cdot \Delta_{j+1,j} \\ &= \begin{cases} \Omega_{i1} \cdot \Delta_{11} + \Omega_{i2} \cdot \Delta_{21} = H^T \cdot M_7 + H^T \cdot N^T, & \text{if } j = 1 \\ \Omega_{i,j-1} \cdot \Delta_{j-1,j} + \Omega_{ij} \cdot \Delta_{jj} + \Omega_{i,j+1} \cdot \Delta_{j+1,j} = H^T \cdot N + H^T \cdot M_7 + H^T \cdot N^T, & \text{if } 2 \leq j \leq i-2 \end{cases} \\ &= \mathbf{0} \in \mathcal{M}_7\left(\mathbb{Z}_2\right). \end{aligned} \tag{25}$$

(e) Finally consider the coefficients above the first upper diagonal, Φ_{ij} with $1 \leq i \leq k - 2$ and $i + 2 \leq j \leq k$. A similar calculus shows that

$$\begin{aligned} \Phi_{ij} &= \sum_{l=1}^{k} \Omega_{il} \cdot \Delta_{l,j} = \Omega_{i,j-1} \cdot \Delta_{j-1,j} + \Omega_{ij} \cdot \Delta_{jj} + \Omega_{i,j+1} \cdot \Delta_{j+1,j} \\ &= \begin{cases} \Omega_{i,j-1} \cdot \Delta_{j-1,j} + \Omega_{ij} \cdot \Delta_{jj} + \Omega_{i,j+1} \cdot \Delta_{j+1,j} = H \cdot N + H \cdot M_7 + H \cdot N^T, & \text{if } i+2 \leq j \leq k-1 \\ \Omega_{i,k-1} \cdot \Delta_{k-1,k} + \Omega_{ik} \cdot \Delta_{kk} = H \cdot N + H \cdot M_7, & \text{if } j = k \end{cases} \\ &= \mathbf{0} \in \mathcal{M}_7\left(\mathbb{Z}_2\right). \end{aligned} \tag{26}$$

Consequently,

$$\Phi_{ij} = \begin{cases} Id, & \text{if } i = j \\ \mathbf{0}, & \text{if } i \neq j \end{cases} \tag{27}$$

thus $I_{7k} \cdot M_{7k} = Id \in \mathcal{M}_{7k}\left(\mathbb{Z}_2\right)$. In a similar way, one can check that $M_{7k} \cdot I_{7k} = Id \in \mathcal{M}_{7k}\left(\mathbb{Z}_2\right)$.

(2) First of all, note that the local transition matrix of the inverse cellular automaton can be expressed in terms of a block matrix, as follows.

$$I_{7k+1} = \begin{pmatrix} I_{7k} & [J^T L^{T^{\overset{(k-1)}{\cdots}}} L^T]^T \\ [J^T L^{T^{\overset{(k-1)}{\cdots}}} L^T] & K_7 \end{pmatrix} \tag{28}$$

where $[J^T L^{T^{\overset{(k-1)}{\cdots}}} L^T] \in \mathcal{M}_{7,7k}(\mathbb{Z}_2)$. On the other hand, it is also easy to check that

$$M_{7k+1} = \begin{pmatrix} M_{7k} & [0^{\overset{(k-1)}{\cdots}} 0\, Q^T]^T \\ [0^{\overset{(k-1)}{\cdots}} 0\, Q^T] & M_7 \end{pmatrix} \tag{29}$$

where

$$Q = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_{8,7}(\mathbb{Z}_2). \tag{30}$$

To finish the proof, we have to prove that $I_{7k+1} \cdot M_{7k+1} = M_{7k+1} \cdot I_{7k+1} = \mathbf{0}$. Note that

$$I_{7k+1} \cdot M_{7k+1} = \begin{pmatrix} I_{7k} \cdot M_{7k} + [J\, L^{\overset{(k-2)}{\cdots}} L]^T \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q^T] & I_{7k} \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q]^T + [J\, L^{\overset{(k-2)}{\cdots}} L]^T \cdot M_7 \\ [J^T L^{T^{\overset{(k-2)}{\cdots}}} L^T] \cdot M_{7k} + K_7 \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q^T] & [J^T L^{T^{\overset{(k-2)}{\cdots}}} L^T] \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q]^T + K_7 \cdot M_7 \end{pmatrix}. \tag{31}$$

Now, by recurrence over k it is easy to check that

$$Id = I_{7k} \cdot M_{7k} + [J\, L^{\overset{(k-2)}{\cdots}} L]^T \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q^T] \in \mathcal{M}_{7k}(\mathbb{Z}_2), \tag{32}$$

$$Id = [J^T L^{T^{\overset{(k-2)}{\cdots}}} L^T] \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q]^T + K_7 \cdot M_7 \in \mathcal{M}_7(\mathbb{Z}_2), \tag{33}$$

$$\mathbf{0} = I_{7k} \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q]^T + [J\, L^{\overset{(k-2)}{\cdots}} L]^T \cdot M_7 \in \mathcal{M}_{7k,7}(\mathbb{Z}_2), \tag{34}$$

$$\mathbf{0} = [J^T L^{T^{\overset{(k-2)}{\cdots}}} L^T] \cdot M_{7k} + K_7 \cdot [0^{\overset{(k-2)}{\cdots}} 0\, Q^T] \in \mathcal{M}_{7,7k}(\mathbb{Z}_2), \tag{35}$$

thus finishing. A similar argument shows that $M_{7k+1} \cdot I_{7k+1} = \mathbf{0}$. □

4. A Potential Application to Image Encryption

This section introduces a possible application for image encryption of the theoretical results shown in Section 3. J. Fridrich proposed a methodology to design cryptographic protocols for digital images consisting of the successive application of two phases: the confusion phase and the diffusion phase [29]. In the confusion phase, all pixels of the digital image are permuted without changing its numerical color code (that is the histogram of the image remains constant), whereas, in the diffusion phase, the color code of each pixel is modified according to different mathematical techniques. This paradigm has been considered in the great majority of digital image encryption protocols proposed in the scientific literature (see, for example, works by the authors of [30,31]).

A gray-scale digital image can be interpreted as an $r \times s$ matrix $Y = (Y_{ij})_{1 \le i \le r, 1 \le j \le s}$, where the coefficient $Y_{ij} \in \mathbb{Z}_{256}$ represents the numeric value of the gray level assigned to pixel (i, j). On the other hand, an RGB color digital image is defined by means of an array $X = (X_{ij})_{1 \le i \le r, 1 \le j \le s}$ of dimension

$r \times s$, such that $X_{ij} = (R_{ij}, G_{ij}, B_{ij}) \in \mathbb{Z}_{256} \times \mathbb{Z}_{256} \times \mathbb{Z}_{256}$. In this case, the coordinates of X_{ij} denote the intensity of each color (red, green, and blue, respectively) as an integer between 0 and 255.

The reversibility of $\mathcal{A}_{8,3}$ (whose global transition function is denoted by F_8) shown in the last section allows defining a byte-level transformation $\mathcal{T}$ that could be used as a part of the diffusion phase of an encryption algorithm for both gray-scale and RGB color digital images. It is defined as follows.

(a) If $Y \in \mathcal{M}_{r,s}(\mathbb{Z}_{256})$ stands for the matrix associated to a gray-scale image, then the transformed image is defined by the matrix $\mathcal{T}(Y) = \left(\tilde{Y}_{ij}\right)_{1 \leq i \leq r, 1 \leq j \leq s} \in \mathcal{M}_{r,s}(\mathbb{Z}_{256})$, $\tilde{Y}_{ij}$ is the decimal expression associated to $F_8^k(C_{ij})$, C_{ij} is the binary expression (one byte) associated to Y_{ij}, and $k \in \mathbb{Z}^+$.

(b) If $X = \left(X_{ij}\right)_{1 \leq i \leq r, 1 \leq j \leq s}$ is the array representing an RGB color digital image, then $\mathcal{T}(X) = \left(\tilde{X}_{ij}\right)_{1 \leq i \leq r, 1 \leq j \leq s}$ determines the transformed digital image, such that $\tilde{X}_{ij} = \left(\tilde{R}_{ij}, \tilde{G}_{ij}, \tilde{B}_{ij}\right)$ with

$$\tilde{R}_{ij} = \text{decimal expression associated to } F_8^k\left(C_{ij}^R\right), \tag{36}$$

$$\tilde{G}_{ij} = \text{decimal expression associated to } F_8^k\left(C_{ij}^G\right), \tag{37}$$

$$\tilde{B}_{ij} = \text{decimal expression associated to } F_8^k\left(C_{ij}^B\right), \tag{38}$$

where C_{ij}^R, C_{ij}^G, and C_{ij}^B are the binary expressions of R_{ij}, G_{ij}, and B_{ij}, and $k \in \mathbb{Z}^+$, respectively.

In Figures 5 and 6, two illustrative examples of this technique are shown. As the global state transition diagram of $\mathcal{A}_{8,3}$ exhibits 16 cycles of length 14, four cycles of length 7, and four time-invariant configurations (see Figure 3), $\mathcal{T}$ is a periodic transformation of period 14. As a consequence, the original image is recovered after 14 iterations.

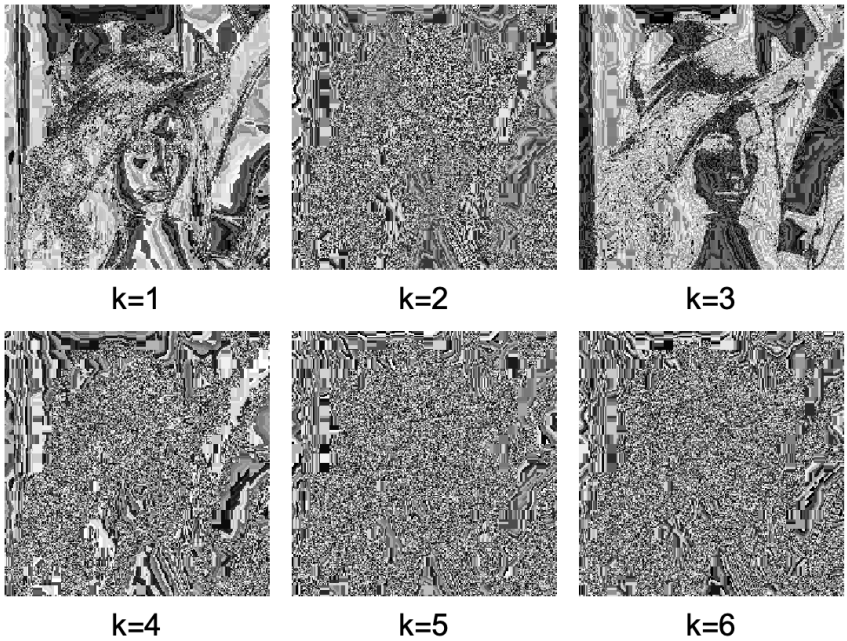

Figure 5. *Cont.*

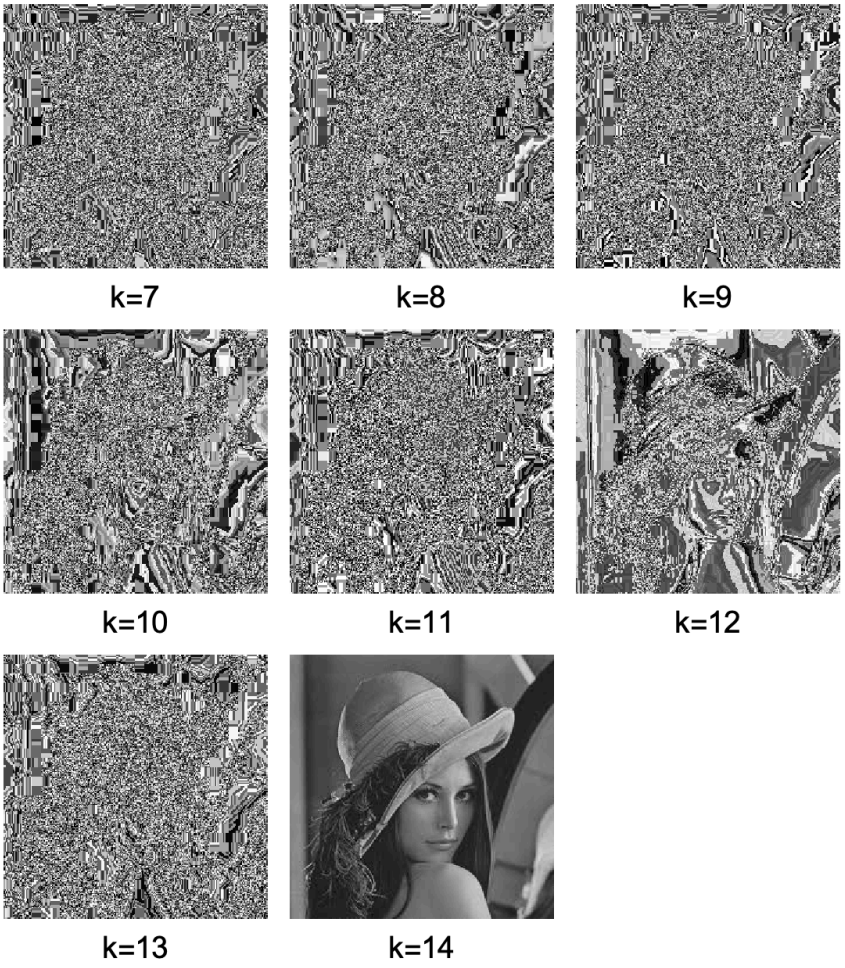

Figure 5. Gray-scale images obtained by applying $\mathcal{A}_{8,3}$.

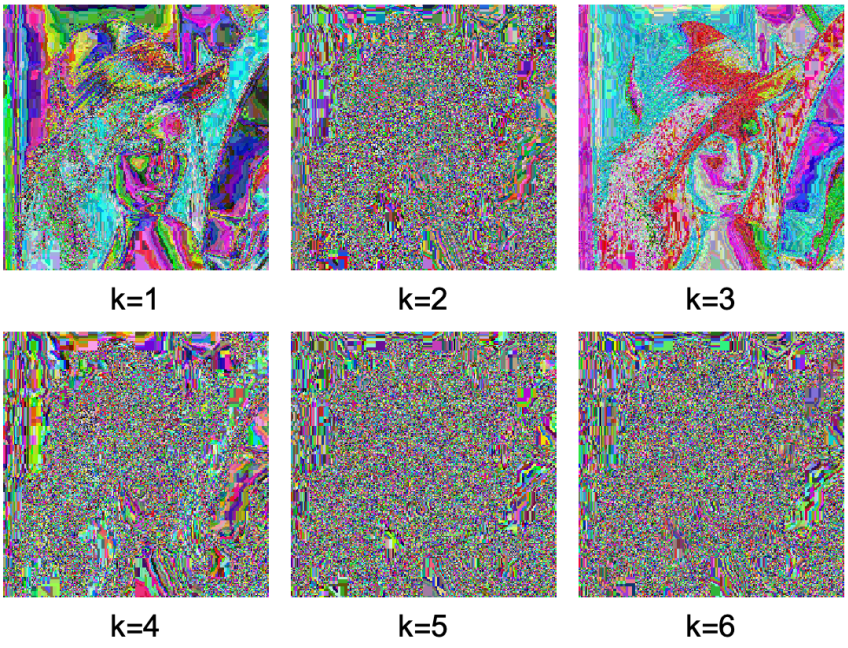

Figure 6. *Cont*.

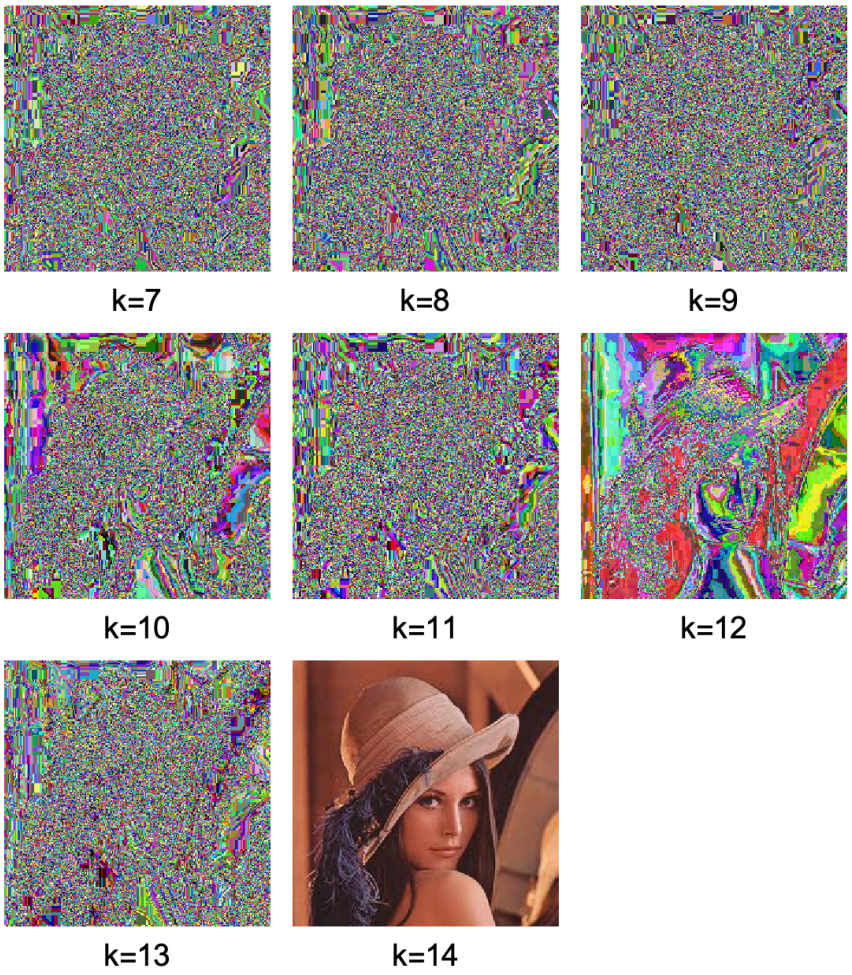

Figure 6. Color images obtained by applying $\mathcal{A}_{8,3}$.

It is important to note that this transformation by itself is not secure against cryptanalysis (see, for example, the homogeneous patterns exhibited by some transformed images in the examples). In this sense, it is necessary to include it as a part of a more complex algorithm.

5. Conclusions

In this work, the reversibility problem for symmetric linear cellular automata with n cells, radius $r = 3$, and state set $\mathbb{F}_2$ has been completely solved. Specifically, it is shown that these 1D boolean cellular automata are reversible when $n = 7k$ or $n = 7k + 1$ with $k \in \mathbb{Z}^+$, and, in these cases, the explicit expressions of the inverse cellular automata are derived in terms of the local transition matrices.

Furthermore, a potential application to Cryptography has been presented. Specifically, these reversible cellular automata can be used as additional transformations to be applied in the diffusion phase of a digital image encryption algorithm.

Future work aims at exploring other applications of reversible cellular automata, such as voting systems, data compression, etc.

Author Contributions: A.M.d.R., R.C.V., and D.H.S. conceived and designed the study and A.M.d.R. performed the computational implementations. The paper has been written, edited, and revised by all authors.

Funding: This research was funded by Ministerio de Ciencia, Innovación y Universidades (MCIU, Spain), Agencia Estatal de Investigación (AEI, Spain), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project TIN2017-84844-C2-2-R (MAGERAN) and project SA054G18 supported by Consejería de Educación (Junta de Castilla y León, Spain).

Acknowledgments: The authors want to thank the anonymous referees for their valuable suggestions and comments.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Von Neumann, J.; Burks, A.W. *Theory of Self-Reproducing Automata*; University of Illinois Press: Urbana, IL, USA; London, UK, 1966.
2. Gardner, M. Mathematical games—The fantastic combinations of John Conway's new solitaire game "life". *Sci. Am.* **1970**, *223*, 120–123. [CrossRef]
3. Wolfram, S. *Cellular Automata and Complexity: Collected Papers*; Addison-Wesley: Reading, MA, USA, 1994.
4. Ilachinski, A. *Cellular Automata: A Discrete Universe*; World Scientific: Singapore, 2001.
5. Wolfram, S. *A New Kind of Science*; Wolfram Media Inc.: Champaign, IL, USA, 2002.
6. Chopard, B.; Droz, M. *Cellular Automata Modeling of Physical Systems*; Cambridge University Press: Cambridge, UK, 2005.
7. Gutowitz, H. (Ed.) *Cellular Automata: Theory and Experiment*; MIT Press: Cambridge, MA, USA, 1991.
8. Sarkar, P. A brief history of cellular automata. *ACM Comput. Surv.* **2000**, *32*, 80–107. [CrossRef]
9. Bhattacharjee, K.; Naskar, N.; Roy, S.; Das, S. A survey of cellular automata: Types, dynamics, non-uniformity and applications. *Nat. Comput.* **2018**, 1–29. [CrossRef]
10. Toffoli, M.; Margolus, N. Invertible cellular automata: A review. *Phys. D* **1990**, *45*, 229–253. [CrossRef]
11. Morita, K. Reversible computing and cellular automata—A survey. *Theor. Comput. Sci.* **2008**, *395*, 101–131. [CrossRef]
12. Seck-Tuoh-Mora, J.C.; Medina-Marin, J.; Hernandez-Romero, N.; Martinez, G.J.; Barragan-Vite, I. Welch sets for random generation and representation of reversible one-dimensional cellular automata. *Inform. Sci.* **2017**, *382–383*, 81–95. [CrossRef]
13. Di Lena, P.; Margara, L. Nondeterministic Cellular Automata. *Inform. Sci.* **2014**, *287*, 13–25. [CrossRef]
14. Gajardo, A.; Kari, J.; Moreira, A. On time-symmetry in cellular automata. *J. Comput. Syst. Sci.* **2012**, *78*, 1115–1126. [CrossRef]
15. Kari, J. Reversible Cellular Automata: From Fundamental Classical Results to Recent Developments. *New Gener. Comput.* **2018**, *36*, 145–172. [CrossRef]
16. MacLean, S.; Montalva-Medel, M.; Goles, E. Block invariance and reversibility of one dimensional cellular automata. *Adv. Appl. Math.* **2019**, *105*, 83–101. [CrossRef]
17. Uguz, S.; Akin, H.; Siap, I.; Sahin, U. On the irreversibility of Moore cellular automata over the ternary field and image application. *Appl. Math. Model.* **2016**, *17–18*, 8017–8032. [CrossRef]
18. Temiz, F.; Sah, F.; Akin, H. Reversibility of a Family of 2D Cellular Automata Hybridized by Diamond and Cross Rules Over Finite Fields and an Application to Visual Cryptography. *J. Cell. Autom.* **2019**, *14*, 241–262.
19. Su, Y.R.; Wo, Y.; Han, G.Q. Reversible cellular automata image encryption for similarity search. *Signal Process. Image Commun.* **2019**, *72*, 134–147. [CrossRef]
20. Martín del Rey, A. A multi-secret sharing scheme for 3D solid objects. *Expert Syst. Appl.* **2015**, *42*, 2114–2120.
21. Chang, C.-H.; Chang, H. On the Bernoulli automorphism of reversible linear cellular automata. *Inform. Sci.* **2016**, *345*, 217–225. [CrossRef]
22. Cinkir, Z.; Akin, H.; Siap, I. Reversibility of 1D Cellular Automata with Periodic Boundary over Finite Fields $\mathbb{Z}_p$. *J. Stat. Phys.* **2011**, *143*, 807–823. [CrossRef]
23. Hernández Serrano, D.; Martín del Rey, A. A closed formula for the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule. *Appl. Math. Comput.* **2019**, *357*, 23–34.
24. Hernández Encinas, L.; Martín del Rey, A. Inverse rules of ECA with rule number 150. *Appl. Math. Comput.* **2007**, *189*, 1782–1786.
25. Siap, I.; Akin, H.; Koroglu, M.E. The reversibility of $(2r+1)$-cyclic rule cellular automata. *TWMS J. Pure Appl. Math.* **2013**, *4*, 215–225.
26. Martín del Rey, A.; Rodríguez Sánchez, G. On the reversibility of 150 Wolfram cellular automata. *Int. J. Mod. Phys. C* **2006**, *17*, 975–984.

27. Martín del Rey, A.; Rodríguez Sánchez, G. Reversibility of linear cellular automata. *Appl. Math. Comput.* **2011**, *217*, 8360–8366.
28. Martín del Rey, A.; Rodríguez Sánchez, G. Reversibility of a symmetric linear cellular automata. *Int. J. Mod. Phys. C* **2009**, *20*, 1081–1086.
29. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
30. Kaur, M.; Kumar, V. A Comprehensive Review on Image Encryption Techniques. *Arch. Comput. Methods Eng.* **2018**. [CrossRef]
31. Ghadirli, H.M.; Nodehi, A.; Enayatifar, R. An overwiew of encryption algorithms in color images. *Signal Process.* **2019**, *164*, 163–185. [CrossRef]