Reversibility of a Family of 2D Cellular Automata Hybridized by Diamond and Cross Rules Over Finite Fields and an Application to Visual Crypto....

Article *in* Journal of Cellular Automata · March 2019

CITATIONS
4

READS
223

3 authors:

Ferhat Sah
Adıyaman University
15 PUBLICATIONS **98** CITATIONS
SEE PROFILE

Fatih Temiz
Yıldız Technical University
7 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Hasan Akin
Harran University
153 PUBLICATIONS **1,494** CITATIONS
SEE PROFILE

Journal of Cellular Automata, Vol. 14, pp. 241–262
Reprints available directly from the publisher
Photocopying permitted by license only

Reversibility of a Family of 2D Cellular Automata Hybridized by Diamond and Cross Rules Over Finite Fields and an Application to Visual Cryptography

FATIH TEMIZ[1], FERHAT SAH[2,*] AND HASAN AKIN[3]

[1]*Faculty of Economics, Administrative and Social Sciences, Istanbul Gelisim University, Istanbul, Turkey*
E-mail: ftemiz@gelisim.edu.tr

[2]*Department of Mathematics, Adiyaman University, Adiyaman, Turkey*

[3]*Gokkusagi Mahallesi, 1164.Cadde, No:9/4, Cankaya-Ankara, Turkey*
E-mail: hasanakin69@gmail.com

Received: January 4, 2019. Accepted: March 8, 2019.

This article studies the behavior of two-dimensional finite cellular automata defined by two special family of rules under null boundary condition. The rule matrices of these families of two-dimensional hybrid cellular automata composed by diamond and cross rules respectively over the finite field $\mathbb{F}_p$ (p prime) are established. Further, explicit formulae that gives the rank of these rule matrices are provided. Hence, we are able to determine the reversibility of these cellular automata. Finally, we conclude by presenting an application of this family to pseudo random number generators applied to visual cryptography.

Keywords: Hybrid cellular automata, rule matrix, cryptography.

1 INTRODUCTION

Cellular automata (CA) have been first introduced by Ulam and von Neumann [19] in the 1940s. Later, in the beginning of the eighties, Stephen

* Contact author: E-mail: sefersah@gmail.com

Wolfram [29] has considered simple one-dimensional (1-D) CA rules for which he has shown that even they represent very complicated structures. Since then, studies and explorations in cellular automata have been of great interest the researchers. Some of the studies are presented by Chattopdhyay *et al.* [25] where the characterization of 2-dimensional hybrid cellular automata (2-D HCA) are studied. They obtained matrix algebraic formulae concerning some exceptional rules of two dimensional cellular automata. Khan *et al.* [2, 3] attempted to develop an analytical tool for studying all the nearest neighborhood 2-D linear CA. They gave the VLSI (very large scale integration) architecture of a CA and also worked on text compression using 2-D CA. CA have been widely investigated and received remarkable attention in the last few years in many fields [2–4, 17, 20, 23, 24, 28, 31, 32]. In [5] the use of HCA for cancer therapy is introduced. Siap *et al.* [14, 15] focused on the 2-D CA over ternary fields. Most of the work for CA is done for the finite fields.

Among cellular automata families, the CA that are reversible hence called reversible CA, have received remarkable attention since they have found applications in many disciplines (e.g., mathematics, physics, computer science, chemistry and so on) with different purposes (e.g., simulation of natural phenomena, pseudo-random number generation, image processing, analysis of universal model of computations, cryptography) [18]. Akin and Siap [13] studied the reversibility of 1-D CA over Galois rings and Siap *et al.* [16] studied the reversibility of 2-D hexagonal CA.

In this paper, we consider two families of CA by hybridization (2-D HCA) under null boundary condition and study the properties by using matrix algebra. First, we determine their rule matrices which are composed by so called *diamond* and *cross* rules respectively over finite fields (e.g., rules $2460N$ and $7380N$ over $\mathbb{F}_3$) [15]. We formulate the rank of these rule matrices and therefore we show whether the 2-D HCA are reversible or not. In conclusion, we present an application to visual cryptography for which we propose a method for generating random number generator that serves as a random key for symmetric cryptography. The properties of the key obtained is also analyzed.

2 TECHNICAL PRELIMINARIES

In this section, we introduce 2-D HCA families over the finite field $\mathbb{F}_p$ where p is a prime number, by using two special local rules. First, we recall the definition of a finite linear cellular automata. The 2-D LCA consists of $m \times n$ cells arranged in m rows and n columns, which may be considered as an $m \times n$ matrix where each cell (entry) takes one of the values of $0, 1, \ldots, p-1$ from the finite field. A set of cells in an array with a state

0	0	0	0	0
0	$x_{(i-1,j-1)}$	$x_{(i-1,j)}$	$x_{(i-1,,j+1)}$	0
0	$x_{(i,j-1)}$	$x_{(i,j)}$	$x_{(i,j+1)}$	0
0	$x_{(i+1,j-1)}$	$x_{(i+1,j)}$	$x_{(i+1,j+1)}$	0
0	0	0	0	0

TABLE 1
Null Boundary Condition

is called a configuration or information matrix. A configuration of CA is an assignment of states to all cells. Every configuration of a (linear) CA determines a next configuration via a (linear) transition rule that is local in the sense that the state of a cell at time $(t+1)$ depends only on the states of some of its neighbors at time t using algebra modulo p. For 2-D CA nearest neighbors, there are nine cells arranged in a 3×3 matrix centering that particular cell and there are some classical type of neighborhoods, but in this work we only restrict ourselves to some specific adjacent neighbors. So, we define the $(t+1)^{st}$ state of the $(i, j)^{th}$ cell in a LCA as follows:

$$\begin{aligned} x_{(i,j)}^{(t+1)} &= f\left(\begin{array}{c} x_{(i,j)}^{(t)}, x_{(i+1,j)}^{(t)}, x_{(i+1,j-1)}^{(t)}, x_{(i,j-1)}^{(t)}, x_{(i-1,j-1)}^{(t)}, \\ x_{(i-1,,j)}^{(t)}, x_{(i-1,j+1)}^{(t)}, x_{(i,j+1)}^{(t)}, x_{(i+1,j+1)}^{(t)} \end{array}\right) \\ &= a_0 x_{(i,j)}^{(t)} + a_1 x_{(i,j+1)}^{(t)} + a_2 x_{(i+1,,j+1)}^{(t)} + a_3 x_{(i+1,j)}^{(t)} + a_4 x_{(i+1,j-1)}^{(t)} \\ &\quad + a_5 x_{(i,j-1)}^{(t)} + a_6 x_{(i-1,j-1)}^{(t)} + a_7 x_{(i-1,j)}^{(t)} + a_8 x_{(i-1,j+1)}^{(t)} \pmod{p}, \end{aligned} \tag{1}$$

where $a_0, a_1, \ldots, a_8 \in \mathbb{F}_p$.

The value of each cell for the next state may not depend upon all nine neighbors. By making a restriction to a local relation then a delicate interpretation of the rules on the border of cells need to be addressed. One may notice the issue of what will be the neighborhood of the cells on the edge of the array. The cells at the extreme side ends have no neighbors. In order to accomplish this matter, there are some well-known approaches. Here, we introduce one of them which is called null boundary condition. The nonexistent neighbors of the extreme end cells are taken as zero. (see Table 1).

The conventional method of defining a rule number for a linear rule in 2-D CA can be explained via Table 2 as follows:

Here, p is a prime number which is the order of the finite field. The number within each cell shows the rule number for that cell and determining any rule number is formed by adding the values of cells which affect the evolution of the main cell. A rule number is determined as a linear combination of the rule numbers in Table 2. If the rule is given as (1) then the rule number

p^6	p^7	p^8
p^5	1	p
p^4	p^3	p^2

TABLE 2
Fundamental rule numbers for a 2-D linear CA

will be $a_0p^0 + a_1p^1 + \cdots + a_8p^8$. For simplicity, we rename the coefficients in (1) by $a_1 = b, a_2 = h, a_3 = c, a_4 = g, a_5 = d, a_6 = z, a_7 = a, a_8 = f$. If we consider $\mathbb{F}_3$ as our field with $a, b, c, d = 1$ and $f = g = h = z = 0$, then the rule number for this CA will be $3 + 3^3 + 3^5 + 3^7 = 2460$, for instance. If we take $f = g = h = z = 1$ and $a = b = c = d = 0$, then the rule number will be $3^2 + 3^4 + 3^6 + 3^8 = 7380$. We will name the family of rules with $a, b, c, d \neq 0$ while $f = g = h = z = 0$ as *diamond* and the family of rules with $a = b = c = d = 0$ while $f, g, h, z \neq 0$ as *cross*, respectively.

If the same rule is applied to all cells of a configuration, then CA is called uniform or regular. Otherwise, it is known as hybrid. Here in this paper, we introduce and characterize HCA combined with the rules diamond and cross over $\mathbb{F}_p$. By hybrid, here we mean application of the first (diamond) rule to odd number rows and second (cross) rule to even number rows. In order to visualize this, let us take $p = 3$ and consider the following configuration of order 5×5

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 2 \\ 2 & 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 1 & 2 & 1 & 0 & 1 \\ 2 & 1 & 2 & 0 & 2 \end{pmatrix}.$$

If we apply the rule 2460 to the first, third and fifth rows of the configuration and then we apply the rule 7380 to the second and fourth rows of the configuration, we obtain the next state configuration

$$\begin{pmatrix} 2 & 0 & 2 & 0 & 2 \\ 1 & 2 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \\ 2 & 0 & 2 & 1 & 1 \end{pmatrix}.$$

For example, the middle cell is evolved as the sum of the cells which are located its above, right, below, and left in modulo 3. Also, the cell in the

fourth row and the second column is evolved as the sum of crosswise cells (right upper, right bottom, left bottom, left upper).

The following lemma formulates both the rules diamond and cross algebraically [2]. We will denote the t^{th} state of a 2-D CA by X_t and we consider it as a matrix.

Lemma 1. *The* $(t+1)-$*state of a 2-D CA with rule diamond can be represented by the sum of* $t-$*state matrices as*

$$X_{t+1} = bX_tT_2 + cT_1X_t + dX_tT_1 + aT_2X_t \tag{2}$$

and similarly, one can represent the $(t+1)-$*state of a 2-D finite CA with rule cross by the sum of* $t-$*state matrices as*

$$X_{t+1} = hT_1X_tT_2 + gT_1X_tT_1 + zT_2X_tT_1 + fT_2X_tT_2 \tag{3}$$

where

$$T_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } T_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The characterization problem of 2-D configurations will be transformed to the characterization of one dimensional configurations by viewing $m \times n$ configurations as $mn \times 1$ configurations [2, 3]. In order to accomplish this goal we define the following transformation map $\Psi : M_{m\times n}(\mathbb{Z}_p) \to \mathbb{Z}_p^{mn}$. Here $M_{m\times n}(\mathbb{Z}_p)$ denotes the space of $m \times n$ matrices over the field $\mathbb{Z}_p$. Ψ takes the t^{th} state X_t and makes it a column vector as follows:

$$\begin{pmatrix} x_{11}^{(t)} & x_{12}^{(t)} & \cdots & x_{1n}^{(t)} \\ x_{21}^{(t)} & x_{22}^{(t)} & \cdots & x_{2n}^{(t)} \\ \vdots & \vdots & \cdots & \vdots \\ x_{m1}^{(t)} & x_{m2}^{(t)} & \cdots & x_{mn}^{(t)} \end{pmatrix} \longrightarrow (x_{11}^{(t)}, x_{12}^{(t)}, \ldots, x_{1n}^{(t)}, \ldots, x_{m1}^{(t)}, \ldots, x_{mn}^{(t)})^T. \tag{4}$$

The matrix stated above is sometimes denoted by $C^{(t)}$ and called the configuration of the 2-D finite CA at time t or the $p-$ary information matrix.

From (4), we can define $(T_{Rule})_{mn\times mn} \cdot (X_t)_{mn\times 1} = (X_{t+1})_{mn\times 1}$. Note that, according to different rules, (T_{Rule}) has different representations and this

matrix is called representation matrix, transition matrix or rule matrix. In order to study construction of matrix representations, due to HCA we need to split the problem into two main sections: m even and m odd.

3 CONSTRUCTION OF MATRIX REPRESENTATIONS OF 2-D FINITE HCA OVER FINITE FIELDS

3.1 THE EVEN CASE

In this section, we construct the rule matrix (matrix representation) of a 2-D finite HCA with null boundary composed by the diamond and cross rules respectively over $\mathbb{F}_p$. We want to construct the rule matrices T_0 and T_1 corresponding to the hybridization of diamond and cross rules respectively by operating on the current $p-$ary information matrix (configuration) X_t of order $m \times n$ at time t and thus obtain the next information matrix X_{t+1} (see [27] for the representation of linear transformations).

Theorem 1. *Let $a, b, c, d, z,\ f, g, h \in \mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$. If m is an even positive integer, then for any positive integer n, the representation matrix T_{HN} representing a 2-D finite HCA composed by the rules diamond and cross respectively, is given by the following matrix:*

$$(T_{HN})_{mn\times mn} = \begin{pmatrix} S(d,b) & cI & 0 & 0 & \dots & 0 & 0 \\ S(z,\ f) & 0 & S(g,h) & 0 & \dots & 0 & 0 \\ 0 & aI & S(d,b) & cI & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & aI & S(d,b) & cI \\ 0 & 0 & 0 & 0 & \dots & S(z,\ f) & 0 \end{pmatrix}$$

where each submatrix is of order $n \times n$ and for any $k, l \in \mathbb{Z}_p^*$

$$S(k,l) = \begin{pmatrix} 0 & l & 0 & \dots & 0 & 0 \\ k & 0 & l & \dots & 0 & 0 \\ 0 & k & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & k & 0 & l \\ 0 & 0 & 0 & \dots & k & 0 \end{pmatrix}.$$

Proof. Let $T_M(x_{ij}) = y_{ij}$ where M represents the diamond or cross rules. In order to determine the rule matrix T_M, we need to determine the action of T_M on the bases vectors. First, we consider the linear transformation T_M from $m \times n$ matrix space onto itself. Let e_{ij} denotes the $m \times n$ matrix where the

$(i, j)^{th}$ position is one and all other entries are zero. It is well known that these matrices form the standard basis for $M_{m\times n}(\mathbb{F}_p)$.

Assume that T_0 represents the diamond rule. For a given e_{ij}, if i is odd, then the transformation of e_{ij} under T_0 i.e. $T_0\left(e_{ij}\right)$ is related to the neighbor determined by the diamond rule and equals to a linear combination of its neighbors in the following way:

$$T_0\left(e_{ij}\right) = ae_{i-1,j} + be_{i,j+1} + ce_{i+1,j} + de_{i,j-1}$$

where $e_{ij} = 0$ where $i < 0$ or $j < 0$ or $i > m$ or $j > n$ (these restrictions apply since in these particular cases the borders of the configuration matrix are exceeded.)

On the other hand, assume that T_1 represents the cross rule. If i is even, then the transformation of e_{ij} under T_1 i.e. $T_1\left(e_{ij}\right)$ is a linear combination of its vertex neighbors in the following way:

$$T_1\left(e_{ij}\right) = fe_{i-1,j+1} + he_{i+1,j+1} + ge_{i+1,j-1} + ze_{i-1,j-1}$$

where $e_{ij} = 0$ where $i < 0$ or $j < 0$ or $i > m$ or $j > n$.

Now, let E_i be the column vector in $\mathbb{F}_p^{mn}$ where all entries equal to zero except the entry positioned at i which equals to one. These vectors also give the standard basis of the $\mathbb{F}_p-$space $\mathbb{F}_p^{mn}$. The transition from the matrix space basis to the standard basis of $\mathbb{Z}_p^{mn}$ is given by $\Psi\left(e_{ij}\right) = E_{(i-1)n+j}$, where $1 \le i \le m$ and $1 \le j \le n$. Let T_{HN} represent the rule matrix of the hybrid cellular automata composed by the diamond and cross rules respectively. Then, T_{HN} will act on the rows of configurations accordingly. The first row of the configuration will be transformed by under the influence of the diamond rule such as follows:

$$T_{HN}(E_1) = dE_2 + zE_{n+2} \tag{5}$$

and this gives the first column of the rule matrix. The second row of the configuration will be transformed according to the cross rule i.e T_{HN} and

$T_{HN}(E_2) = bE_1 + dE_3 + fE_{n+1} + zE_{n+3}$.

By applying induction with care on the borders of the configuration matrix, one determines the rest of the columns. □

Let us now work on a concrete example that will help to illustrate the proof of theorem above.

Example 1. If we take $m = 4, n = 3,$ then we get the rule matrix T_{HN} of order 12. We consider a configuration of size 4×3 with null boundary condition

0	0	0	0	0
0	x_{11}	x_{12}	x_{13}	0
0	x_{21}	x_{22}	x_{23}	0
0	x_{31}	x_{32}	x_{33}	0
0	x_{41}	x_{42}	x_{43}	0
0	0	0	0	0

This configuration is represented by an information matrix as the following

$$X_{4\times 3} = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \\ x_{41} & x_{42} & x_{43} \end{pmatrix}.$$

Now, we apply rule diamond to all cells of the first row of $X_{4\times 3}$ and next apply the rule cross to all cells of the second row of $X_{4\times 3}$. If we apply the rules alternately in this manner, then we obtain a new $p-$ary information matrix $Y_{4\times 3}$ with entries as follows:

$$\begin{aligned}
y_{11} &= cx_{21} + bx_{12} \mod p \text{ (diamond rule applied)} \\
y_{12} &= dx_{11} + cx_{22} + bx_{13} \mod p \text{ (diamond rule applied)} \\
y_{13} &= dx_{12} + cx_{23} \mod p \text{ (diamond rule applied)} \\
\\
y_{21} &= fx_{12} + hx_{32} \mod p \text{ (cross rule applied)} \\
y_{22} &= zx_{11} + gx_{31} + fx_{13} + hx_{33} \mod p \text{ (cross rule applied)} \\
y_{23} &= zx_{12} + gx_{32} \mod p \text{ (cross rule applied)} \\
\\
y_{31} &= ax_{21} + bx_{32} + cx_{41} \mod p \text{ (diamond rule applied)} \\
&\vdots \quad \vdots \\
y_{43} &= zx_{32} \mod p \mod p \text{ (cross rule applied).}
\end{aligned}$$

Note that, in order to obtain the rule matrix T_{HN} the diamond rule is applied to all cells in even rows and cross rule is applied to all cells in odd rows. Now,

in order to find the final form of the representation matrix, we evaluate the image of basis vectors E_i for $1 \leq i \leq 12$ under the transformation T_{HN} and take their transpose as the columns of T_{HN}.

$$\begin{aligned}
T_{HN}(E_1) &= \begin{pmatrix} 0 & d & 0 & 0 & z & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T \\
T_{HN}(E_2) &= \begin{pmatrix} b & 0 & d & f & 0 & z & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^T \\
&\vdots \\
T_{HN}(E_{12}) &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & c & 0 & 0 & 0 \end{pmatrix}^T.
\end{aligned}$$

Hence, we obtain the rule matrix T_{HN} of order 12 by combining the results above:

$$T_{HN} = \left(\begin{array}{ccc|ccc|ccc|ccc}
0 & b & 0 & c & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
d & 0 & b & 0 & c & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & d & 0 & 0 & 0 & c & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & f & 0 & 0 & 0 & 0 & 0 & h & 0 & 0 & 0 & 0 \\
z & 0 & f & 0 & 0 & 0 & g & 0 & h & 0 & 0 & 0 \\
0 & z & 0 & 0 & 0 & 0 & 0 & g & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & a & 0 & 0 & 0 & b & 0 & c & 0 & 0 \\
0 & 0 & 0 & 0 & a & 0 & d & 0 & b & 0 & c & 0 \\
0 & 0 & 0 & 0 & 0 & a & 0 & d & 0 & 0 & 0 & c \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & f & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & z & 0 & f & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & z & 0 & 0 & 0 & 0
\end{array}\right)_{12\times 12}$$

By renaming the submatrices in T_{HN}, we can express this matrix as

$$T_{HN} = \begin{pmatrix} S_3(d,b) & cI_3 & O_3 & O_3 \\ S_3(z,\ f) & O_3 & S_3(g,h) & O_3 \\ O_3 & aI_3 & S_3(d,b) & cI_3 \\ O_3 & O_3 & S_3(z,\ f) & O_3 \end{pmatrix}_{12\times 12}. \tag{6}$$

Next, we focus on determining the reversibility of HCA for which we need to consider the submatrices and their ranks.

Lemma 2. *If n is an even positive integer then the submatrix $S(z,\ f)$ given above is invertible and its determinant is $(-1)^{\frac{n}{2}} f^{\frac{n}{2}} z^{\frac{n}{2}}$*

Proof. Consider the submatrix $S(z,\ f)$:

$$S(z,\ f) = \begin{pmatrix} 0 & f & 0 & 0 & \dots & 0 & 0 \\ z & 0 & f & 0 & \dots & 0 & 0 \\ 0 & z & 0 & f & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & z & 0 & f \\ 0 & 0 & 0 & 0 & \dots & z & 0 \end{pmatrix}.$$

Apply the row operation $(p-1)zf^{-1}R_1 + R_3 \to R_3$ which gives the equivalent matrix

$$S'(z,\ f) = \left(\begin{array}{cc|ccccc} 0 & f & 0 & 0 & \dots & 0 & 0 \\ z & 0 & f & 0 & \dots & 0 & 0 \\ \hline 0 & 0 & 0 & f & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & z & 0 & f \\ 0 & 0 & 0 & 0 & \dots & z & 0 \end{array}\right).$$

Then,

$$\det S_{2t\times 2t}(z,\ f) = \det S'_{2t\times 2t}(z,\ f) = \det S_{2\times 2}(z,\ f)\det S_{2t-2\times 2t-2}(z,\ f)$$

and similarly,

$$\det S_{2t-2\times 2t-2}(z,\ f) = \det S'_{2t-2\times 2t-2}(z,\ f) = \det S_{2\times 2}(z,\ f)\det S_{2t-4\times 2t-4}(z,\ f).$$

Hence, by induction, it is easy to see that

$$\det S_{2t\times 2t}(z,\ f) = (\det S_{2\times 2}(z,\ f))^t = (-1)^t f^t z^t. \tag{7}$$

□

We see that the submatrix $S(z,\ f)$ is invertible and hence it has full rank. We will use this fact for the sake of determining the rank of the hybrid rule matrix. It is not hard to see that, by applying elementary row and column operations to our rule matrix T_{HN} given in Theorem 1, we obtain the follow-

ing matrix and from now on, we will call it T_{HN}

$$(T_{HN})_{mn\times mn} = \begin{pmatrix} cI & 0 & 0 & \dots & 0 & S(d,b) & 0 & 0 & \dots & 0 \\ aI & cI & 0 & \dots & 0 & 0 & S(d,b) & 0 & \dots & 0 \\ 0 & aI & cI & \dots & 0 & 0 & 0 & S(d,b) & \dots & 0 \\ 0 & 0 & aI & \dots & 0 & 0 & 0 & 0 & S(d,b) & 0 \\ 0 & 0 & 0 & \dots & cI & 0 & 0 & 0 & \dots & S(d,b) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & S(z,f) & S(g,h) & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & S(z,f) & S(g,h) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & S(g,h) \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & S(z,f) \end{pmatrix} \tag{8}$$

In order to determine the dimension of the kernel of a 2-D finite HCA, we need to study the rank of T_{HN}. It is well known that the dimension of the kernel of a transformation gives a clue to draw the state transition diagram [25]. Further, if the kernel of the transformation is zero, then it is reversible since the transformations in this study are over finite dimensional spaces. Kari [18] has proved that the reversibility of a cellular automaton with dimension larger or equal to two is not decidable. In other words, due to its complexity, Kari has shown that the inverse of a given cellular automaton with higher dimension cannot be found by an algorithm in general. Further, Durand in [4] shows that the problem of finding the inverse of a 2-D cellular automaton is a very difficult problem. Here, by determining the dimension of the kernel of the rule, we also answer the question of reversibility of these 2-D cellular automata.

Theorem 2. *Let T_{HN} be the hybrid rule matrix of order $m \times n$ as given in Theorem 1. If m and n are even positive integers such that $m = 2k$ and $n = 2t$, then $rank(T_{HN}) = mn$.*

Proof. Consider the rule matrix T_{HN} given in (8). We want to achieve to show that T_{HN} is invertible. Obviously,

$$\det(T_{HN}) = \det \begin{pmatrix} cI & 0 & 0 & \dots & 0 \\ aI & cI & 0 & \dots & 0 \\ 0 & aI & cI & \dots & 0 \\ 0 & 0 & aI & \dots & 0 \\ 0 & 0 & 0 & \dots & cI \end{pmatrix}$$

$$\det \begin{pmatrix} S(z,f) & S(g,h) & 0 & \dots & 0 \\ 0 & S(z,f) & S(g,h) & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & S(g,h) \\ 0 & 0 & \dots & 0 & S(z,f) \end{pmatrix}.$$

Again by induction, similar to proof of Lemma 2, we have $\det(T_{HN}) = c^{m/2}(\det S(z, f))^{m/2}$ and hence

$$\det(T_{HN}) = (-1)^{\frac{n}{2}} c^{\frac{m}{2}} f^{\frac{mn}{4}} z^{\frac{mn}{4}} = (-1)^t c^k f^{kt} z^{kt}$$

which shows that the matrix is invertible in $\mathbb{F}_p$. Therefore, we deduce that

$$\text{rank}(T_{HN}) = mn.$$

□

Remark 1. *Note that, if m and n are both even positive integers, then the rule matrix corresponding to cellular automaton has full rank that is, cellular automaton is reversible.*

Theorem 3. *Let T_{HN} be the hybrid rule matrix as given in (8). If m is an even positive integer and if n is an odd positive integer such that $m = 2k$ and $n = 2t + 1\,(t \geq 1)$, then*

$$rank(T_{HN}) = m(n-1) + \frac{m}{2}. \tag{9}$$

Proof. Consider the rule matrix T_{HN} given in (8). As in the previous theorem, we can determine the rank of T_{HN} by only considering the matrices cI and $S(z, f)$ which is slightly different from the case n is even. Consider the submatrix

$$S(z, f) = \begin{pmatrix} 0 & f & 0 & \dots & 0 & 0 \\ z & 0 & f & \dots & 0 & 0 \\ 0 & z & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & z & 0 & f \\ 0 & 0 & 0 & \dots & z & 0 \end{pmatrix}_{2t+1 \times 2t+1}.$$

Clearly $rank(cI) = n = 2t + 1$. To compute the rank of $S(z, f)$, we apply some elementary row operations. First, replace each row with above cyclically and then,

$$\begin{aligned} z^{-1}(p-1) f R_2 + R_n &\to R_n \\ z^{-2}(p-1)^2 f^2 R_4 + R_n &\to R_n \\ &\vdots \\ z^{-j}(p-1)^j f^j R_{2j} + R_n &\to R_n \end{aligned}$$

for each $1 \leq j \leq (n-1)/2$. Consequently $S(z,\ f)$ is equivalent to

$$\begin{pmatrix} z & 0 & f & \dots & 0 & 0 \\ 0 & z & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & z & 0 & f \\ 0 & 0 & 0 & \dots & z & 0 \end{pmatrix}_{2t \times 2t+1}.$$

By considering the matrix above, we see that $S(z,\ f)$ has rank $n-1 = 2t$. Therefore, we conclude that the rule matrix T_{HN} has rank $(2t+1)k + (2t)k = n(m/2) + (n-1)(m/2) = m(n-1) + (m/2)$. □

3.2 THE ODD CASE

Theorem 4. *Let $a, b, c, d, z,\ f, g, h \in \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. For any positive integer n, if m is an odd positive integer, then the matrix T_{HN} of order $mn \times mn$ representing 2-D finite HCA composed by the* diamond *and* cross *rules respectively, is given by*

$$(T_{HN})_{mn\times mn} = \begin{pmatrix} S(d,b) & cI & 0 & 0 & \dots & 0 & 0 \\ S(z,\ f) & 0 & S(g,h) & 0 & \dots & 0 & 0 \\ 0 & aI & S(d,b) & cI & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & S(z,\ f) & 0 & S(g,h) \\ 0 & 0 & 0 & 0 & \dots & aI & S(d,b) \end{pmatrix}.$$

Proof. Assume that m is odd. Analogous to the even case, we apply the diamond and cross rules to the rows of the information matrix alternately and respectively. Different from the even case, since m is odd, here we apply the diamond rule to all cells of the last row of the information matrix $X_{m\times n}$. Therefore, we have

$$\begin{aligned} T_0(e_{m1}) &= ge_{m-1,2} + de_{m,2}, \\ T_0(e_{ml}) &= he_{m-1,l-1} + ge_{m-1,l+1} + de_{m,l+1} + be_{m,l-1} \\ T_0(e_{mn}) &= he_{m-1,n-1} + be_{m,n-1}. \end{aligned}$$

where $2 \leq l \leq n-1$. Let E_i denote the standard basis vectors of the $\mathbb{F}_p-$space $\mathbb{F}_p^{mn}$. The transition from the matrix space basis to the standard basis of $\mathbb{F}_p^{mn}$ is given by

$$\Psi(e_{ij}) = E_{(i-1)n+j}$$

where $1 \leq i \leq m$ and $1 \leq j \leq n$. Similar to the proof of Theorem 1, $T_{HN}(E_i)$ gives the i^{th} column of the rule matrix T_{HN}. In this way, we can obtain all the columns straightforwardly but tediously. □

Example 1. *Let us take $m = 3$ and $n = 3$, then we get the rule matrix T_{HN} of size 9×9. We consider a configuration of size 3×3 with hybrid null boundary condition*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & x_{11} & x_{12} & x_{13} & 0 \\ 0 & x_{21} & x_{22} & x_{23} & 0 \\ 0 & x_{31} & x_{32} & x_{33} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Now, we apply diamond rule to all cells of the first row, and continuing alternately and applying the cross rule to the second row and continuing alternately of $p-$ary information matrix $X_{3\times3}$ we obtain the following rule matrix:

$$T_{HN} = \begin{pmatrix} 0 & b & 0 & c & 0 & 0 & 0 & 0 & 0 \\ d & 0 & b & 0 & c & 0 & 0 & 0 & 0 \\ 0 & d & 0 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & f & 0 & 0 & 0 & 0 & 0 & h & 0 \\ z & 0 & f & 0 & 0 & 0 & g & 0 & h \\ 0 & z & 0 & 0 & 0 & 0 & 0 & g & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & a & 0 & d & 0 & b \\ 0 & 0 & 0 & 0 & 0 & a & 0 & d & 0 \end{pmatrix} = \begin{pmatrix} S_3(d,b) & cI_3 & O_3 \\ S_3(z,\ f) & O_3 & S_3(g,h) \\ O_3 & aI_3 & S_3(d,b) \end{pmatrix}$$

By applying elementary row and column operations to the above matrix, we have

$$T_{HN} = \begin{pmatrix} cI_3 & S_3(d,b) & O_3 \\ aI_3 & O_3 & S_3(d,b) \\ O_3 & S_3(z,\ f) & S_3(g,h) \end{pmatrix},$$

where each submatrix is of order 3×3 and

$$S_{3\times3}(k,l) = \begin{pmatrix} 0 & l & 0 \\ k & 0 & l \\ 0 & k & 0 \end{pmatrix}.$$

We also find the rank of the rule matrix T_{HN} by determining the dimension of the kernel of this 2-D finite HCA. We note that, by applying elementary

row and column operations to the matrix given in Theorem 4, the rule matrix becomes

$$(T_{HN})_{mn\times mn} = \begin{pmatrix} cI & 0 & 0 & \dots & 0 & 0 & S(d,b) & 0 & 0 & \dots & 0 \\ aI & cI & 0 & \dots & 0 & 0 & 0 & S(d,b) & 0 & \dots & 0 \\ 0 & aI & cI & \dots & 0 & 0 & 0 & 0 & S(d,b) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & aI & cI & 0 & 0 & \dots & S(d,b) & 0 \\ 0 & 0 & 0 & \dots & 0 & aI & 0 & 0 & 0 & \dots & S(d,b) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & S(z,f) & S(g,h) & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & S(z,f) & S(g,h) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & 0 & 0 & \vdots & \vdots & \vdots & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & S(z,f) & S(g,h) \end{pmatrix}. \quad (10)$$

Theorem 5. *If m and n are odd positive integers such that $m = 2k+1$ with $k \geq 1$ and $n = 2t+1$ with $t \geq 1$ and if the rule matrix T_{HN} of order $mn \times mn$ is given as in* (10)*, then*

$$rank\,(T_{HN}) = mn - n - \frac{m-1}{2}.$$

Proof. Assume that $m = 2k+1$ and $n = 2t+1$ are odd positive integers. If we denote T by

$$T = \begin{pmatrix} U & F \\ O & L \end{pmatrix},$$

then the we have $rank(T) = rank(U) + rank(L)$. It can be easily seen that the rank of

$$U = \begin{pmatrix} cI & 0 & 0 & 0 & \dots & 0 & 0 \\ aI & cI & 0 & 0 & \dots & 0 & 0 \\ 0 & aI & cI & 0 & \dots & 0 & 0 \\ 0 & 0 & aI & cI & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \dots & aI & cI \\ 0 & 0 & 0 & \dots & \dots & 0 & aI \end{pmatrix} \sim \begin{pmatrix} cI & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & cI & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & cI & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & cI & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \dots & 0 & cI \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 \end{pmatrix}$$

is $(m-1)/2$. We can also show that

$$\begin{aligned} rank(L) &= rank\,(S(z,\ f)) + rank\,(S(z,\ f)) + \cdots + rank\,(S(z,\ f)) \\ &= (n-1)\left(\frac{m+1}{2} - 1\right). \end{aligned}$$

Hence the result. □

Theorem 6. *If $m = 2k+1$ is an odd positive integer and $n = 2t$ is an even positive integer with $k, t \geq 1$ and if the hybrid rule matrix T_{HN} of order $mn \times mn$ is given by (10), then*

$$rank\,(T_{HN}) = n(m-1).$$

Proof. The proof is very similar to the previous case. The only difference in this case is that, $S(z,\ f)$ has full rank since n is even. Therefore, we have

$$rank(T) = n\left(\frac{m-1}{2}\right) + n\left(\frac{m+1}{2} - 1\right).$$

□

Remark 2. *According to theorem 6, if $m = 2k+1$ is an odd positive integer and $n = 2t$ is an even positive integer with $k, t \geq 1$, then 2-D finite HCA is irreversible.*

Example 2. *Take $m = 3$ and $n = 4$ then our rule matrix T_{HN} will be in the form:*

$$T_{HN} = \left(\begin{array}{cccc|cccc|cccc} c & 0 & 0 & 0 & 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & c & 0 & 0 & d & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & d & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & d & 0 & 0 & 0 & 0 & 0 \\ \hline a & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 & b & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 & b \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & f & 0 & 0 & 0 & h & 0 & 0 \\ 0 & 0 & 0 & 0 & z & 0 & f & 0 & g & 0 & h & 0 \\ 0 & 0 & 0 & 0 & 0 & z & 0 & f & 0 & g & 0 & h \\ 0 & 0 & 0 & 0 & 0 & 0 & z & 0 & 0 & 0 & g & 0 \end{array}\right)$$

$$= \begin{pmatrix} cI & S(d,b) & O \\ aI & O & S(d,b) \\ O & S(z,\ f) & S(g,h) \end{pmatrix}.$$

Submatrices of T_{HN} can be denoted alternatively by;

$$U = \begin{pmatrix} cI \\ aI \end{pmatrix}_{8\times 4},\ F = \begin{pmatrix} S(d,b) & O \\ O & S(d,b) \end{pmatrix}_{8\times 8},\ O = \begin{pmatrix} O \end{pmatrix}_{4\times 4} \text{ and}$$
$$L = \begin{pmatrix} S(z,\ f) & S(g,h) \end{pmatrix}_{4\times 8}$$

In order to compute rank of T_{HN} we compute $rank(U) + rank(L)$. Obviously, $rank(U) = 4$. Next, we compute $rank(L)$: By applying elementary row operations respectively as follows:

$$(p-1)zf^{-1}R_1 + R_3 \to R_3,\ R_1 \leftrightarrow R_2,\ R_3 \leftrightarrow R_4$$

we obtain the equivalent matrix:

$$\left(\begin{array}{cccc|cccc} z & 0 & f & 0 & g & 0 & h & 0 \\ 0 & f & 0 & 0 & 0 & h & 0 & 0 \\ 0 & 0 & z & 0 & 0 & 0 & g & 0 \\ 0 & 0 & 0 & f & 0 & g - zhf^{-1} & 0 & h \end{array}\right)_{4\times 8}$$

and clearly it has rank 4*. Hence we have $rank(T) = rank(U) + rank(L) = 4 + 4 = 8$ as given our formula that $(m-1)n = 2 \cdot 4 = 8$.*

4 AN APPLICATION TO PSEUDO-RANDOM NUMBER GENERATORS

Random numbers have an extensive application in various contexts including statistical mechanics, gaming industry, cryptography and communication etc. Two basic types of random number generators exist: true random number generators (TRNGs) and pseudo-random number generators (PRNGs) [33]. In this section, we present an application of 2-D HCA with null boundary composed by the diamond and cross rules respectively over the fields $\mathbb{F}_3$ and $\mathbb{F}_{251}$. Random number sequences have found many applications in engineering, cryptography, Monte Carlo simulations and many industrial applications [26, 29, 30]. Finding a good source for generating pseudo random numbers is still a very difficult problem [22]. There are several methods for generating pseudo random number sequences, but because of the parallel structure and effective hardware implementation of cellular automata, cellular automata are very attractive for generating pseudo random number sequences [10]. In order to obtain a suitable pseudo number via cellular automata an initial configuration is feeded into CA. CA on the other hand are vulnerable due to the

linearity. However, in this particular application we choose some entries of CA that is going to provide randomness as shown in the sequel. Due to this approach, we are able to expect a pseudo number. In order to test the randomness of such sequences, some well known tests are applied. We also find the expected values and degree of freedoms in order to process these statistical tests for $p-$ary sequences. A pseudo-random number generator (PRNG) is a program written for, and used in, probability and statistics applications when large quantities of random digits are needed. Although PRNG via CA is vulnerable to some cryptanalyst attacks if the number of cells is less than 500 [9], we provide an example of order 36×36 due to place limit which still encourages the study of hybrid CA.

Let $C^0 = [011220100111101201022001211020022 2101]$ be the initial configuration and $a = b = c = d = f = g = h = z = 1 \in \mathbb{F}_3$. Then the 36×36 representation matrix of 2-D finite HCA with null boundary condition is

$$T_{HN} = \begin{pmatrix} S_6(d,b) & cI_6 & O_6 & O_6 & O_6 & O_6 \\ S_6(z,\ f) & O_6 & S_6(g,h) & O_6 & O_6 & O_6 \\ O_6 & aI_6 & S_6(d,b) & cI_6 & O_6 & O_6 \\ O_6 & O_6 & S_6(z,\ f) & O_6 & S_6(g,h) & O_6 \\ O_6 & O_6 & O_6 & aI_6 & S_6(d,b) & cI_6 \\ O_6 & O_6 & O_6 & O_6 & S_6(z,\ f) & O_6 \end{pmatrix}.$$

Our generating PRN process is not concatenating some set of configurations for the sake of security. Instead, after 1024 iterations, we get a sequence of numbers from the field $\mathbb{F}_3$ of length 1024 by picking one special cell, say the 13^{th} from each configuration [6]. This choice is the reason to obtaining the randomness compared to the case where a block of vectors are used in CA cryptography.

In order to save space the first 1024 components of sequences are given in blocks of $64-$point converted to hexadecimal form:

17E9333111F9DAB1B204D59917 - 2166C47CA512FC771365143F4D - 294A397C4C600FD20963990A84 - 29C5FA33A5FBD167DA695BC4D2 - 4032AC85E32557DFD0DD56C7 - 2180E699B139AC248E751785DF - 3F7EC777A2A4490669C46F0D7 - 10E92F5C2014D737EA59B9ACED - 23284EC4762DDF0C945B9EB514 - 17E9333111F9DAB1B204D59917 - 2166C47CA512FC771365143F4D - 294A397C4C600FD20963990A84 - 29C5FA33A5FBD167DA695BC4D2 - 4032AC85E32557DFD0DD56C7 - 2180E699B139AC248E751785DF - 3F7EC777A2A4490669C46F0D7

The 1024 length ternary sequence passes serial, run, frequency, and poker tests. For every test the χ^2-value for $0,05$ confidence level is smaller than the value in the χ^2- table.

Statistical test	Degree of freedom	χ^2-value
Frequency	2	0, 55
Serial	6	3, 2
Poker	26	14, 3
Runs	7	8, 4

TABLE 3
Table 1 χ^2-value and d_f for frequency, serial, poker and runs tests.

Further we carry these results to image encryption. It is a well known fact that one-time-pad is the most efficient symmetric encryption technique. A key of the same length as plaintext is generated and each bit or character is **XOR** ed (combined) with the corresponding bit or character. Each pixel is determined by a value in color depth. If we take a $8-$bit gray color image, then each pixel is scaled between 0 and 255. However, most of the pictures does not contain a pixel whose value is larger than 251. This motivates us to generate a considerable sequence of numbers from the finite field $\mathbb{F}_{251}$ (instead of binary field for the sake of showing the effectiveness of this study) of same size with a picture and use it as a secret symmetric key. The encryption algorithm then is simply XORing i.e. adding the matrix of picture and the key matrix modulo two. Figure 1 shows the plain image and Figure 2 shows the cipher image.

Encryption with a good key implies that the histogram of the cipher image is nearly uniform. Otherwise the key will be vulnerable to statistical attacks [7]. We also give the histogram of the plain image and the cipher image respectively in Figure 3 and in Figure 4 to indicate that our key withstands the statistical attacks.

FIGURE 1
Plain Image.

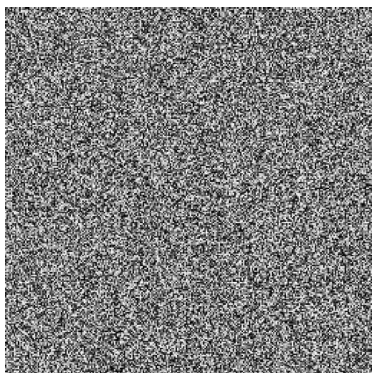

FIGURE 2
Cipher Image.

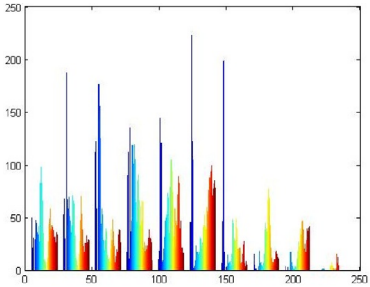

FIGURE 3
(Color online) Histogram of Plain Image.

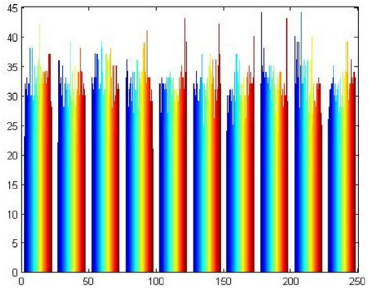

FIGURE 4
(Color online) Histogram of Cipher Image.

5 CONCLUSION

In this work, we have studied a special family of two dimensional hybrid cellular automata. We have constructed their rule matrices and next we formulate their ranks which leads to the determination of their reversibility. Further, we have obtained a pseudo number generating by a member of this family with a particular and nonstandard choice of the values of CA. We have shown that this pseudo number passes some well-known statistical test and we have applied this pseudo number to visual cryptography where again we have a successful result [8].

ACKNOWLEDGMENT

This research was supported by the project 110T713 TUBITAK (Scientific and Technological Research Council of Turkey) TBAG.

REFERENCES

[1] Adamatzky A. (1999). *Nonconstructible blocks in 1D cellular automata: minimal generators and natural systems*, Applied Mathematics and Computation, **99**, 77–91.

[2] Khan A. R., Choudhury P. P., Dihidar K., Mitra S., Sarkar P. (1997). *VLSI architecture of a cellular automata*, Comput. Math. Applic., **33**, 79–94.

[3] Khan A. R., Choudhury P. P., Dihidar K., Verma R. (1999). *Text compression using two dimensional cellular automata*, Comput. Math. Applic., **37**, 115–127.

[4] Durand B. (1994). *Inversion of 2D cellular automata: some complexity results*, Theoret. Comput. Sci., **134**, 387–401.

[5] Ribba B., Alarcon T., Marron K., Maini P.K., and Agur Z. (2004). *The Use of Hybrid Cellular Automaton Models for Improving Cancer Therapy*, ACRI 2004, LNCS 3305, 444–453.

[6] Rubio C. F. *et al.* (2004). *The Use of Linear Hybrid Cellular Automata as Pseudo Random Bit Generators in Cryptography*, Neural Parallel and Scientific Computatiions, **12**(2), 175–192.

[7] Jin D. and Lin S. eds. (2012).*Advances in Computer Science and Information Engineering*, Vol. 2. Springer Science & Business Media.

[8] Jin, Jun, and Wu Z.-h. (2012). *A secret image sharing based on neighborhood configurations of 2-D cellular automata*, Optics & Laser Technology, 44.3:538–548.

[9] Raul D. L. *et al.* (2003). *Wolfram cellular auto mata and their cryptographic use as pseudorandom bit generators.*

[10] Temiz F., Siap I., and Akin H. (2014). *On Pseudo Random Bit Generators via Two-Dimensional Hybrid Cellular Automata*, Acta Physica Polonica A, **125**(2):534–537.

[11] Alvarez G., Encinas L. H., del Rey A. M. (2008). *A multisecret sharing scheme for color images based on cellular automata*, Information Sciences, **178**, 4382–4395.

[12] Akın H. (2005). *On the directional entropy of $\mathbb{Z}^2$ -actions generated by additive cellular automata*, Appl. Math. Computation, **170**(1):339–346.

[13] Akın H., Siap I. (2007). *On cellular automata over Galois rings*, Information Processing Letters, **103**(1):24–27.

[14] Siap I., Akın H. and Sah F. (2011). *Characterization of two dimensional cellular automata over ternary fields*, Journal of the Franklin Institute, **348**, 1258–1275.

[15] Siap I., Akın H. and Sah F. (2010). *Garden of eden configurations for 2-D cellular automaton with rule 2460N*, Information Sciences, **180**(18):3562–3571.

[16] Siap I., Akın H., and Uguz S. (2011). *Structure and reversibility of 2-dimensional hexagonal cellular automata*, Computers Mathematics with Applications, **62**(11):4161–4169.

[17] Siap I., Akin H. and Koroglu M. E. (2012). *Reversible cellular automata with penta-cyclic rule and ECCs*, International Journal of Modern Physics C, 23(10).

[18] Kari J. (1990). *Reversibility of 2D cellular automata is undecidable*, Physica D, **45**, 386–395.

[19] Neumann J. V. (1966). The theory of self-reproducing automata, (Edited by A.W.Burks), Univ. of Illinois Press, Urbana.

[20] Dihidar K., Choudhury P. P. (2004). Matrix algebraic formulae concerning some exceptional rules of two dimensional cellular automata, Inf. Sci., **165**, 91–101.

[21] Encinas L. H., White S. H., del Rey A. M., Sánchez G. R. (2007). *Modelling forest fire spread using hexagonal cellular automata*, Applied Mathematical Modelling, **31**(6):1213–1227.

[22] Sipper M. and Tomassini M. (1996). *Co-evolving Parallel Random Number Generators*, Proceedings of the 4th International Conference on Parallel Problem Solving from Nature, LNCS 1141, 950–959.

[23] Koroglu M.E., Siap I. and Akn H. (2014). *Error correcting codes via reversible cellular automata over finite fields*, Arab. J. Sci. Eng., **39**(3):1881–1887.

[24] Koroglu M.E., Siap I. and Akn H. (2016). *The reversibility problem for a family of two-dimensional cellular automata*, Turkish J. Math., **40**(3):665–678.

[25] Chattopdhyay P., Choudhury P. P., Dihidar K. (1999). *Characterisation of a particular hybrid transformation of two-dimensional cellular automata*, Comput. Math. Applic., **38**, 207–216.

[26] Hellekalek P. (1998). *Good Random Number Generators are (not so) Easy to Find*, Mathematics and Computing Simulation, **46**(5-6):485–505.

[27] Lipschutz S. (1990). *Theory and problems of linear algebra*, Mc Graw Hill Inc.

[28] Blackburn S.R., Murphy S. and Peterson K.G. (1997). *Comments on theory and applications of cellular automata in cryptography*, IEEE Trans. Comput., **46**, 637–638.

[29] Wolfram S. (1983). *Statistical mechanics of cellular automata*, Rev. Mod. Phys., **55**(3):601–644.

[30] Wolfram S. (1985). *Cryptography with Cellular Automata*, Advances in Cryptology: Crypto '85 Proceedings, LNCS 218, 429–432.

[31] Zhai Y., Yi Z., Deng P. (2010). *On behavior of two-dimensional cellular automata with an exceptional rule under periodic boundary condition*, The Journal of China Univ. of Posts and Telec. **17**(1):67–72.

[32] Ying Z., Zhong Y. and Pei-min D. (2009). *On behavior of two-dimensional cellular automata with an exceptional rule*, Information Sci., **179**(5):613–622.

[33] Yang Y.G., Zhao Q.-Q. (2016). *Novel pseudo-random number generator based on quantum random walks*, Sci. Rep. 6, 20362; doi:10.1038/srep20362.