K. J. Somaiya College of Engineering, Mumbai-77

(A Constituent College of Somaiya Vidyavihar University)

Department of Information Technology

TOC IA-II Literature Survey Report
AY ODD 2022-23

Group No: 23

Personal Information	**Roll Number**	16010420112	16010420113	16010420114	16010420117
	Name	*Hardika Nehate*	*Prathik Chadaga*	*Preeti Shah*	*Soham Bhoir*

By Student 1 Name :Hardika Nehate

Topic Description:

Wire-crossing is an issue in quantum-dot cellular automata (QCA) design. In this paper, QCA based universal logic gate (ULG) is proposed to reduce the number of wire-crossings. Using the ULGs, full adder/subtraction, full comparator and 4-to-1 multiplexer are designed. QCA Designer simulation results show that the proposed circuits have correct logic function. Compared with traditional design based on majority gates and inverters (MIs), the ULG based design can reduce the number of wire-crossings.

Concept behind the paper :

Design and Application of Universal Logic Gate based on Quantum-Dot Cellular Automata

Problem/Solution discussed :

Using the Universal Logic Gate, full adder/subtraction, full comparator and 4-to-1 multiplexer are designed. Compared with traditional design based on majority gates and inverters, the Universal Logic Gate based design can reduce the number of wire-crossings. In current Quantum-Dot Cellular Automata based design, the fundamental logic element is the majority gate. Majority gate and inverter, which consist of logic set, are used to design Quantum-Dot Cellular Automata and circuits.

Adder [3,4], comparator, multiplier multiplexer designs are some typical examples. Minimization of wire-crossings is one of the major issues for Quantum-Dot Cellular Automata based design. MI based design may not be optimized in terms of wire-crossings. Some common combinational circuits are designed based on Universal Logic Gate. Compared with MI based design, Universal Logic Gate based design can reduce the number of wire-crossings.

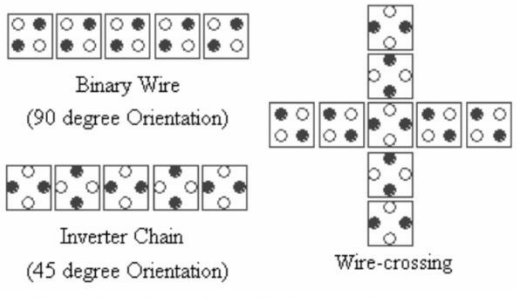


Figure 4. QCA wire and wire-crossing structure

Quantum-Dot Cellular Automata cell is a nano-scale device which can store logic states and transmit information by Coulomb interaction.

Quantum-Dot Cellular Automata Logic Gates - the logic function of majority gate is both logic AND and OR functions can be implemented by setting one input into 0 or 1. Since the majority logic gate only is not logic completed, Quantum-Dot Cellular Automata inverter is also used to form a completed logic set. Logic set 5 shows its logic symbol, four clocked Quantum-Dot Cellular Automata cells with different colors and the Quantum-Dot Cellular Automata implementation. Logic symbol and Quantum-Dot Cellular Automata implementation of the UNIVERSAL LOGIC GATE A function with m-inputs can achieve any function with a given number of variables, known as universal logic function, the corresponding gate is known as universal logic gate. From, its logic schematic diagram and Quantum-Dot Cellular Automata implementation can be obtained

Logic set 8 shows the logic schematic diagram and Quantum-Dot Cellular Automata implementation of the full comparator based on the MI design. it can be seen that for the Universal Logic Gate based design, 353 cells are required, there are 9 wire-crossings in the circuit and the time delay is 2.25 clocks while for the MI based design . Compared to the MI based design, the Universal Logic Gate based implementation achieves 22.2% reduction in terms of the number of wire-crossings.

Circuit		Full adder/ subtraction	Full comparator	4-to-1 multiplexer
ULG based design	QCA cells	432	353	273
	Time delay (clocks)	2.25	2.25	2.25
	Number of wire crossings	15	9	12
MI based design	QCA cells	288	222	287
	Time delay (clocks)	1.5	2	2
	Number of wire crossings	16	11	16

TABLE l summarizes the result implementing these circuits by using ULG and MI based design, respectively. From TABLE I, it can be seen that ULG based design has advantage in term of the reduction of wire-crossings.

It is pointed out that in the design of 4-to-1 multiplexer, the Universal Logic Gate based design requires fewer number of Quantum-Dot Cellular Automata cells than MI based design apart from the reduction of wire- crossings. Logic schematic diagram of the full comparator of Universal Logic Gate based design & Quantum-Dot Cellular Automata implementation of the full comparator of Universal Logic Gate based design minimises the wire-crossings is a crucial in Quantum-Dot Cellular Automata design. Three classic circuits are designed to test the efficiency of the proposed approach.

Conclusion :

The results show that Universal Logic Gate based design can reduce the number of wire-crossings compared with MI based design & it minimises the wire-crossings is a crucial in Quantum-Dot Cellular Automata design.

By Student 2 Name : Prathik Chadaga

Topic Description:

Public and private organisations are adamant on developing cryptographic techniques to ensure safety and authenticity in many fields. To achieve this objective, there are various applications used in this domain and cellular automata is one of them. Cellular automata are used due to its ability of generating pseudo-random bit sequences for symmetric systems where the encryption and decryption are similar/ calculated from each other.

Concept behind the paper:

Application of cellular automata (CAs) to symmetric key cryptography - stream cipher is particularly described in this paper. A cellular automaton is a arrangement of cells in a grid where every cell changes its state according to its given function. One dimensional Cellular Automata are generally used for generating a Pseudo-random Number Sequence (PNSs) which is employed in a secret key cryptographic system, especially in stream and block cipher [2]. The randomness of PNS depends on the set of applied CA rules the principles depend on a technique called cellular programming. When started from a random initial configuration, its configuration remains random at whenever step; however, any configuration with only finite non-zero cells become a replicator that eventually fills all of the cells with copies of itself.

Problem/Solution discussed:

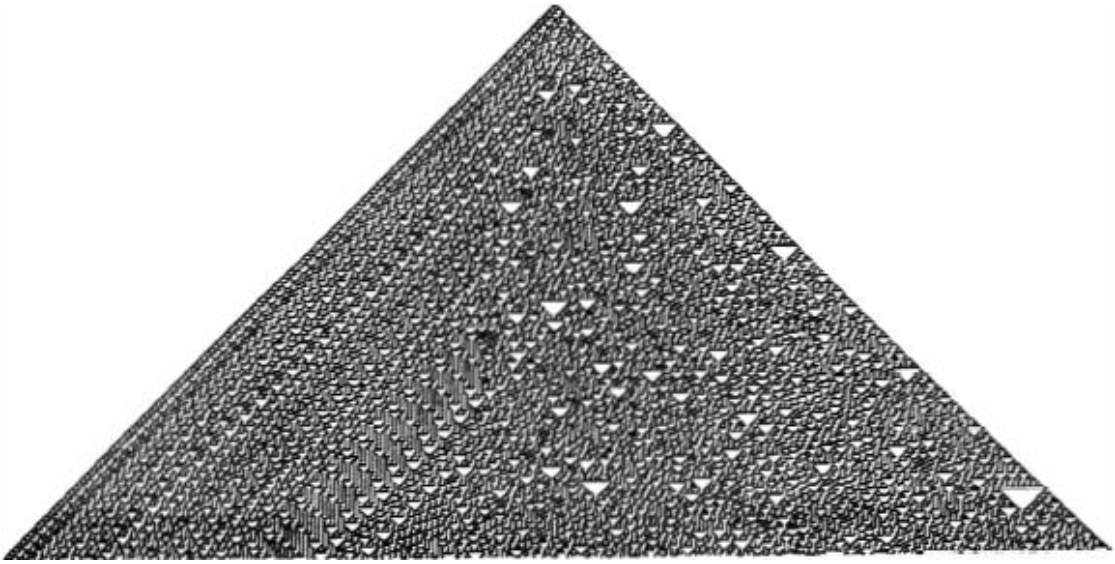
Implementation Steps

An elementary cellular automaton is predicated on a function. Consider a cellular automaton having a circular register. It consists of a one-dimensional array of N cells, each of which may hold either a 0 or a 1 value represented by a_i ; in each time step all values are simultaneously replaced by the exclusive or of the two neighboring values. Current value of the cell is denoted by $\mathbf{a_i'}$.

The values are updated according to given function:

$$\mathbf{a_i' = (a_{i-1} + a_{i+1} + a_i a_{i+1}) mod 2}$$

The filled cellular automata according to the function will be represented by the following:



Where 1 denotes black colour and 0 denoted white colour.

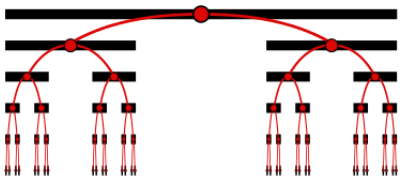
Since $\mathbf{a_i'}$ can also be determined by $\mathbf{a_{i-1}}$ **XOR (** $\mathbf{a_i}$ **OR** $\mathbf{a_{i+1}}$**)** it can be said that the iterations are a **Boolean** function of initial cell values. A binary plain text $\mathbf{P_i}$ will be considered as the input for the cryptographic system. A specific sequence of values from the entire pattern will be used as a random stream at i^{th} generation instant $\mathbf{a_i}$. Hence the cipher text C_i will be represented by

$\mathbf{C_i = P_i}$ **XOR** $\mathbf{a_i}$

Since it is a stream cipher, the similar process is repeated for decryption i.e.

$\mathbf{P_i = C_i}$ **XOR** $\mathbf{a_i}$

Problems



Assuming N tends to infinity, the automata over a period of time generates into a **cantor** set which is represented by the following diagram which will increase the time complexity of the entire cipher and exponentially increase the length of the PNSs.

The security of this cipher will be based on finding the state value (initial seed value of the cellular automata) and if it is known then it is easy to find the entire automata using the function through which a_i is generated and the cipher can be deciphered in a very slow manner.

Conclusion:

The system that has been discussed is secure and will be further secured when a 2-D CA is used. Different rulesets (given by Stephan Wolfram) can be considered since the result of the functions given by the particular ruleset generates high quality PNSs. Indeed, the standard of PNSs outperforms the quality of known one dimensional CA-based and therefore PNS generators using 1DCA can used for secret key cryptography.

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Department of Information Technology

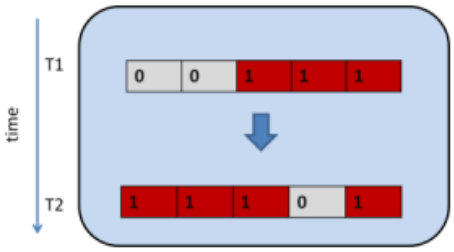
By Student 3 Name : Preeti Shah

Topic description: Cellular automaton is the problem-solving approach that works on simple rules to give solutions in a non-obvious way. In this approach a cellular model is built for the problem space, several rules are implemented to predict the state of the system at some time instance. CA deals with only local information of each cell and provides an excellent platform to solve complex problems.

Concept behind the paper: Motivation is taken from Stan Ulham and J. Von Neumann's work wherein Neumann worked on the concept of a self-reproductive machine. A cellular automaton builds the model of the universe and treats it as a system (cellular system). It is convenient to study some system by breaking it in small parts, finding the influence of parts on each other and then predicting the system as a whole. Humans have created computers that can solve exceedingly complicated issues in a matter of seconds to solve the universe's problems quickly and with little effort. This paper discusses how Cellular automata have proven to be extremely effective in the direction of automating the problem-solving approach.

Problem/Solution discussed:

- Basic ingredients of Cellular system:
  1. Cellular space: A cellular system is a system that is broken into small pieces (cells) The space of the collection of these cells is called the cellular space. These cells can reside in one dimensional, 2 dimensional, or n-dimensional space.
  2. State and State set: In computer programming, a state set is the set of all possible values that can be taken by the state of a cell in a system at any one time. A special state that represents a cell's resting or inactive condition is called the quiescent state.
  3. Time Variable: the model of any universal object in cellular space i.e. cellular system changes with time, hence the state of the cells changes with every time instance, in turn, it helps to easily trace the system at every instance of time.



  4. Neighborhood: A cell is a. collection of cells that directly influences the behavior of another cell (including current cell) - i.e. its neighbors - termed as the neighborhood of the current cell. There are different types of neighborhoods like Neumann neighborhood, Moore and extended Moore neighborhood etc.
  5. State transition function:The rule according to which a cell acquires its future state on the basis of its own and neighbors'current state is called the state transition rule/function.The rules are further divided into different categories on the basis of the dependence of the current cell upon its neighbors which are:
     a) Standard rule: new state of the cell is related to the state of its neighborhood cells.
     b) Totalistic: new state depends only upon the sum of values of neighborhood states (including it). . If state of the cells at time t is represented as si(t) and

ϕj(t) is the transition function for cell j, then mathematically we can write:

$$\phi_j(t) = \sum_{i=1}^{n} s_i(t)$$

where i represents the number of the neighbor of the cell.

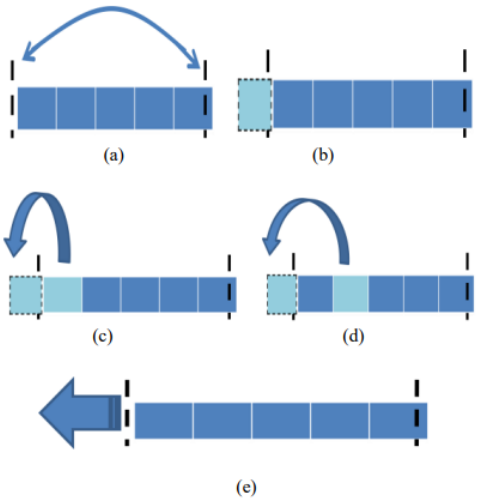
c) Outer totalistic - New state depends upon the sum of values of neighborhood states (excluding it). If state of the cells at time t be represented as si(t) and ϕj(t) be the transition function for cell j, then mathematically we can write where i represents the number of neighbor of the cell.

$$\phi_j(t) = \sum_{\substack{i=1 \\ i \neq j}}^{n} s_i(t)$$

d) Symmetric- the rule is symmetric with respect to permutation if it is not affected by the permutation of the neighborhood cells.

6. Boundary conditions: Sometimes for a finite space boundary cells do not have enough neighbors so that we can apply the transition rule to them. To solve this problem there are various boundary conditions according to the problem one or more condition is used. The conditions are as follows:

a) Periodic- Gluing opposite boundary cells to form a toroid.
b) Assigned- A virtual cell is assumed a neighborhood with some state.
c) Adiabatic- Copying boundary cell itself of cellular space to form neighborhood cell.
d) Mirror- Copying the cell state of the cell next to the boundary cell.
e) Absorbing- Simulate the finite space and the behavior of the infinite space.
For better understanding:



7. Initialization and termination: Assigning the initial state to the system is called the initial condition. The condition to stop updating process is called the termination condition.

- Definition: Consider a space divided into cells, where each cell is repeatedly "updated" to a new state in an evolving sequence. A program of this nature is specifically called a cellular automaton when it is 1) parallel, 2) local, and 3) homogeneous (optional).
- We should use cellular automata over mathematical equations because it is easier as

well as effective to deal with pictures than to solve the problem with pure mathematical equations which have many conditions and may consume more memory due to many variables.

- Cellular systems (CA) are classified according to the states of cells used, rules of transition used, or patterns that occur in various generation,s etc. Some of the categories are Homogeneous state, homogeneous transition, Periodic system, chaotic and structured.
- John Conway's game of life: We have a 2d matrix of cells wherein each generation switches cell on(alive) or off(dead) depending on the state of the cells that surround a given cell. 8 cells surround a given cell in this game. Based on how many cells are on(alive) we determine the death, birth or stasis of a cell [5].
  If cell is dead:
  — Reproduction- It becomes alive if it has exactly 3 alive neighbors among eight surrounding neighbors.
  — Stasis:R emain dead otherwise.
  If a cell is alive:
  — Loneliness- It Dies if it has less than 2 alive neighbors.
  — Stasis - Remains alive if it has 2 or 3 alive neighbors
  __ Overcrowding- Dies if it has more than 3 alive neighbors.
- Cellular automata and Cryptography: Cryptography is the branch of communication that was developed to build some rules in order to make secure communication between two or more parties. In private key cryptography, we encrypt the message (that is to be secured) with one secret key. At the receiving end the same secret key is used to decrypt the message. The key should be random (unpredictable) and used only once to achieve this goal CA is used to generate the key for one session.
- The complexity of cellular automata directly depends upon the states of the cells used and the neighboring cells used. In fact, an increment in these numbers increases the complexity, hence the time taken in execution increases.

Conclusion: Cellular automata help to explain the working of complex phenomena with the help of limited information about the local environment. Modeling and analysis of real-world models are very simple and effective with the help of Cellular Automata.

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Department of Information Technology

By Student 4 Name: Soham Bhoir

Topic description: Moving 2 dimensional cellular automata to a broader light by introducing to the problems like image noise removal and border detection in digital images. One of the key features of proposed approach discussed by researchers is that different schemes constructed on the basis of classic explicit scheme and classic implicit scheme combined with alternate segmentation technique.

Concept behind the paper: In several scientific domains, image processing has a wide range of applications. For instance, editing photos to make them seem better is known as image enhancement. The goal of image augmentation such as enhancing picture quality, readability, Traditionally, image enhancement is described in terms of transform or spatial (essentially the Wiener filter is likely the most well-known method in transform domains) ([6]). Another crucial step in image processing is edge detection. The study of edges has become a crucial part of the processing of biological or medical pictures.

Problem/Solution discussed:

1) **The CA Model for Filtering Digital Images**

A digital image consists of a two-dimensional array of n x n pixels. Each pixel is denoted by the triplet (i, j, k), where (i, j) signify its position in the array and k its corresponding colour. Researchers proposed a dynamic rule that has potential to solve the problem, the rule shall possess pathway from its initial noisy image to its final configuration of noise reduced image. It is desired that the dynamics apply without discrimination to all image types (monochromatic, grey level or color).

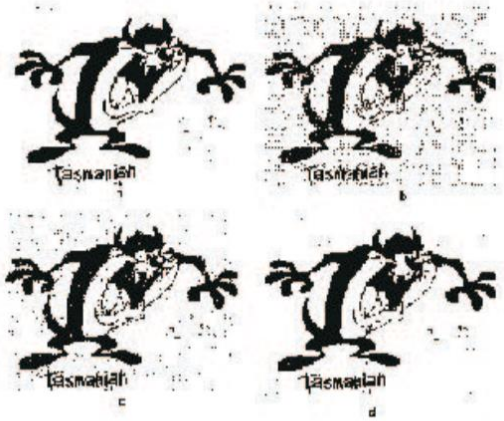


Figure 1: a) Original image; b) Image with noise;
c) Result of the Gaussian filter; d) Result produced by CA

This model's outcomes are depicted in Figure 1 d). A comparison with the Gaussian filter demonstrates (see Figure 1 c and d) that CA provides a superior image improvement.

2) **The CA Model for Border Detection in Digital Images**

In general, the relevance of a particular physical change in an image relies on the image's nature. For instance, a shift in intensity that is categorized as an edge in one application may not be deemed an edge in another. In this regard, it is essential that the boundary detection approach be independent of the image's properties. Given an image as the initial configuration state, this rule must demand that the cellular automaton reaches a final

configuration in which the only active cells correspond to the picture's borders. If the difference between the central cell state and each of the neighbouring cells is less than a threshold value, the central cell state will be zero next time; otherwise, it will remain unaltered. The rule applies whether the image is black-and-white, grayscale, or colour. Synchronously apply the transition rule.

Figure 2: Original image

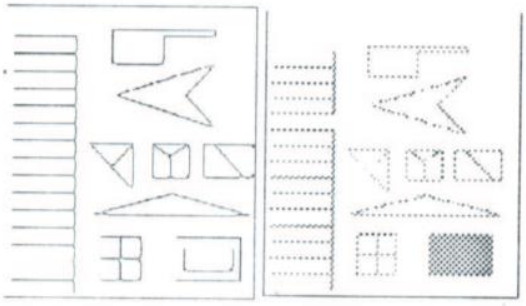


Figure 3: a) Result of SUSAN edge detector; b) Result of CA edge detector

Figure 3 (a) and (b) show the SUSAN edge detector and CA boundary detector outputs for Figure 2. The CA edge detector's border exhibits edge connection at junctions, no spurious edges, and qualitative resemblance to SUSAN's.

Conclusion: For a very effective border detector in digital photos, a two-dimensional cellular automaton with a very basic transition rule may be utilized. The cellular automaton-based boundary detection technique is generally applicable to monochrome, grayscale, and colored pictures. The outcomes are quite encouraging, and the cellular automaton border detector's output in digital pictures with no noise is highly good. In some circumstances, they could be equivalent to results obtained through the use of other edge detectors. Since the suggested approach is implemented on a cellular automaton, where individual cells update in a synchronous way and independently of one another, this method's inherent parallelism is a highly significant property. The suggested edge detector approach, we may infer, is quicker than other common edge detector methods.

K. J. Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Department of Information Technology

Summary of Literature Survey: We explored different applications of **Cellular automata**. Using cellular automata for deriving universal logic gates using quantum dots. With the use of universal gates it can reduce the number of wired crossings compared with MI(majority gates and inverters) based designs. 1 dimensional cellular automaton helps in improving stream cipher by generating pseudo random sequence for stream cipher. We also discussed basic ingredients of cellular systems, its definition, game of life and various classification of cellular automata and how and where it is used in cryptography. In the end we understood the application of 2 dimensional automata ie how to improve the quality of gray-scale, colored, and monochrome pictures. Image border detection and filtering methods in digital images have been discussed.

References:

1) Wang, S., Cai, L., & Guo, L. (2005). A Novel Full Adder Implementation Using Quantum Cellular Automata. RESEARCH AND PROGRESS OF SSE, 25(2), 148.
2) Cho, H., & Swartzlander, E. E. (2007). Adder designs and analyses for quantum-dot cellular automata. IEEE Transactions on Nanotechnology, 6(3), 374-383.
3) Wolfram, S. (1986). Random sequence generation by cellular automata. Advances in applied mathematics, 7(2), 123-169.
4) Wolfram, S. (1985). Origins of randomness in physical systems. Physical Review Letters, 55(5), 449.
5) Nordlund, K. (2006). Basics of Monte Carlo simulations. Lecture Notes, University of Helsinki.
6) Lim, J. S. (1990). Two-dimensional signal and image processing. Englewood Cliffs.