IJCSN International Journal of Computer Science and Network, Volume 5, Issue 1, February 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Cryptography Using Three-Dimensional Cellular Automata (3-D CA)

[1] Dr. Abdulwasea M. Obaid Alezzani, [2] Hilal Mohammed Yousif Al-Bayatti (Ph. D)

[1] Computer Science Department, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Republic of Yemen.

[2] Computer Science Department, Applied Science University, Kingdom of Bahrain

Abstract - **A cellular automaton (CA) has several characterizations. Recently it has become a target for many researchers. For this reason, A CA is applied in many fields: building, modeling, computer applications and simulation of several natural systems. CA characteristics refer to building the mathematical in a CA construction. Thereby, these have given CA an advanced possibility to be applied in wide domains. Cryptography is important in the security domain to reserve the citizen and military information from unauthorized disclosing and modification. Therefore, this paper presents a new block cryptosystem by using three-dimensional cellular automata (3-D CA), whereas the block of data fill a 3-D CA cells. An updating process of cells values of 3-D CA is based upon the neighbor cells and the selected rules that will be applied in the calculating of the next state for CA.**

Keywords - *Cellular Automata, Cryptography, Pseudorandom Number Generators.*

1. Introduction

Since early times till now, humans has a concern on how to protect their data from an unauthentication person. Therefore, several algorithms and techniques are presented to this reason. A cryptosystem plays an essential role to maintain confidentiality, integrity, and availability of data. The digital era development, the power of the computation devices helps the encryption algorithms develop the ability to design a complex encryption algorithm. A cryptanalyst develops a new technique to break new encryption algorithms by exploiting the power of the computation devices.

The rise of communication and information technology development leads to growth and an increase of data transmission via communication networks. Therefore, many problems of security threats of data occur during its transmission by intruders.

1.1 Cellular automata (CA)

A cellular automata (CA) is a finite array of cells, where each cell can store a bit of information. The collections of values of the cells constitute the global state of the CA, whereas the state of the cell is called a local state. The CA evolves globally in discrete time steps, with the state of each cell changing at each time step [1].

A CA can be represented in one, two, and three-dimensional arrays. The value of the next state of the cell in CA depends on the number of cells that share in the computing of this cell state. The numbers of the cell neighbors are based on the radius of the cell. Therefore, a cellular space has several characteristics that are presented in [2]. Such features arise the cryptography-based as important domain which is used in building a secured cryptosystem. It increases the effort of a cryptanalysts of the cryptosystem to break it, where a cryptanalyst needs to search through a possible initial configuration, possible rules, and a boundary configuration of a CA.

The major motivation of this paper is to provide an interest in new tools for CA with a high security level for a cryptosystem. Hence, three-dimensional CA technique is used in this paper. Both reversible and irreversible of 3-D CA are suggested and can be used to building and designing a new cryptosystem.

2. Concepts of Cryptography and CA

Secret writing was probably the first technique for secure communication via secure channel. The ciphertext was invisible or unreadable to an unsuspicious reader. This technique depends on the degree of the security level of the encryption algorithm that used to encrypt a sensitive data.

A cryptographer attempts to build or design a powerful cryptosystem to conceal sensitive data from an unauthorized access, where a cryptanalyst attempts to analysis and break this cryptosystem disclosure sensitive data.

The scope of cryptology has increased dramatically. It is now seen as the field that provides the theory and practical guide for the design and analysis of cryptographic tools which then can be used to build up complex secure services. The secrecy part of the field, traditionally concentrated around the design of new encryption algorithms, was enriched by the addition of authentication, cryptographic hashing, digital signature and secret sharing schemes [3].

2.1 Cryptography

Cryptography (from Greek kryptós, "hidden", and gráphein, "to write") is the study of the principles and techniques by which information can be concealed in a garbled version that is much more difficult to read for an unauthorized. Most cryptosystems are used two techniques a *substitution* and *transposition (permutation)*. The goal of substitution and transposition is *confusion* and *diffusion* respectively. The main use of cryptography is to reserve the most security requirements such as confidentiality, integrity, and availability [4,5]. A cryptosystem can be divided into two types a secret-key and public-key cryptosystems. The secret-key cryptosystem uses one key to encryption and decryption. It has a high performance and it is used to encrypt a data files. There are several algorithms such as DES, AES, one-time pad, and etc. The main problem in symmetric cryptosystem is getting the sender and receiver to agree on the secret-key. If they are in separate locations, they must use some kind of communication medium to prevent the disclosure of the secret key.

The public-key cryptosystem uses two keys, a public key to encryption (decryption) and a private key to decryption (encryption), so each user has two keys public key and private key. It is slower than a secret-key cryptosystems, then it is used to a transmission keys between parties. Public key cryptosystems ensure secret key between communicating parties without the need to distribute secret keys. Olu Lafe presented desirable properties to construct and design cryptosystem that has a high level-security [6].

2.2 Cellular Automata

The concept of CA started in 1948 by von Neumann. After that, CA has been developed by many studies and used in several applications [7].

Definition: *Cellular Automata (CA)* are dynamic systems in which space and time are discrete. The cells are arranged in the form of a regular lattice structure and each must have a finite number of states. These states are updated synchronously according to a specific local rule of interaction. The state of each cell in the next state of CA depends only on the state of neighboring cells in the previous state of CA and the cell itself [6,8].

Definition [9]: A CA is a quadruple A= (*d, S, N, f*), where;

d: is a positive integer indicates the dimension of A.

S: is a finite state set.

N: is a neighborhood vector N=(c_1, c_2, …., c_n) of n different elements of Z^d and f is the local rule of the CA presented as ; f: $S_n \rightarrow S$.

The local rule f gives the new state of a cell from the old state of its neighbors. A configuration of a CA A=(*d, S, N, f*) is a function $\boldsymbol{c}$: $\boldsymbol{Z^d \rightarrow S}$ that assigns state to all cells.

Cellular Automata Representation

CA can be represented in one, two or higher–dimensions; these organizations are allowed to moderate the CA state easily. One–dimensional CA consists of a line of cells. Two-dimensional CA is represented as a two-dimensional array (square) of cells. Three-dimensional CA are represented as a cube in three axes x, y, z, whereas this organization represents a three-dimensional matrix, where x represents the horizontal–axis, y represents the vertical–axis and z represents the axis of the grid [10].

Cell state can be (0 or 1) in terms of binary representation or k-states (0, 1, 2, …, k-1) in terms of decimal representation. Each of which updated depends on ***neighbor cells***. The neighborhood of a cell is typically based on the cell itself and all immediately adjacent cells or some adjacent cells. The values at each cell are updated synchronously are based on the values of the neighborhood at the preceding time step, and according to definite set of "local rules".

The function formula that used to update one-dimensional array as the following equation:

$$c_i^{t+1} = f(c_{i-r}^t, c_{i-r+1}^t, ..., c_i^t, c_{i+1}^t, ..., c_{i+r}^t) \quad (1)$$

Where:

t: represent a time-step;

r: represent a radius of the rule;

c_i^t : represent the state of the cell c_i at time ***t***; and

c_i^{t+1} : represent a new state of cell c_i at time ***t+1***.

In two-dimensional array; the function formula that is used to update two-dimensional array as in the following equation:

$$c_{ij}^{t+1} = f(c_{i-1,j-1}^{t}, c_{i-1,j}^{t},..., c_{i+1,j+1}^{t}) \quad (2)$$

In three-dimensional array; Neighborhood of CA can be divided into six neighbors and 27-neighbor as well as the cell itself. The function formula that is used to update three-dimensional array as in the following equation:

$$c_{ijk}^{t+1} = f(c_{i-r,j-r,k-r}^{t}, c_{i-r,j-r,k-r+1}^{t},..., c_{i+r,j+r,k+r}^{t}) \quad (3)$$

Where; if ***r =1*** and the values of cells in binary case, the number of neighbors that share in the next time-step (the next state of the cell) of any cell in CA is:

- $(2r+1)^1$ in one-dimensional CA.
- $(2r+1)^2$ in two-dimensional CA.
- $(2r+1)^3$ in three-dimensional CA.

In general, the number of neighbors that used to update cells of CA is: $(2r+1)^d$ (4)

Where;
r: represents a radius of the CA, and
d: is dimension of CA.

In CA, there are two types of rules; these types are:

- ***Irreversible Rules***: An irreversible rule operates forward to updating CA.
- ***Reversible rules***: Reversible CA rules mean that: if the rule updating CA in forward, another rule will exist in rule space to operate backwards on CA to obtain the original CA.

When update a CA, the CA resulted is:

- ***Uniform CA***: when a CA is updating by a one rule, or
- ***Non-uniform CA***: when a CA is updating by a two or more rules.

There are two reasons for the construct efforts of the cryptosystems based on CA [11]:

i. CA is a simple model that can generate pseudorandom patterns.
ii. CA can be efficiently implemented by hardware.

3. Cryptosystems with CA (Previous Works)

One version of this idea is presented by S. Wolfram [12] who employs cellular automaton (rule 30) to generate temporal sequences which have a high degree of randomness. The secret key is the initial state of the system. Reversible CA may be particularly valuable in public-key encryption. Kari [13] proposed a system in which the public key is a cellular automaton inverse to the private key cellular automaton. The security of public-key cryptosystems depends on the difficulty of finding the private key given knowledge of the public key and/or chosen plain and ciphertext. Quality of randomness has been evaluated, it has been established that the patterns generated by maximal length CA's meet all the criteria and the quality of randomness of the pattern generated by CA's is significantly better than that of Linear Feedback Shift Register (LFSR) based structure [14]. Nandi et al.[15] used non-uniform CAs with two rules 90 and 150, and it was found that the quality of generated PNSs was better than the quality of the Wolfram system. The system proposed by Gutowitz et. al. [16] uses both forward and inverse iteration of a dynamical system. The very significant difference here is that the dynamical system used by Habutsu et al. is irreversible. An irreversible system is one in which some states have none, or more than one, antecedent state. A very simple such map is the tent map.

Sheng-Uei Guan and Shu Zhang [17], proposed a novel CA-dynamical system. A block cipher and key stream generator based on that novel CA were introduced. Lafe [6,18], proposed to use one-dimensional CA transforms for data compression and encryption, where the transformations can be obtained from basic basis functions. The basis functions are related to evolving the states of the CA. Jesůs Urias, et al. [19], introduced a cryptosystem based on CA, where the mechanism based on synchronization in CA is presented. They provide two primitives system, the pseudorandom generator of keys and the indexed families of permutation. Chunren Lai [20], introduced CA based block cipher algorithm (CA256-2) which was designed to provide the high-speed encryption/decryption. Two-dimensional CA used for design hash function to provide the digital signature and serve as "check-sums" for error detection/correction. He used four transformations with four cycle length to encryption and decryption message.

Tomassini and Sipper [21], show that a two-dimensional non-uniform CA provides high quality PNSs. They use cellular programming to evolve the rules of CA. Tomassini and Perrenoud [22], propose using non-uniform, 1D CAs with r =1 and four rules 90, 105, 150 and 165, which provide high quality PNSs and a huge space of possible secret keys which are difficult for cryptanalysis. Instead of designing rules for CAs, they use evolutionary technique called cellular programming (CP) to search for them. Tomassini and Perrenoud [23], described a single key cryptographic system based on one- and two-

dimensional non-uniform CA randomizers obtained by artificial evolution (cellular programming). Sammer [24] introduced CA based key stream generator, where he used two-dimensional CA which were used for this purpose. Two-dimensional cellular automat is significantly better than linear feedback shift register (LFSR). Sen, Shaw, D. R. Chowdhri, Ganguly, and P. P. Chaudhuri [25] introduced one-dimensional CA based a secret key cryptosystem (CA cryptosystem (CAC)) for block cipher, two CA (CA) are used, one is called Minor CA, the other is called major CA. The minor CA is used to transform a secret key into a secret state S_N, which controls the four transforms of the CAC, namely T_1,T_2, T_3 and T_4. The CAC is analyzed by Feng Bao [11], show that the system is insecure. It can be broken by chosen-plaintext attack.

Finally Seredynski, Bouvery and Zomaya [26,27], consider Vernam cipher and used it in CA-based secret key cryptosystem, they used finite 1-D non-uniform CAs. However, they extend the potential space of rules by consideration of two sizes of rule neighborhood, namely neighborhood of radius r = 1, 2. The interested researchers in CA field are increasing because a CA has a huge search space [6].

4. Three-dimensional Cellular Automata (3-D CA)

Our interest in a 3-D CA, not a 1-D or 2-D CA is not enough to building a secure cryptosystem. But 3-D CA additional characteristics are found attractive and motivating to study and search how these characteristics can be exploited and introduce a high-secure cryptosystem. Because, when a 3-D CA is used in cryptography, the task of the intruder will become difficult to analyze and infer a cryptosystem with 3-D CA to obtain the original text.
In this section, 3-D CA characteristics that will be exploited in designing a new cryptosystem will be presented. In addition, a 3-D CA behavior, and its space that illustrate a computation difficulties without knowing the characteristics of a CA used in cryptosystem.

4.1 3-D CA characteristics

A 3-D CA states updating is depending on the cell itself and on the neighbor cells. For updating CA, using one rule or a group and functions that used will take the following formula:

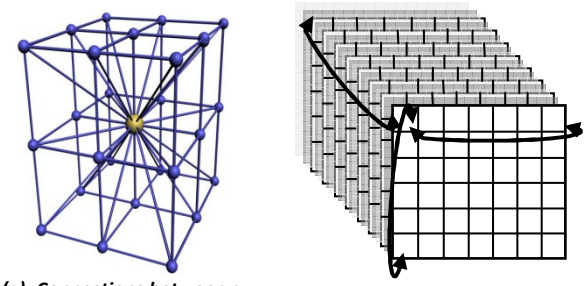
$$c_{ijk}^{t+1} = f(c_{i-r,j-r,k-r}^{t}, c_{i-r,j-r,k-r+1}^{t}, ..., c_{i+r,j+r,k+r}^{t})$$

Whereas, c_{ijk}^{t} , represents the current state and c_{ijk}^{t+1} , represents the new state and ***r***, represents the radius of the applied rule.

For instance, if ***r***=1, then the cell is the same and the adjacent cells will be distributed upon 3-adjacent sub matrix, its dimensions are ***(2r+1)*(2r+1)*(2r +1)***. The no. of neighbors' cells that used to update the current value of any cell is 27-cell with a cell itself.

In this case (27-cell neighbors), the connections between neighbors have a high density for updating one-cell of CA and the computation becomes more complicated. The search space of the rules in this case will be very large, where the numbers of rules are $2^{2^{27}}$ in binary case.

During the updating process of three-dimensional CA, then the ***periodic (cyclic) boundary*** to three-dimensional CA will be applied. When calculating the rule value of the extreme cells, then the extreme planes will be adjacent with each other, that is to say plan 0 and Plane n-1, are adjacent, concerning the z-axis of the grid, but for index x- and y-axis, then the index 0 and n-1, will be adjacent. Figure (1) illustrates the connections between any cell and its cell neighbors, and the periodic boundary of 3-D CA.



(a): Connections between a Cell and its Neighbors; ***(b): Periodic Boundary***

Figure 1: the connections between any cell and its neighbors, and the periodic boundary of 3-D CA

In figure (1), it is clear that three-dimensional CA is classified upon slide, whereas its number equals to the z-axis of the grid, the slide represents the plane, therefore, calculating the rule value is based upon the adjacent cells and these cells are distributed upon the planes.

4.2 3-D CA Space

Tree-dimensional CA distributes their cells and associate finite automata over a section of $\boldsymbol{R^3}$, where the form of any rules takes the form:

$\boldsymbol{f: R^3 \rightarrow \{0,1\}}$ in binary case, or
$\boldsymbol{f: R^3 \rightarrow \{0,1,2,\ldots, k\text{-}1\}}$ in ***k***-state.

To evolve a *K*-state, *m*-neighbor, *LMN*-cell, and *T* discrete time steps; then we find:

i. K^{K^m} the total of possible rules to update CA;

ii. K^{L+M+N} the different patterns of initial configurations;

iii. $K^{d(L+M+N+T)}$ the number of boundary configuration patterns; and

iv. $K^{K^m+(2^d-1)(L+M+N)+dT)}$ The number of ways to evolve CA.

Where *d* is the dimension of CA.

4.3 3-D CA Behavior

Behavior of CA depends on the rules that applied to update cells of CA. A rule of CA depends on the number of neighbors which can be used for updating the cells of CA. Neighboring numbers in three-dimensional CA can choose six neighbors or greater than six upon to 26 neighbors and a cell itself.

The simplest neighborhood of three-dimensional CA is the Alfonseca and Ortega [28] type consisting the node and its six closest neighbors. There are many conflicts to determine the behavior of three-dimensional CA. To know a behavior 3-D CA, you can back to the Wolfram representation [29]. Then, the behavior of 3-D CA can't be representing it by using a paper and pen to draw the different figures in different time steps.

5. A Cryptosystem with 3-D CA

A three-dimensional CA have a very useful feature due to their inherent computational complexity. With the rich set options, it is possible to devise rules for birth and survival with up to 26 neighboring cells. The simulation can start from one point in three-dimensional space of a random set of points with a boundary cube. A cellular programming technique to choice a 3-D CA rules will be used [10].

A 3-D CA space needs to a huge search to select rules that will introduce high-quality pseudo-randomness.The selected rules will be used in new cryptosystem to updating the states of a 3-D CA cells in discrete time steps. The major interest to use a 3-D CA with cryptography is the characteristics of the 3-D CA. these characteristics are as follows:

- Number of neighbors that used by rules during update each cell in CA,
- Number of rules that are used to updating CA cell values,
- Number of initial configurations that are used as key,
- Number of boundary configuration patterns that result during each time step,
- Number of ways to evolve CA,
- Number of time steps that represent cycles to update CA,
- A CA can updated by using a non-uniform and uniform rules,
- A periodic boundary condition can be implemented to update a cells extreme, and also
- Can not simulate a 3-D CA to implement it using 3-D machines to cryptanalysis a ciphertext.

5.1 The design Elements of a New Cryptosystem

The characteristics of 3-D CA play the basic role to introduce a cryptosystem with non-uniform 3-D CA. the cryptosystem that will be designed is a symmetric block cryptosystem. The key of the cryptosystem formed the random initial states that resulted from applying a non-uniform rules, and the rules that are used to update the states of the cells of CA. The design elements of this cryptosystem are:

1. Block size: the block size of the plaintext is equal to the dimensions of 3-D CA, where the value of each cell equal to one byte.
2. Key size: the key size is equal to the block size of the plaintext.
3. The number and order of a selected non-uniform rules set that are used to update a 3-D CA cells.
4. Number of time steps: the number of time-step is ***n*** time steps that represent the cycle's number to forward update the cells values of 3-D CA1. During these cycles, the substitution is obtained from applying a non-uniform rules set used to update a 3-D CA cells to produce a high confusion technique in the ciphertext result.
5. Generate a sub-key: in each cycle, a new sub-key is used to add/combine with a block of data.
6. A permutation concept is applied on the plaintext n-time to permute a 3-D CA cells values to obtain a diffusion technique in the plaintext.

5.2 A New Cryptosystem Design

In this cryptosystem, a two three-dimensional CA, are represented in two three-dimensional matrices and their dimensions are equal. One CA (3-D CA2) non invertible CA, will take the initial state (random numbers), that

represents the secret key to the system, and other invertible CA (3-D Inv. CA1) will be filled with block of plaintext. Each cell in this system will store an information byte or bit. An ***encryption process*** of a cryptosystem will be implemented on message (plaintext) as following steps:

1. The entire plaintext is divided into blocks, each block size is equal to a 3-D CA1 dimensions (***LMN***);
2. apply a non-uniform rules that selected to update a 3-D CA2 cells that represent a key to generate a sub-key;
3. Add sub-key to a plaintext block or combine a plaintext block with sub-key using XOR.
4. apply a non-uniform rules that selected to update a 3-D CA1 cells to ***3***-time steps;
5. Apply a permutation.
6. repeat step from 2 to 5 for ***n*** cycles;
7. The result is ciphetext block.

Figure (2) illustrates the operations of the encryption process.

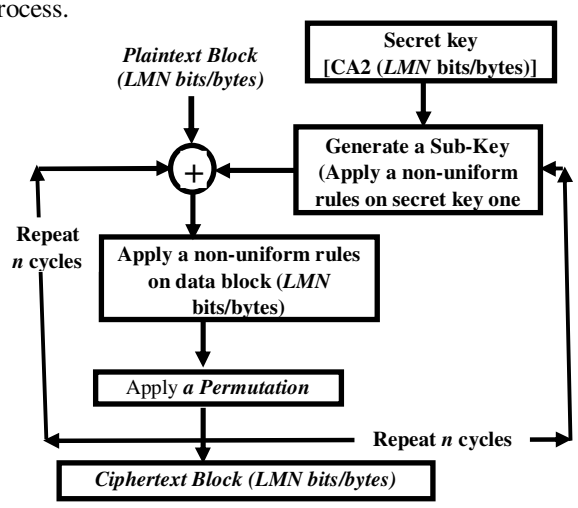


Figure 2: a new cryptosystem using 3-D CA

The ciphertext that results from this cryptosystem has the following characteristics:

- A voidance from the floating-point operations.
- Can be implemented by software/hardware in efficiently.
- Fast implementation.
- The ciphertext that result from the cryptosystem operations passes the statistical tests.
- A cryptosystem is an implementation on the decimal system.
- Number of neighbors that is used by rules during updates each cell in CA; the no. of neighbors is 27.
- Number of rules that is used to updating CA, the attacker will face difficulty to determine the rules that is used to update cells values of 3-D CA1. The no. of rules is very large in addition to the order of the selected rules. Where the no. of rules is equal to $256^{256^{27}}$.
- Number of initial configurations that is used as key, the length of the key is LMN bytes. The attacker who attempts to obtain the key of this cryptosystem will face difficulty. Where the possible no. of the attempts to obtain the key is equal to 256^{L+M+N}.
- Number of a ways to evolve CA, the no. of the a ways to evolve a 3-DCA is $256^{256^{27}+(2^d-1)(L+M+N)+17d}$, and addition to:
- Number of time steps that represent cycles to update CA,
- A 3-D CA cells are updated by using a non-uniform rules,
- A periodic boundary condition can be implemented to update a cells extreme, and also
- Can't simulate a 3-D CA to implement it using a 3-D machine to cryptanalysis a ciphertext result.

A ***decryption process*** of the cryptosystem is an inverse of encryption process, where the steps of the decryption process are follows:

1. The entire ciphertext is divided into blocks, each block size is equal to a 3-D CA1 dimensions (***LMN***);
2. Apply a permutation.
3. apply a non-uniform rules that selected to update a 3-D CA1 cells to ***3***-time steps;
4. Apply a permutation.
5. apply a non-uniform rules that selected to update a 3-D CA2 cells that represent a key to generate a sub-key;
6. Add sub-key to a plaintext block or combine a plaintext block with sub-key using XOR.

7. repeat step from 2 to 5 for ***n*** cycles;
8. The result is plaintext block.

6. Cryptanalysis of the Cryptosystem

In this section we discuss the security of a new designed cryptosystem. When a cryptanalyst attempts to analyze this cryptosystem he/she faces many difficulties. The ciphertext that result from the cryptosystem operations passes the statistical tests, that means the cryptanalyst cannot obtain a relationship between a ciphertext and key. A cryptanalyst cannot simulate the cryptosystem with three-dimension hardware to cryptanalysis a ciphertext.
The ciphertext that results from this cryptosystem is immunity to a brute-force attack. Because a brute-force cryptanalyst task is impossible, so that he/she needs to search in huge space of number of neighbors, the no. of rules that is equal to $256^{256^{27}}$, the possible no. of the key that is equal to 256^{L+M+N}, the no. of the a ways to evolve a 3-DCA is $256^{256^{27}+(2^d-1)(L+M+N)+17^d)}$, and a number of time steps that represent cycles to update a bytes information of 3-D CA.

A new cryptosystem is immunity to a differential cryptanalyst. Because it uses the concepts of permutation and substitution alternately during encryption each block of data. A permutation operation produces diffusion technique that dissipates statistical structure of plaintext over bulk of ciphertext. A substitution operation produces the confusion technique that makes a relationship between ciphertext and key as complex as possible. Then, a cryptanalyst task is complex to obtain an original plaintext or infer a key or both.

Finally, a new cryptosystem is immunity to malicious insertions or modification, because a cryptanalyst cannot expect the change results on the ciphertext. A cryptosystem have an avalanche effect, where any attempt to change one bit will have an effect on all block ciphertext.

7. Conclusion

A new cryptosystem that presented in this paper is designed by using a non - uniform of 3-D CA. This cryptosystem implement two primitive cryptographic techniques. These are confusion and diffusion to conceal the relationship between the key and ciphertext and the characteristics of the plaintext language. A cryptosystem is immune to a various of a cryptanalysis methods and performs an encryption and decryption operations in efficiency that referred to its absence from floating point operations. A block length and key size of the cryptosystem are 256-byte/bit, 512-byte/bit, or more, and it can produces a multiple ciphertext for one plaintext when change one byte/bit in key value or in ordering of the used rules. Finally, cryptanalyst faces many difficulties to deduce the key or plaintext from ciphertext, where he cannot expect the behavior of 3-D CA, needs to search in huge search space to discover a possible set of rules, initial key, a discrete time-step, initial configuration, and boundary condition.

References

[1] P. Sarkar, S. Maitra "*Efficient Implementation of "Large" Stream Cipher Systems*", 2001.
[2] E. F. Codd, "*Cellular Automata*", Academic Press, Inc. New York and London 1968.
[3] M. J. B. Robshaw, "*Stream Ciphers*", RSA Laboratories Technical Report Tr-701, Version 2.0-July 25, 1995.
[4] B. Schneier, "Applied Cryptography", Jhon Wiley and Sons Inc., second Edition, 1997.
[5] Peter Gutmann, "*Cryptography and Data Security*", University of Auckland.
[6] Olu Lafe, "*Cellular Automata Transforms, Theory and Applications in Multimedia Compression, Encryption, and Modeling*", Kluwer Academic Publishers, 2000.
[7] P. P. Chaudhuri, D. R. Chowdhry, S. Nandi, and S. Chattopadhay,"*Additive Cellular Automata, Theory and Applications*", Volume I, IEEE Computer Society, 1997.
[8] Tim Tyler, "Cellular Automata", http://cell-auto.com/largeinverse.
[9] http://www.alife.co.uk/ca
[10] A. M. Alazzani, "*a proposed block cipher system Based on Three-Dimensional Cellular Automata*", PhD thesis in Computer Science, Informatics Institute for Postgraduate studies, University of Technology, 2004.
[11] Feng Bao, "*Cryptanalysis of A New Cellular Automata Cryptosystem*", Institute for Information Research, Sengapore, 2002.
[12] S. Wolfram, "*Cryptography With Cellular Automata*", Institute for Advanced study, 1985.
[13] J. Kari, "*Cryptosystem Based on Reversible Cellular Automata*", Mathematics Department, University of Turku, Finland, April 16, 1992.
[14] S. Nandi, B. K. Kar, and P. P. Chadhuri,"*Theory and Applications of Cellular Automata in Cryptography*", IEEE Transaction on Computers, Vol.43, No. 12, December 1994.
[15] S. Nandi, B. K. Kar, and P. P. Chadhuri,"*Theory and Applications of Cellular Automata in Cryptography*", IEEE Transaction on Computers, Vol.43, No. 12, December 1994.
[16] H. Gutowitz, "*Cryptography With Dynamical Sytems*", ESPCI,Laboratoire d'Electronque, Paris, France, 1995.
[17] Sheng-Uei Guan and Shu Zhang,"An *Encryption Method Based on Dynamical Cellular Automata*", Department of Electrical Engineering, National University of Singapore, 2000.

[18] Olu Lafe, "*Data Compersion And Encryption Using Cellular Automata Transforms*", Lafe Technologies,USA, 1997.

[19] J. Urias, E. Ugalde, and G. Salazar, "*A Cryptosystem Based on Cellular Automata*", Mexico, 14 September 1998.

[20] Chunren Lai, "*High-Spead Cellular–Automata Based Block Cipher and Fault Tolerant Public-Key Cryptosystems*", M. Sc. thesis, Department of Computer Science, University of Regina 2000.

[21] M. Tomassini, M. Sipper, and M. Perrenoud "*On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata*", IEEE Trans. on Computers, v. 49, No. 10, October 2000, pp. 1140-1151.

[22] M. Tomassini and M. Perrenoud, "*Stream Ciphers with One- and Two-Dimensional Cellular Automata*", in M. Schoenauer at al. (Eds.) Parallel Problem Solving from Nature - PPSN VI, LNCS 1917, Springer, (2000) 722-731.

[23] M. Tomassini and M. Perrenoud, "*Cryptography With Cellular Automata*", Institute of Computer Science, University of Lausanne, 1015 Lausanne, Switzerland, 4 July 2001.

[24] S. S. Essa."*Key Stream Generation Using Cellular Automata*", M.Sc. thesis, Department of Computer Science and Information Systems, University of Technology, 2001.

[25] S. Sen, C. Shaw, D. R. Chowdhuri, N. Ganguly, and P. P. Chaudhuri," *Cellular Automata Based Cryptosystem (CAC)*", Computer Center, Calcutta, Indian, 2000.

[26] F. Seredynski, P. Bouvery, and A. Y. Zayama, "*Secret Key Cryptography with Cellular Automata*", in IPDPS'03/NIDISC, Nice (France), April 2003.

[27] F. Seredynski, P. Bouvery, and A. Y. Zayama, "*Cellular Programming and Symmetric Key Cryptography Systems*", GECCO conference, Published by Springer in LNCS, Chicago, USA, July 2003.

[28] M. Alfoseca and A. Ortegaa, "*Representation of some Cellular Automata by Means of Equivalent L Systems*", Madrid, Spain, 2000.

[29] S. Wolfram, "*A New Kind Of Science*", Wolfram Media Inc., 2002.

Authors Profile

Dr. Abdulwasea M. Obaid Alezzani graduated in Mathematics and computer, college of science, Sana'a University in 1994, MSc in Computer Science at Technology University in 2001, and PhD in Computer Science at Technology University in 2004. Vice Dean of computer center, Sana'a University from December 2006 to September 2007. Vice Dean of the Faculty of Computer & Information Technology (FCIT) for the Academic Affairs & Higher Studies, Student Affairs, and computer center at Sana'a University, from 22 Sep. 2007 to 29 Jan. 2010. Head of Quality Assurance Unit at the FCIT at Sana'a University, July 2008 to Jan. 2010. Vice Dean of the FCIT for the Student Affairs, from 30 Jan. 2010 to 22 May 2012. Head of Quality Assurance Unit at FCIT at Sana'a University, June 2014 to Jan. 2016. Currently, vice manager of Computer Center at Sana'a University from 23 Jan. 2016 till now. I am teaching a graduate and MSc postgraduate programs in Computer Science at FCIT. He has published three papers, the research interests lie in computer science, computer and information security. He has association with Professor Hilal Mohammed Yousif Al-Bayatti, Professor Ghaleb H. Al-Gaphari, and associate Professor Sharaf A. Alhomdy.

Professor Hilal Mohammed Yousif Al-Bayatti graduated in Mathematics-college of science, Baghdad University in 1970, MSc in Computer Science at University College London, University of London in 1977, and PhD in Computer Science at Loughborough University of Technology in 1986. Professor Al-Bayatti promoted to professor in 1998. He joined Applied Science University as Vice President for Academic Affairs and Development in 2007, and as Advisor to VP Academic and Development since September 2015 till now. He has published over 50 scientific papers and book chapters. Professor Al-Bayatti acted as a peer reviewer, and a member of editorial boards of many scientific journals. Professor Al-Bayatti supervised over 60 PhD/MSc students to completion. As an academic, professor Al-Bayatti research interests lie in computer science, computer and information security.