International Journal of Communication Networks and Security

Volume 1 | Issue 1 Article 5

2011

Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography

Sambhu Prasad Panda
C V Raman Computer Academy, Bidyanagar, Mahura, Janla Bhubaneswar-752054, Orissa, India,
sambhu.prasad.panda@gmail.com

Madhusmita Sahu
C V Raman Computer Academy, Bidyanagar, Mahura, Janla Bhubaneswar-752054, Orissa, India,
madhu_sahu@yahoo.com

Umesh Prasad Rout
C V Raman Computer Academy, Bidyanagar, Mahura, Janla Bhubaneswar-752054, Orissa, India,
umesh.upr@gmail.com

Surendra Kumar Nanda
C V Raman Computer Academy, Bidyanagar, Mahura, Janla Bhubaneswar-752054, Orissa, India,
situnanda@gmail.com

Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography

Sambhu Prasad Panda, Madhusmita Sahu, Umesh Prasad Rout, Surendra Kumar Nanda
Department of MCA
C V Raman Computer Academy, Bidyanagar, Mahura, Janla
Bhubaneswar-752054, Orissa, India
sambhu.prasad.panda@gmail.com, madhu_sahu@yahoo.com, umesh.upr@gmail.com, situnanda@gmail.com

Abstract—**In this paper we present a new encryption and decryption algorithm for block cipher based on the linear (periodic boundary-PB) and nonlinear cellular automata rules. First we apply non linear CA rules (complements) to both plain text and key. Then PB CA rule is applied to the above results separately followed by the XOR operation of above results. After that the result of XOR operation is fed to substitution box(S-box) and again PB CA rules are applied followed by S-Box. The decryption process is carried out just similar to that of encryption but in the reverse way. Both the process of encryption and decryption is performed for 8 number of rounds in order to avoid the dependency between the plain text and cipher text so that the our proposed algorithm is more secure than that of AES and DES algorithms.**

Keywords-Cryptography, cellular automata, substitution byte, linear, non linear, Periodic boundary, correlation immunity

I. INTRODUCTION

Cryptography is an important and vital application in security, defense, medical, business and many other application areas. The effective measure of a cryptosystem is how long it can be used to encrypt and decrypt messages without the 'key' being broken using cellular automata (CA) rules. A class of cellular automata (CA) based encryption algorithms presents a particular promising approach to cryptography, since the initial state of the CA is the key to the encryption, evolving a complex chaotic system from this 'initial state' which cannot be predicted.

The remainder of the paper is organized as follows. Section II introduces the concept of Boolean functions and cellular automata. In Section III, we discuss some works of cryptography applied to one dimensional and two dimensional cellular automata. Section IV, Section V and Section VI describe our new encryption and decryption algorithm by using cellular automata rules.

II. BACKGROUND

A. Boolean Function and its properties

Any Boolean Function f in n variables is defined as a map

$f:\{0,1\}^n \quad \{0,1\}$

There are 2^{2^n} Boolean functions out of which 2^n are linear Boolean functions and - 2^n are nonlinear Boolean functions.

The Boolean functions are classified into two categories

- Group of linear functions.
- Group of non-linear functions.

A boolean function f in n-variable is said to be linear if it satisfies the following linearity property: $f(x+y) = f(x) + f(y)$, where $x = (x_1, x_2, —, x_n)$ and $y = (y_1, y_2, —, y_n)$.

There are 2^n linear Boolean functions in n-variables. Those are

- The zero function $f(x_1, x_2, —, x_n) = 0$ is always a linear function and is termed as Rule 0.
- $f(x_1, x_2, —, x_n) = x_i$, (i= 1,2,3,—,n) are n-linear boolean functions which are termed as fundamental linear rules.
- The combinations of these n-linear functions taking some or all at a time, give rest of the 2^n-1 linear Boolean functions.

For n variables, there are Boolean functions, out of which there are 2^n linear Boolean functions and rest are non-linear Boolean functions.

B. Cryptographic criteria for Boolean functions

Balanced ness: A Boolean function must output zeroes and ones with the same probabilities.

Good non-linearity: The Boolean function must be at the sufficiently high distance from any affine function.

High algebraic degree: The Boolean function must be at high algebraic degree.

Good correlation-immunity (of order m): The output of Boolean function must be statistically independent of combination of any m inputs. A balance correlation-immunity of order m Boolean function is called m-resilient**.**

Simple implementation in hardware: Hardware implementation should be very simple.

A. Cellular Automata (CA)

A Cellular Automata (CA) is defined by the 4 tuple: (D, S,N,R)
Where, D is the dimension of CA
S is the set of the finite states
N is the neighborhood vector=(x_1, x2, x3, x4,……..,x_n)
R is the set of local rules.

This is an idealized parallel processing machine, which is an array (1-D, 2-D, 3-D or nD) of numbers or symbols called cell values together with an updating rule. A cell value is updated based on this updating rule, which involves the cell value as well as other cell values in a particular neighborhood.

B. Neighbourhood

If we consider d-dimensional grid it is possible to define different kinds of neighbourhood. In particular if we consider two-dimenson CA then the most common neighbourhoods are :

1. VonNeumann:Only North, South, West and East neighbourhood.(Four neighbourhoods)
2. Moore: One adds the diagonals to Von Neumann to form nine neighbourhoods.
3. Extended Moore: One extends the distance of neighborhood beyond one.

Figure 1 shows the structure of two dimensional cellular automata neighborhood cells respectively. In both of these figures, central cell is denoted by CELL and all of it's 9 neighbourhood are denoted by N.

N	N	N
N	CELL	N
N	N	N

Figure 1: 2D Moore neighborhood

A. Two-dimensional cellular automata

Two-dimensional cellular automaton consists of an infinite (or finite) grid of cells, each in one of a finite number of states. Time is discrete and the state of a cell at time t is a function of the states of its neighbors at time t-1.For two-dimensonal cellular automata two types of cellular neighbourhoods are usually considered .In Von Neumann neighbourhood five cells are considered. That is Only North, South, East, West, and itself. In Moore neighborhood nine cells are considered (as shown in figure 1).

B. 2D CA rules as Boolean functions

Table 1 shows all the rules of two dimensional cellular automata.

64	128	256
32	1	2
16	8	4

Table I: 8-neighborhood CA rules

In 2-D eight neighborhood CA the next state of a particular cell is affected by the current state of itself and eight cells in its nearest neighborhood (Table 1). Such dependencies are accounted by various rules. The central cell represents the current cell (i.e. the cell being considered) and all other cells represent the eight neighbors of that cell. The number within each cell represents the rule number(i.e. Rule 1, Rule 2, Rule 4, Rule 8, Rule 16, Rule 32, Rule 64 and Rule 128) characterizing the dependency of the current cell on that particular neighbor only. These 8 rules are called fundamental rules of cellular automata and are known as linear rules of cellular automata. In case the cell has dependency on two or more neighboring cells, the rule number will be the arithmetic sum of the numbers of the relevant cells, which gives the linear rules of cellular automata. So XOR operation is also linear rule of CA.

For example the 2D CA rule 170 (=2+8+32+128) refers to the 4 neighborhood dependency of the central cell on right, bottom, left and top. The number of such rules is ${}^8C_0+{}^8C_1+....+{}^8C_8=256$.Rule-170 will be applied uniformly applied to each cell. From the following matrix (given below), it is clear that rule-170 is same as changing each cell by adding the states of its 4-orthogonal neighbors and the resultant matrix is:

0 0 1 0		1 1 1 0
1 0 1 1	Rule 170	1 1 0 0
1 1 0 1		0 1 1 1

A. Definitions

Null Boundary Cellular automata (NB CA): A null boundary CA is the one in which the extreme cells are connected to logic - 0 states.

Periodic boundary cellular automata (PB CA): A periodic boundary (PB) CA is the one in which the extreme cells are connected to each other.

Uniform Cellular Automata (UCA): A uniform cellular automata is the one in which same rules are applied to each cell.

Hybrid Cellular Automata (HCA): If different rules are applied to different cells , then we call it as hybrid cellular automata..

I. RELATED WORK

Carlet [1] performed study on Boolean functions for cryptography. He utilized cryptographic criteria to identify the linearity (diffusion) and nonlinearity (confusion) operations involved in Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithm. Wolfram [2] applied the one-dimensional cellular automata rules on stream cipher for security. Maitra et. al. [3] applied the method of generating key stream sequences for stream ciphers by combining the outputs of several linear feedback shift registers (LFSR) using a combined Boolean function. Das and Ray [7] present a new block encryption algorithm based on Reversible Programmable Cellular Automata theory. Their work ensures to generate 2^{256}

potential keys. They use 128 bit block size and Reversible Programmable Cellular Automata. Tripathy and Nandi [10] proposed a light weight symmetric key cryptosystem using CA, called Lightweight Cellular Automata-based Symmetric-key Encryption (LCASE). LCASE meets the same speciûcation as AES, that of satisfying the base security criteria (confusion and diffusion). They proposed a lightweight block cipher supports 128-bit block size with 128-, 192- and 256-bit keys, to conûrm with the Advanced Encryption Standard (AES) speciûcation. All these works were based on one dimensional and two dimensional cellular automata for stream and block cipher [9].

II. ENCRYPTION & DECRYPTION ALGORITHM USING CELLULAR AUTOMATA RULE

This algorithm contains substitution (non-linear cellular automata rule), permutation (linear cellular automata rule), complement (non-linear cellular automata rule), and XOR (linear cellular automata rule) operations. In crypto system, use of non-linear rule is more secure then use of linear rule. But creation of confusion (non linear CA rule) and diffusion(linear CA rule) operations are the two fundamental principles of cryptography .So in order to develop any encryption and decryption algorithm in cryptography we will apply both linear(diffusion) and non linear (confusion)operations or rules .But if we use more number of non linear rules and few linear rules for encryption and decryption then the algorithm will be more secure . In our encryption and decryption algorithm more number of non linear rules are applied as compared to Advanced Encryption Standard (AES) algorithm and also the number of rounds are less as compare to AES and hence our algorithm is more secure than that of AES algorithm. Figure 2 shows the encryption and decryption for eight number of rounds where as Figure 7 and Figure 9 show operations involved in one round encryption and one round decryption using cellular automata rules.

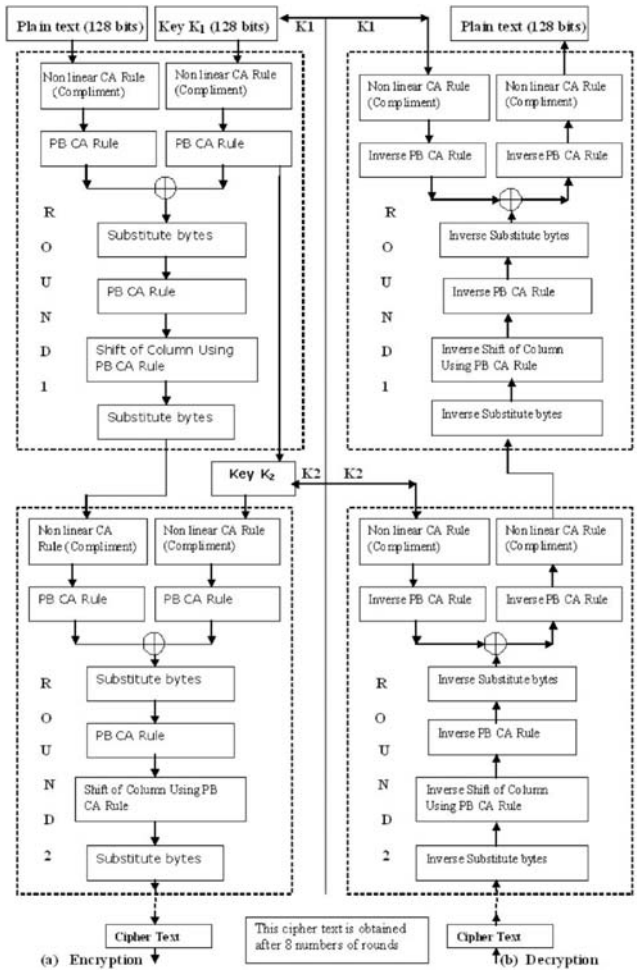

Figure 2: Encryption and Decryption algorithm applying CA rule

I. STEPS OF ENCRYPTION ALGORITHM

A. Non linear CA rule (Complement) and PB CA rule8

We take the length of the plain text as 128 bits and the length of key as 128 bits. First we convert the plain text as 4x4 matrix with each cell containing 1 bytes (= 8 bits). Now we apply non linear cellular automata rule (complement) to each bit of the plain texts. Similarly we write the 128-bits key in a 4x4 matrix and apply non linear CA rule (complement) to each cell of the key matrix. After the complementation we apply PB CA rule8 separately. Figure 3 shows the use of Periodic Boundary CA rule-8 to the matrix.

Figure 3: Periodic Boundary CA rule-8

For example, in the following matrix, the values in the second row have been shifted to first row, values in the third row have been shifted to second row and so on and values in the first row have been shifted to last row after applying periodic boundary (PB) CA rule-8 to each value in the cell of the matrix.

0	1	1	0	PB CA rule-8	1	0	1	0
1	0	1	0		1	0	0	0
1	0	0	0		0	1	1	0

B. XOR operation

XOR operation is applied between the resulted cipher key and cipher text providing the linear rule of cellular automata and hence providing the diffusion property of the cryptography.

C. Substitute Bytes Transformation(S-Box)
(Forward and Inverse Transformation)

The forward substitute byte transformation, called Sub Bytes, is a simple table lookup below. This table is same as AES table. In future we try to develop a S-box which is balanced, high non-linear, high algebraic degree. But AES S-box is balanced, non-linear, and high algebraic degree. AES defines a 16 x 16 matrix of byte values, called S-box that contains a permutation of all possible 256 8-bit values. Each individual byte of state is mapped into a new byte in the following way. The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value. For example, the hexadecimal value {95} references row 9, column 5 of the S-box, which contains the value {2A}. Accordingly, the value {95} is mapped into the value {2A}. Figure 4 shows an example of the Sub Bytes transformation. Figure 5 shows the general form of Substitute byte transformation.

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Figure 4: Sub Bytes transformation

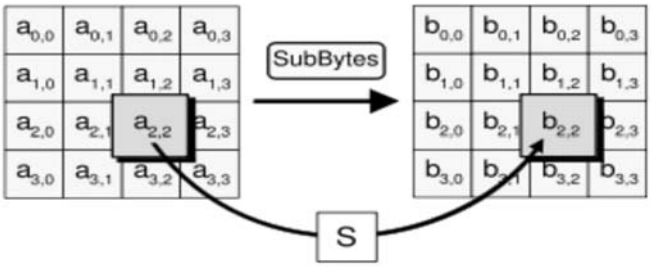

Figure 5: General form of Substitute byte transformation

D. PB CA rule128 and PB CA rule32

Now the output of S-Box is fed to PB CA rule128 and PB CA rule32 (Figure 6) consecutively so that permutation (transposition) operations are performed providing the linear rules of cellular automata and hence providing the diffusion property of cryptography.

For example, in the following matrix, applying the PB CA rule 128 to each cell of the matrix, the values in the first row have been shifted to second row, values in the second row have been shifted to third row and so on and values in the last row have been shifted to first row after applying periodic boundary (PB) CA rule-128 to each value in the cell of the matrix.

0	1	1	0	PB CA rule-128	0	1	1	0
1	0	0	0		0	1	1	0
0	1	1	0		1	0	0	0

For example, in the following matrix, applying PB CA rule 32 to each cell, the values in the first column have been shifted to second column, second column values have been shifted to third column and third column values have been shifted to first column, and so on.

1	1	0	1	PB CA rule-32	1	1	1	0
0	1	0	1		1	0	1	0
0	0	1	0		0	0	0	1

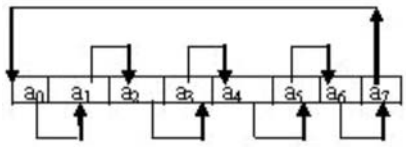

Figure 6:PB CA rule-32 on each cell of plaintext

E. Substitute Bytes Transformation(S-Box):

After the operation of PB CA rule128 and PB CA rule32, we fed the data to S-Box to get the final cipher text of original plain text

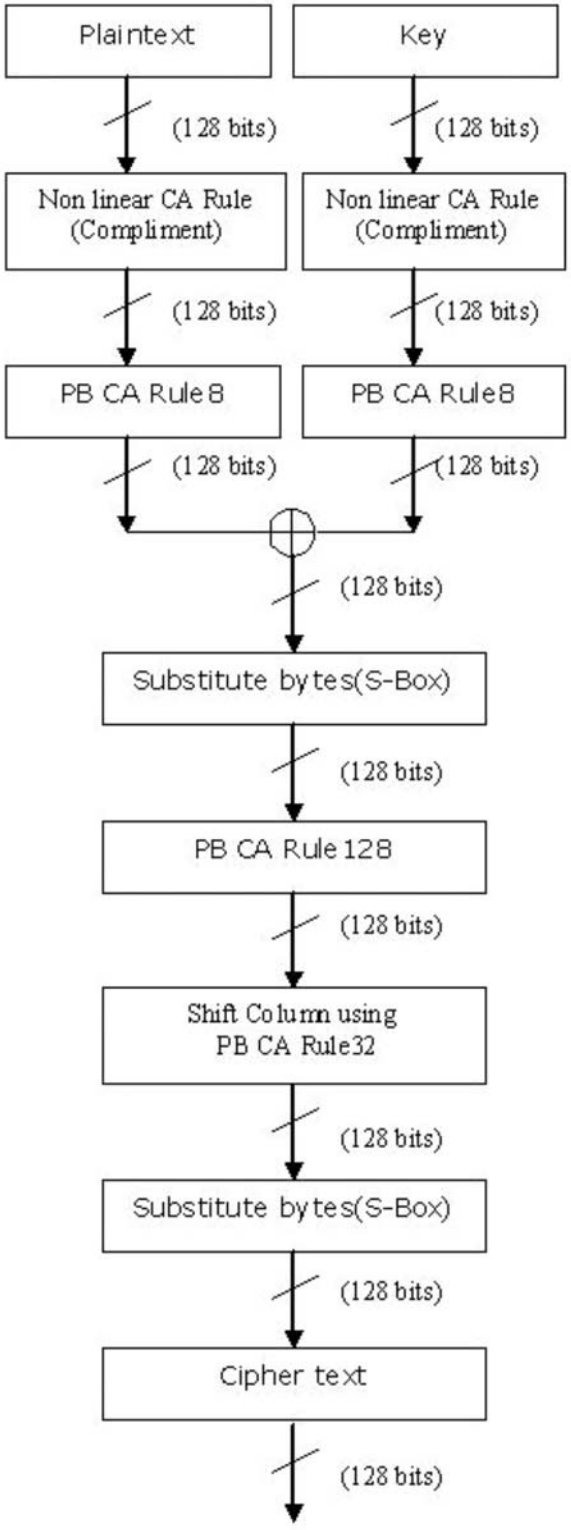

Figure 7: one-round of encryption algorithm applying CA rule

VI. DECRYPTION ALGORITHM

Since non linear CA rule (compliment), PB CA rule8 (linear), XOR (linear), S-Box (non linear), PB CA rule128 (linear) and PB CA rule 32 (linear) are reversible, we can decrypt the cipher text to plain text in reverse way. Here the inverses of compliment, XOR and S-Box are compliment, XOR and inverse S-Box respectively. Also the inverses of PB CA rule 8, PB CA rule128 and PB CA rule 32 are PB CA rule 128; PB CA rule 8 and PB CA rule 2 respectively.

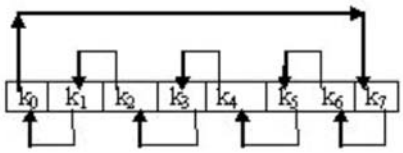

Figure 8: Shifting of rows by PB CA rule-2

Figure 8 shows the use of CA rule-2 Periodic Boundary on each cell of key. For example, in the following matrix, the values in the second column have been shifted to first column, values in the third column have been shifted to second column and so on and values in the first column have been shifted to last column after applying periodic boundary (PB) CA rule-2 to each value in the cell of the matrix.

0	0	1	1	PB CA rule-2	0	1	1	0
0	1	0	1		1	0	1	0
0	1	0	0		1	0	0	0

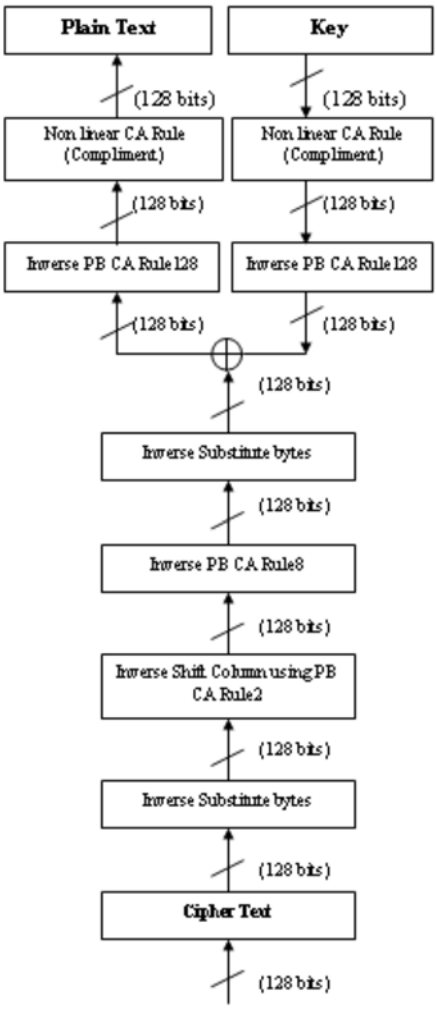

Figure 9: One-round of Decryption algorithm applying CA rule

CONCLUSION AND FUTURE WORK

Our algorithm deals with both linear as well as the non-linear Boolean functions for which we use the linear and non linear rules of cellular automata. This algorithm is more secure than Data Encryption Standard(DES) because the key is used in the beginning of algorithm unlike it is in DES at a later stage and the number of rounds in DES is 16 whereas it is 8 in our algorithm. Also our algorithm contains less number of operations as compared to DES algorithm and hence it will take less time for encryption and decryption as compared to DES algorithm. Our algorithm contains 8 numbers of rounds where as it is 10 in Advanced Encryption Standard (AES) and in this regard it is better than that of AES algorithm and takes less time. Also our algorithm contains more number of non linear functions(confusions or substitutions) than that of AES algorithm, which builds up the better security aspect of cryptography .Because use of non linear functions (substitutions or confusions)have better security than that of linear functions(Permutations or diffusions).

Our algorithm, being based on concept of CA, helps parallel processing of text. Besides, due to availability of chip level design cellular automata machine (CAM), our algorithm can encrypt and decrypt the text at very high speed in the order of nano seconds.

We have planned to develop a new substitute box (S-Box) which will satisfy all the cryptographic properties. Also our aim is to use nonlinear cellular automata rules and its inverse instead of S-Box so that all the operations involved in encryption and decryption algorithm will be done only through CA rules. Also we have planned to apply hybrid cellular automata rules for block cipher.

REFERENCES

[1] Claude Carlet,"Boolean functions for cryptography and error correcting codes". PhD Thesis.

[2] Stephen Wolfram, "Cryptography with cellular automata". Lecture Notes in Computer Science, 218 (Springer-Verlag, 1986) , pages 429-432, 1986.

[3] Subhamoy Maitra and Enes Pasalic, "Further Constructions of Resilient Boolean Functions With Very High Nonlinearity".*IEEE Transactions on Information Theory*, Vol. 48(7), July 2002.

[4] William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, Pearson Education Inc., New Delhi.

[5] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*. Pearson Education Inc., New Delhi.

[6] XIA Xuewen, LI Yuanxiang, XIA Zhuliang, and WANG Rong, "Data Encryption Based on Multi-Granularity Reversible Cellular Automata". Proceedings of *International Conference on Computational Intelligence and Security*, 2009, pages: 192-196.

[7] Debasis Das and Abhishek Ray, "A Parallel Encryption Algorithm for Block Ciphers Based on Reversible Programmable Cellular Automata". *Journal of Computer Science and Engineering*, Volume 1, Issue 1, May 2010, pages: 82-90.

[8] Anirban Kundu, Alok Ranjan Pal, Tanay Sarkar, Moutan Banerjee, Sutirtha Kr. Guha, and Debajyoti Mukhopadhyay, "Comparative Study on Null Boundary and Periodic Boundary 3-Neighborhood Multiple Attractor Cellular Automata for Classification". Proceedings of *third International Conference on Digital Information Management, ICDIM 2008*, pages: 204-209.

[9] Irfan Siap, Hasan Akin, Ferhat Sah, "Garden of eden configurations for 2-D cellular automata with rule 2460 N. Information Sciences, *Volume 180, Issue 18, 15 September 2010, Pages 3562-357.*

[10] Somanath Tripathy and Sukumar Nandi, "LCASE: Lightweight Cellular Automata-based Symmetric-key Encryption". *International Journal of Network Security*, Vol.8, No.2, Pages: 243-252, Mar. 2009.