DIGITAL ASSIGNMENT-1

Cyclic Cellular Automata – Principle and Applications

Team Members:

Harsh Khandelwal (17BIT0191)

Garvit Kataria (17BIT0101)

Ujjwal Sinha(17BIT0099)

Abstract

The Cellular Automata Theory is a distinct model that is currently being utilized in scientific researches and simulations. The model is comprised of some cells that changes in accordance with a particular rule over time. This paper provides a survey of the Modelling and Applications of Cellular Automata Theory, that targets the program realization of Cellular Automata Theory and therefore the application of Cellular Automata in every field, like road traffic, land use, and cutting machines. every application is further explained, and a number of other are related to main models are concisely introduced. This research aims to assist decision-makers formulate applicable development plans.

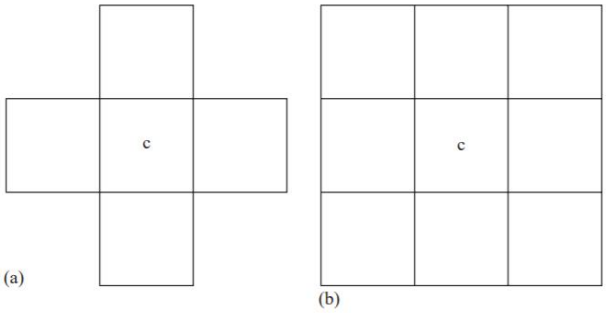


Fig. 1. Two-dimensional (a) von Neumann and (b) Moore neighbors of cell *c*.

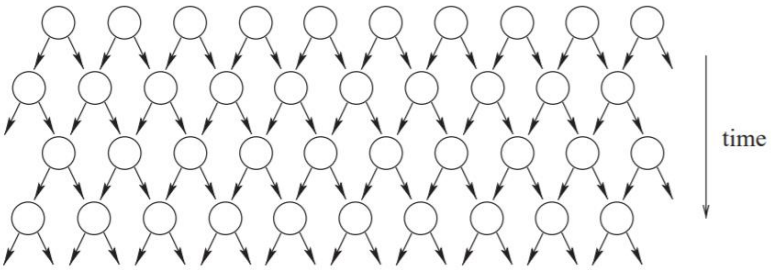


Fig. 2. Dependencies in one-dimensional, radius-$\frac{1}{2}$ CA.

Introduction

Cellular automata (CA) are among the oldest models of natural computing, qualitative analysis back over half a century. the initial CA studies by John Neumann during the late Nineteen Forties were biologically intended, the goal was to develop self-replicating artificial systems that are also computationally universal.

Neumann clearly wanted to analyse artificial computing devices analogous to human brain in which the memory and the process units aren't separated from one another, that are massively parallel which is capable of repairing and building themselves given the required material.

Following suggestions by S. Ulam, he visualised a separate universe consisting of a two-dimensional mesh of finite state machines, known as cells, interconnected regionally with one another. The cells bring changes to their states synchronously reckoning on the states of some close cells, the neighbours, as determined by an area update rule. All cells use identical update rule so the system is homogeneous like several physical and biological systems. These cellular universes are currently known as CA. Von Neumann's line of analysis on self-replicating CA was continued later by different authors.

CA possess many elementary properties of the physical world, they are massively parallel, homogeneous each and every interactions are native. different physical properties like reversibility and conservation laws are often programmed by selecting the native update rule properly. it's not shocking that physical and biological systems are successfully simulated with CA models . separate simulation of fluid flows using CA as even become a field of its own during which CA models are referred to as lattice gases. See, for example, for 2 elementary lattice gas models. different classic CA simulations of physical systems embrace using spin models and diffusion phenomena, e.g.

The physical nature of CA might have even a lot of larger sensible importance once applied to the other direction, that is, once using the physics to simulate CA. Since several CA are computationally universal—and some are simple and easy CA have this property—then maybe we tend to eventually succeed to harness physical reactions of microscopic scale to execute massively parallel computations by running a computationally universal CA. this needs that the simulated CA obeys the foundations of physics, together with reversibility and conservation laws.

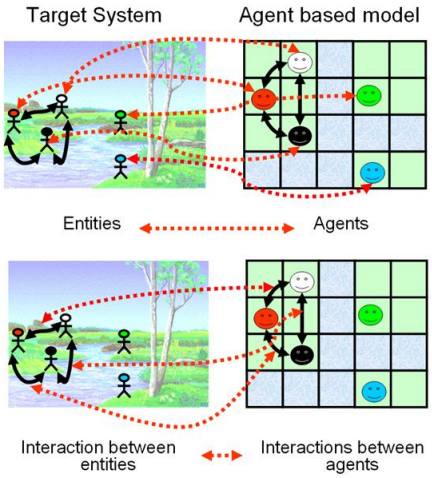
While such truly programmable matter could also be decades away, its potential is nice
In this tutorial article, we tend to review basic theoretical results regarding CA in computer science. the sector is incredibly broad and also the analysis is spirited, therefore it's solely attainable to hide bound
aspects of the sector. the chosen topics replicate the analysis interests of the author, and they include changeability, conservation laws, decidability queries, machine catholicity
and limit behaviour. For different topics see, for instance, books . we tend to begin by defining basic ideas.

Related works

Agent-based models and partial differential equations are techniques which work similar to cellular automata.

Agent is primarily based on modelling focus on the individual active parts of a system. This can be in distinction to all the additional abstract system dynamics approach, and therefore the process-focused separate event technique.

With agent primarily based modeling, active entities, called agents, should be known and their behavior outlined. They will be individuals, households, vehicles, equipment, products, or corporations, whatever has relevancy to the system. Connections between them are established, environmental variables set, and simulations run. The worldwide dynamics of the system then emerge from the interactions of the various individual behaviors.



The **Partial Differential Equations** are a continuous approach and could be used to represent the interaction of variables in space in a similar approach used by cellular automata.

You should consider for each cell an initial condition and represent in the model set of equations how the variables interact and diffuse in the discretized space. A numerical method such as finite differences could be easily implemented to solve these equations.

Comparison of Different Techniques

Techniques	Advantage	Disadvantage	Mathematical Equations
QR Code Encryption Based on Cellular Automata	Advantage is that this method uses the cellular automata to encrypt and	If this system is decrypted incorrectly then there is a huge deviation in	$GDD\ (I, I') = \frac{E'(GD\ (x, y)) - E(GD\ (x, y))}{E'(GD\ (x, y)) + E(GD\ (x, y))}$

	decrypt QR code binary image with such parameters	results due to sensitivity.	
Cellular Automata Based Synthesis of Easily And Fully Testable FSMs	The scheme provides extremely high coverages close to 100 per cent for all single faults in the circuit.	Area requirements are prohibitive and with long scan path chains, the testing time requirement is also quite high.	$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad p(x) = x(1+x)^3.$

Proposed Technique Explanation & Architecture

1) QR Code Encryption Based on Cellular Automata

Technique Explanation

Elementary Cellular Automata State Ring
The state ring is a part of the state transition diagram. An elementary cellular automata with length of 8 has 256 different global states, respectively is 0 to 255. The study of elementary cellular automata can be realized by means of studying the state evolved by the cellular automata under corresponding rule. Each state ring contains 2, 4 or 8 states. The rest states which are not included in the cellular automata diagram evolve according to the last state on the state ring and along the ring. In these state rings, some state rings possesses many properties

XOR operation can start from any state, that is to say, state can be any state on the ring. The properties of state ring is the basic of the following encryption method. To get the encryption information, the method uses the t states of the ring to do t times XOR

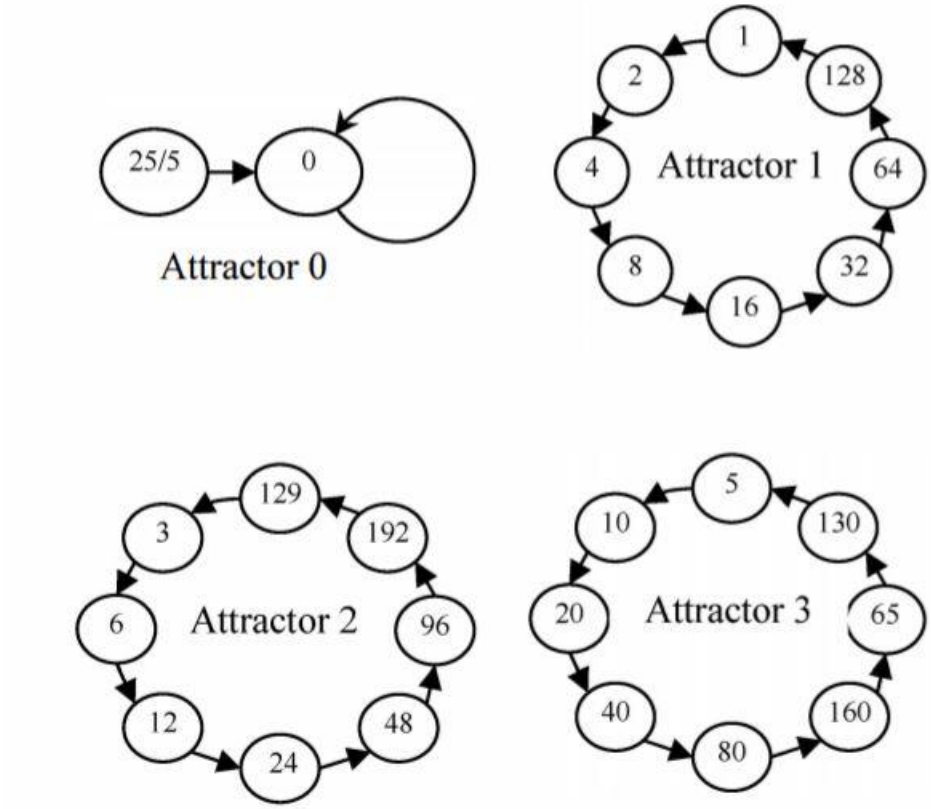
operation with the information d which is to be encrypted. Then, to get the original information, using the rest k - t states of the ring which is obtained last step to do k - t times XOR operation with the information encrypted. The rule can be used for images encryption. In addition, the phenomenon exits in other rules of elementary cellular automata.

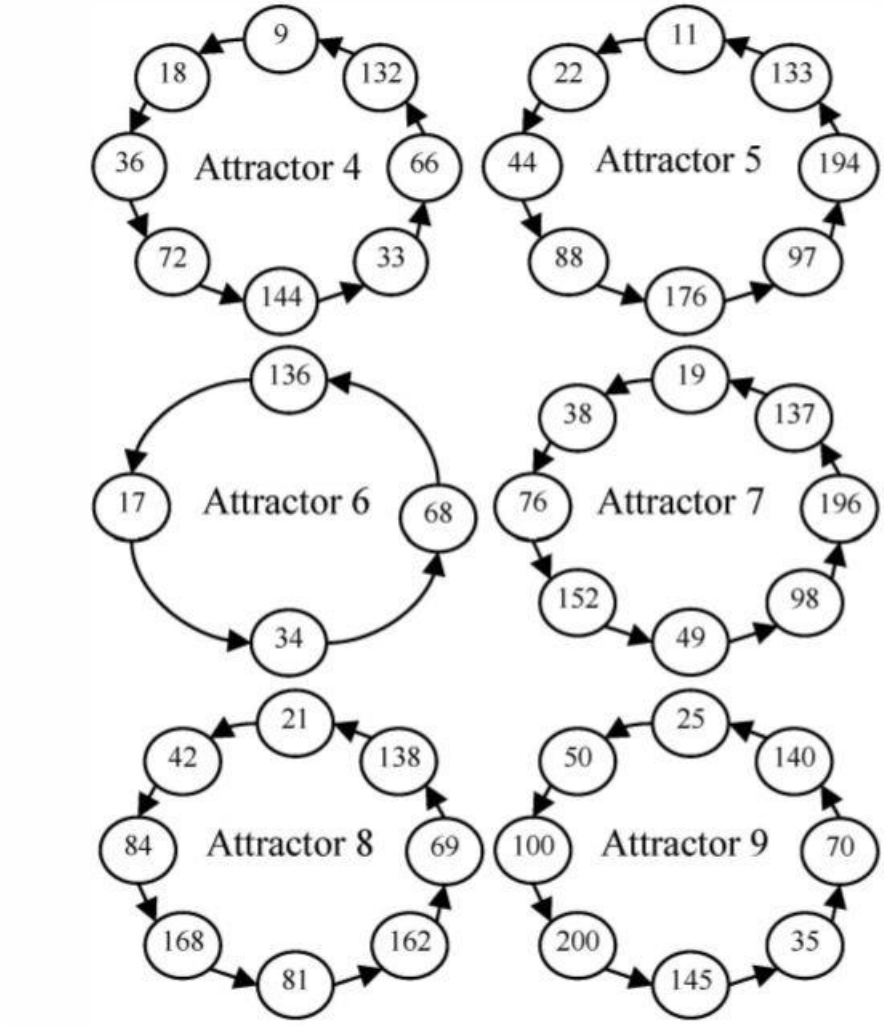
Settings of Key

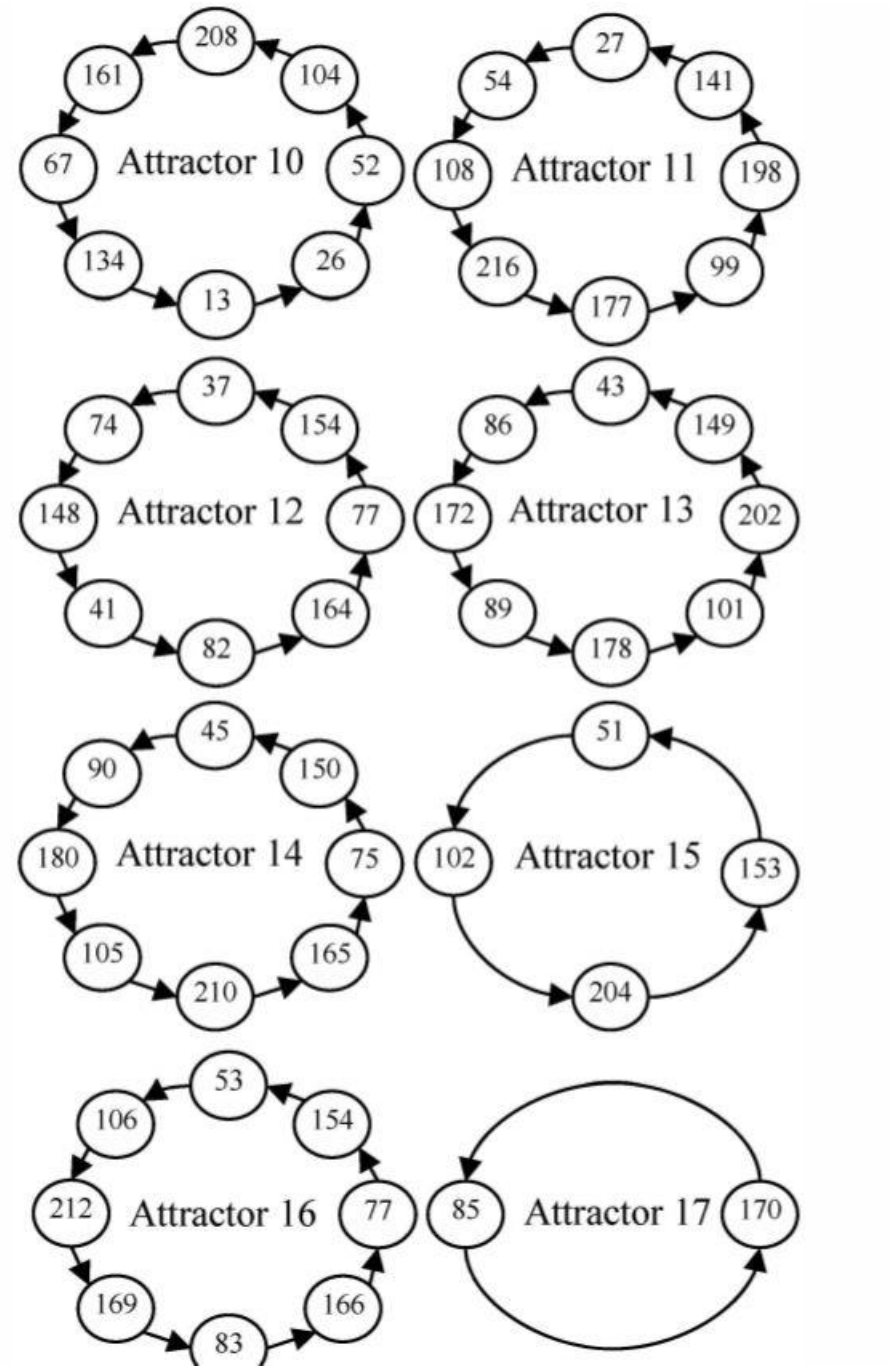
The image encryption mode is the symmetric encryption mode, so the sender and the receiver use the same encryption key and decryption key. The key concludes three parts: the initial state of the state ring state , the rules of ECA rule , and the seed of the random number generator seed. The paper uses the size of 256*256 QR code binary image to do the simulation experiment. The key is (53, 42, 8192). 53 represents the elementary cellular automata's state in state ring 16 as shown in Attractor 16. The random number generator seed is seed = N * N / 8 = 8192 .

Architecture

The Architecture of the above automata can be done in the following way using attractors and generators:


25/5
0
Attractor 0
1
2
128
4
Attractor 1
64
8
32
16
129
3
192
6
Attractor 2
96
12
48
24
5
10
130
20
Attractor 3
65
40
160
80


Attractor 4
9
18
132
36
66
72
33
144
Attractor 5
11
22
133
44
194
88
97
176
Attractor 6
136
17
68
34
Attractor 7
19
38
137
76
196
152
98
49
Attractor 8
21
42
138
84
69
168
162
81
Attractor 9
25
50
140
100
70
200
35
145


208
161
104
67
Attractor 10
52
134
26
13
27
54
141
108
Attractor 11
198
216
99
177
37
74
154
148
Attractor 12
77
41
164
82
43
86
149
172
Attractor 13
202
89
101
178
45
90
150
180
Attractor 14
75
105
165
210
51
102
Attractor 15
153
204
53
106
154
212
Attractor 16
77
169
166
83
85
Attractor 17
170

2) Synthesis of Easily And Fully Testable FSMs

Technique explanation

State encoding strategy

It is well known that in a multilevel implementation of a combinational logic block, the number of literals in the optimized set of equations significantly affects the number of gates required to implement the circuit. Consequently, an attempt to minimize the number of literals in the optimized set of equations would lead to lesser circuit area requirements. This fact has been exploited in existing state encoding strategies like MUSTANG. In our scheme, we have given due consideration to this factor and have also attempted to find matches between the FSM state transitions and the state transitions of Dl*CA. The existence of such matches greatly helps in efficiently embedding the Dl*CA in the synthesized sequential machine. A suitable combination of these two factors is used to guide the state encoding scheme.

Architecture

Characterization of Dl*CA

A Cellular Automata (CA) consists of a number of interconnected cells arranged spatially in a regular manner. In essence, each cell is made up of a memory element (usually a D pap-pop) and a combinational logic generating the next-state of this cell from the present states of its neighbouring cells. If we express the next state function in the form of a truth table, then the decimal equivalent of the output column in the truth table is called the rule number of where @ refers to an ex-or function. A CA uses only Ex-or/Ex-nor as the next state logic. For an n-cell 1-dimensional additive CA it has been shown that the linear operator is an n x n matrix whose ith row specifies the neighbourhood dependency of the its cell. The next state of the CA is generated by applying this linear operator on the present state represented as a column vector. The operation is the simple matrix multiplication, but the addition involved is modulo-2 sum. The matrix is termed as the Characteristic Matrix of the CA, and is denoted by T.

Dl*CA based FSM synthesis

In order to implement an n-state FSM, we have chosen to use a rZog2nl cell Dl*CA, having the rule configuration < 90,102,102. 1012 >. The unique state transition properties of Dl*CA and those of D1 * CA dual make this class of CA the most suitable candidate for our design scheme.

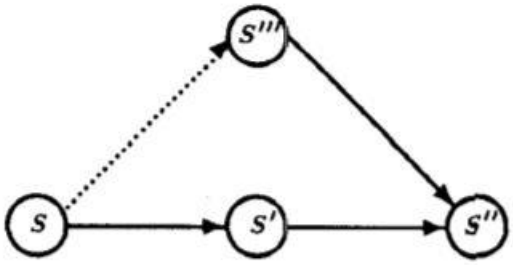


Figure 1: **Relationship of states in a D1*CA and its dual**

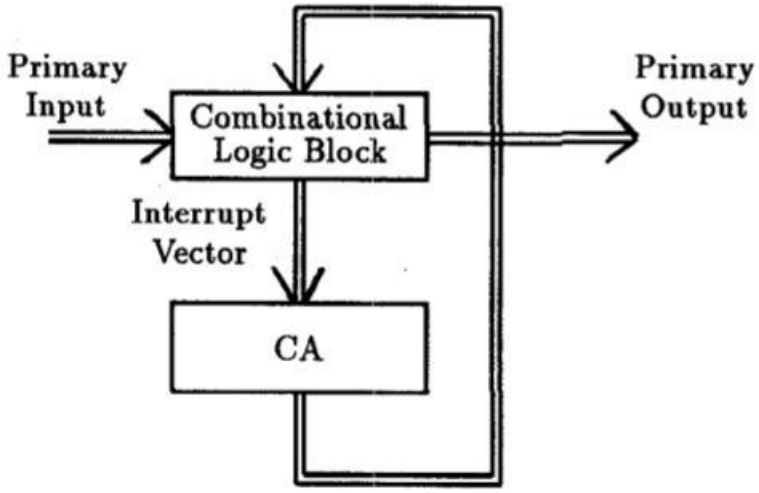


Figure 2: **Block Diagram of a CA Based FSM**

Implementation

Encryption Process

Firstly, convert the grey value matrix of plain image into a one-dimensional array in the form of rows. Then the grey values of 8 consecutive pixels are divided into a group. For example, the size of N * N QR codes binary image will be divided into N * N / 8 group. From the random number seed , a length of seed pseudorandom integer array T is got. T needs to be satisfied by the automata equations, ten) represents the number of encrypt time of the nth group's grey value in QR code binary image. Similarly, k -ten represents the number of deciphering time. Use the size of 256*256 QR code binary image to do the simulation experiment, so N equals to 256, k equals to 8, and seed equals to 8192. Second, using each group of grey value as a unit to encrypt the QR code binary image. Each group of grey value is expressed as pixel/(n). Do XOR operation ten) times consecutively and each time the state of the state ring

do the XOR operation bitwise. These ten states are consecutive on the state ring and represents the state at the beginning of encryption. C(n) represents the nth group of grey values of the ciphered image after encryption. For example, for the eleven group of grey values, i = mod(11,8) = 3 , so the three states for the consecutive XOR operation are 212, 169 and 83. After all data are processed, reassemble them into binary image with size N * N .

The paper uses a size of 256*256 standard QR code binary image as the test image. Using the cellular automata which length is 8, boundary conditions as the cyclic boundary conditions, {O,I} as the state space and (53, 42, 8192) as the key. The core evaluation criterion of a image encryption system is the security of the image encryption. Now analyse the security of the method in the following aspects.

To test the correlation of adjacent pixels in the plain-image and in the ciphered-image, 1000 pairs of adjacent pixels are extracted randomly from the two images in the horizontal direction, vertical direction and diagonal direction. In order to validate the efficiency of encryption and decryption algorithm, the simulation experiments are done on the computer of 4.0 gigabyte memory, 64 bit operating system, 1.5 billion hartz processor. The experiments are implemented with matlab201 0 software. Using the DES encryption method, chaotic sequence encryption method and cellular automata encryption method to encrypt and decrypt the original image which size is 256*256 respectively. Each method does 20 times test respectively. Using the each method does the experiment 20 times respectively. The time of each method can be measured according to the average time to do the test 20 times.

Examples and Experimental Results:

The structure of cellular automata is that the transmission of a single native node to a different one. Thus, any transmission drawback, social or else, are often sculpturesque with a cellular structure with applicable transmission dynamics'.

Yu Xiaoyang, Song Yang, Yu Shuchun, Yu Yang, Cheng Hao, Guan Yanxia in their research paper have described the usage of Cellular Automata in the encryption of QR code. In that paper, he wrote that the the performance of the security and integrity of QR code,i.e, Quick Response Code can be increased by encryption and cryptography supported cellular automata. In order to achieve this feat, encryption technique is used along with cryptography methodology supported elementary cellular automata stage rings was planned during that paper. The cellular automata will stimulate the complex phenomenon for which the cellular automata is being developed by just using a dynamic system. Based upon this feature, the aim of this technique is to employ cellular automata to encode and decode the binary images of the QR code with parameters like length, the cyclic bpundary conditions and the state space of {0,1} as QR code can be considered as an image consisting of only black and white pixels so representing the entire QR code image as a square matrix with only 0 and 1 being the elements representing black and white respectively.

Experimental results of the method given in that paper shows that the new method is much more faster, with good effect and with high security. The key of the of the encrypted image is very sensitive and even a small deviation in the key creates a drastic effect in the decryption of the image. It was also noticed that the correlation between the various adjacent pixels in all directions like vertical, horizontal and diagonal was much higher in the plain image and much lower in the ciphered encrypted image. This ensured that the adjacent pixels in the encrypted image are almost irrelevant, as the correlation coefficient in the encrypted image is very close to zero. It means that the statistical features and the original plain image without encryption are spread well enough in the decrypted ciphered image and hence we can conclude that the encryption with the key can create a unique encryption which ensures the primary condition for cryptography,i.e, one to one correspondence. Coming to the most important aspect, i.e, speed test, experimental results have shown that the time taken in the encryption of a encryption techniques like DES is roughly three times the time taken in the encryption by use of cellular automata. Similarly the decryption time of a encryption by use of DES is roughly four times than that of Cellular automata technique. Also since the key space of a cellular automata is quite large, cellular automata can resist the attack of key effectively.

In the Finite State Machine design procedure based on D1*C1 Cellular Automata, the state itself are encoded by means of an encoding module. Post encoding, we optimize the combinational logic of this Finite State Machine using MISII.

Challenges:

Experimental arithmetic provides a primary approach to the present downside. One performs
explicit simulations of cellular automata, and tries to seek out empirical rules for his or her
behaviour. These could then recommend results which will be investigated by a lot of standard mathematical ways.

Use of the finite information density of cellular automaton configurations, and the finite rate of information propagation in cellular automata, variety of inequalities may be derived between entropies and Lyapunov exponents .

Several straightforward observations could also be created. First, if the cellular automaton lattice is over one-dimensional, one could contemplate Lyapunov exponents in numerous
directions on this lattice.

Random sampling yields some empirical indications of the frequencies of various classes of behaviour among cellular automaton rules of assorted sorts. For centrosymmetric
one-dimensional cellular automata, category one and a pair of cellular automata seem

to become progressively less common as k and r increase; category three becomes a lot of common,and class four slowly becomes less common.

Future Opportunities:

Modern urban traffic:
In this we tend to introduce a replacement cellular automata approach to construct AN urban traffic quality model. supported the developed model,characteristics of worldwide traffic patterns in urban areas area unit studied. Our results show that totally different control mechanisms used at intersections like cycle length, inexperienced split, and coordination of traffic lights have a big impact on bury vehicle spacing distribution and traffic dynamics.These findings give vital insights into the network property behaviour of urban traffic,which area unit essential for planning applicable routing protocols for transport impromptu networks in urban eventualities.

Seed encoding with LFSRs and cellular automata:

Reseeding is employed to enhance fault coverage of pseudo-random testing. The seed corresponds to the initial state of the PRPG before filling the scan chain. During this paper,we gift a method for cryptography a given seed by the quantity of clock cycles that the PRPG must run to succeed in it. This cryptography needs several fewer bits than the bits of the seed itself. The price is that the time to succeed in the supposed seed. We have a tendency to cut back this value mistreatment the degrees of freedom (due to do not cares in check patterns) in determination the equations for the seeds. We have a tendency to show results for implementing our technique utterly in on-chip hardware and for applying it from a tester. Simulations show that with low hardware overhead, the technique provides 100% single-stuck fault coverage. Also, when put next with typical reseeding from associate external tester or on-chip memory board, the technique reduces seed storage by up to eighty fifth. We have a tendency to show the way to apply the technique for each LFSRs and CA.

References:

- Sarkar, P. (2000). A brief history of cellular automata. Acm Computing Surveys, 32(1), 80-107.
- T. Ceccherini-Silberstein, M. Coornaert, Cellular automata and groups, Springer Monographs in Mathematics, Springer-Verlag, Berlin (2010).
- E.R. Berlekamp, J.H. Conway, R.K. Guy, Winning Ways for Your Mathematical Plays, Academic Press (1982).
- M. Margenstern, on a characterization of cellular automata in tilings of the hyperbolic plane, Internat. J. Found. Comput. Sci. 19 (2008), no. 5, 1235–1257.
- J. Kari, Theory of cellular automata: A survey, Theoretical Computer Science 334 (2005), 3–33.
- Shun Wai Tsang, Yee Leung. A Theory-Based Cellular Automata for the Simulation of Land-Use Change. Geographical Analysis 43(2011), no. 2, 142-171.
- Xianjuan Kong. Research on Modelling and Characteristics Analysis of Traffic Flow Based on Cellular Automaton. Beijing Jiaotong University, 2007.
- Xingqin Cao. The Cellular Automata Studying of Complex System. Huazhong University of Science and Technology, 2006.
- Xia Li, Jiaan Ye. Neural network based cellular automata and simulating complex land use system. Geography Research (2005), no. 24, 19-27.
- Wolfram, Stephen. A New Kind of Science. Champaign, IL: Wolfram Media Inc., 2002.
- Davis, Martin. The Universal Computer: The Road from Leibniz to Turing. New York: Norton, 2000.
- J. Albert, K. Culik II, A simple universal cellular automaton and its one-way and totalistic version, Complex Systems 1 (1987) 1–16.
- S. Amoroso, Y. Patt, Decision procedures for surjectivity and injectivity of parallel maps for tessellation structures, J. Comput. System Sci. 6 (1972) 448–464.
- H. Aso, N. Honda, Dynamical characteristics of linear cellular automata, J. Comput. System Sci. 30 (1985) 291–317.
- C. Bennett, Logical reversibility of computation, IBM J. Res. Develop. 6 (1973) 525–532.
- R. Berger, The undecidability of the Domino problem, Mem. Amer. Math. Soc. 66 (1966).
- E.R. Berlekamp, J.H. Conway, R.K. Guy, Winning Ways for Your Mathematical Plays II, Academic Press, New York, 1982.
- F. Blanchard, A. Maass, Dynamical properties of expansive one-sided cellular automata, Israel J. Math. 99 (1997) 149–174.

- N. Boccara, H. Fuks, Number conserving cellular automaton rules, Fund. Inform. 52 (2002) 1–13.
- T. Boykett, C. Moore, Conserved quantities in one-dimensional cellular automata, unpublished manuscript, 1998. 32 J. Kari / Theoretical Computer Science 334 (2005) 3 – 33
- A.W. Burks, Von Neumann's self-reproducing automata, in:A.W. Burks (Ed.), Essays on Cellular Automata, University of Illinois Press, Champaign, IL, 1970, pp. 3–64.
- G. Cattaneo, E. Formenti, G. Manzini, L. Margara, Ergodicity, transitivity, and regularity for linear cellular automata over Zm, Theoret. Comput. Sci. 233 (2000) 147–164.
- C. Choffrut, K. Culik II, On real-time cellular automata and trellis automata, Acta Inform. 21 (1984) 393–409.
- B. Chopart, M. Droz, Cellular Automata Modeling of Physical Systems, Cambridge University Press, Cambridge, 1998.
- E.F. Codd, Cellular Automata, Academic Press, New York, 1968.
- J.H. Conway, unpublished, 1970.
- K. Culik II, An aperiodic set of 13 Wang tiles, Discrete Math. 160 (1996) 245–251.
- K. Culik II, S. Yu, Undecidability of CA classification schemes, Complex Systems 2 (1988) 177–190.
- K. Culik II, L.P. Hurd, S. Yu, Formal languages and global cellular automaton behavior, Physica D 45 (1990) 396–403.
- K. Culik II, J. Pachl, S. Yu, On the limit sets of cellular automata, SIAM J. Comput. 18 (1989) 831–842.
- E. Czeizler, J. Kari, A tight linear bound on the neighborhood of inverse cellular automata, to appear.
- R.L. Devaney, An introduction to chaotic dynamical systems, Addison–Wesley, Reading, MA, 1989.
- B. Durand, Global properties of 2D cellular automata, in:E. Goles, S. Martinez (Eds.), Cellular Automata and Complex Systems, Kluwer, Dordrecht, 1998, .
- B. Durand, E. Formenti, G.Varouchas, On undecidability of equicontinuity classification for cellular automata, in:M. Morvan, E. Remila (Eds.), Discrete Mathematics and Theoretical Computer Science Proceedings AB, 2003, pp. 117–128.
- J. Durand-Lose, Representing reversible cellular automata with reversible block cellular automata, in:R. Cori, J. Mazoyer, M. Morvan, R. Mosery (Eds.), Discrete Models Combinatorics Computation and Geometry, Springer, Berlin, 2001, pp. 145–154.