Image Encryption and Decryption Algorithm Using Two Dimensional Cellular Automata Rules In Cryptography

P. Sanoop Kumar
Department of CSE, Gayatri Vidya Parishad College of Engineering(A),
Madhurawada-530048,Visakhapatnam, India
sanoop@gvpce.ac.in

C. S. U. Sampreeth
Department of CSE, Gayatri Vidya Parishad College of Engineering(A),
Madhurawada-530048,Visakhapatnam, India
sivauday.sampreeth8@gmail.com

S. Aravind Kumar Reddy
Department of CSE, Gayatri Vidya Parishad College of Engineering(A),
Madhurawada-530048,Visakhapatnam, India
aravindkumar.sontireddy@gmail.com

Abstract— This paper presents a newer encryption and decryption scheme for image and also for the data using the cellular automata (CA) rules. This encryption and decryption algorithm for block cipher based on the linear and nonlinear cellular automata rules. The image of any dimension should be the input of this algorithm. First we convert the whole image into pixels that is taken as an input plain text. Then we apply nonlinear CA rules (Complement) to the plain text and also to the key. Then one of the basic PB CA rule is applied to the above results separately. Then the XOR operation should be performed to the above results. After that the result of XOR operation is fed as input to the substitution box (S-BOX). Again basic PB CA rules are applied to the above results and followed by S-BOX. The decryption process is carried out just similar to that of encryption but in reverse way. These encryption and decryption process are performed for 8 numbers of rounds and avoids dependency between the plain text and cipher text such that our proposed algorithm is more secure than the well-known algorithms like AES & DES.

Keywords-Cryptography, cellular automata, substitution byte, linear, nonlinear, Periodic boundary.

I. INTRODUCTION

Cryptography is an important and vital application in security, defence, 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 describes about the history of cellular automata. In Section III, we discuss about literature survey. Section IV and sub sections are describe our new encryption and decryption algorithm by using cellular automata rules.

II. HISTORY

Cellular Automata is a discrete model studied in Mathematics, physics, theoretical biology and micro structure modelling. Cellular Automata is also called cellular spaces, tessellation automata, homogeneous structures and iterative arrays.

Cellular Automation consists of a regular grid of cells, each in one of a finite number of states i.e. ON and OFF. The grid can be any finite number of dimensions. For each cell, a set of cells called its Neighbourhood is defined to the specified cell. A new generation is created, according to the fixed rule that determines the new state of each cell in terms of the current state of the cell and the states of the cells in its neighbourhood. Typically the rule of updating the state of cells is the same for each cell and does not change overtime, and is applied to the whole grid simultaneously. All elementary cellular automata rules are specified by 8 bits because all elementary cellular automata rules are sit on the vertices of the 8 dimensional hyper cube.

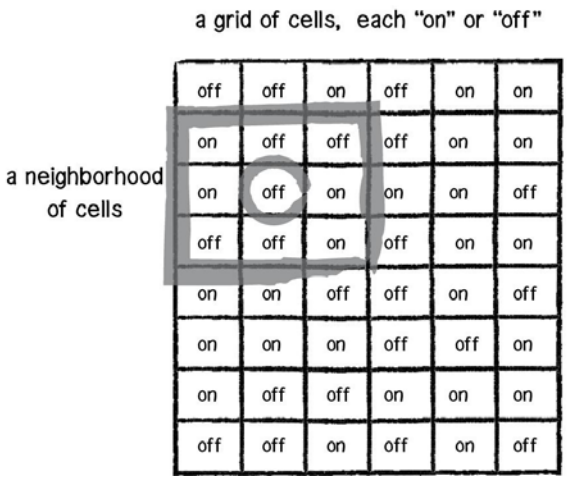

Figure 1:8 dimensional hyper cube

The concept was originally discovered in 1940's by Stanislaw Ulam and John vonNeumann at Los Alomas National laboratory. While studied some throughout 1950's, 1960's it was not until the 1970's and Conway's Game of Life by using 2D cellular Automata.

In the 1980's Stephen Wolfram engaged in a systematic study of one dimensional cellular automata or what he calls elementary cellular automata. He published A New Kind of Science in 2002, claiming that cellular automata have applications in many fields of science. These include Cryptography and computer processor.

A. CELLULAR AUTOMATA

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 Neighbourhood vector

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 Neighbourhood.

B. ELEMENTARY CELLULAR AUTOMATA

The three key elements of CA are

1. Grid: The grid is a line of cells. Simply it would be one-dimensional.
2. States**:** There are two number of states either 0 or 1.
3. Neighbourhood: The neighbourhood in one dimension for any given cell would be the cell itself and its two adjacent neighbours are one to the left and one to the right

In the world of cellular automata a cell state form a group of cells can be compute in many ways. For example blurring an image. A pixels new state (its colour) can be calculated that average of all of its neighbour's colours. We also calculates that a cell's new state is the sum of all of its neighbour's states.

C. 2D CELLULAR AUTOMATA

If we consider d-dimensional grid it is possible to define different kinds of neighbourhood. In particular if we consider two-dimension 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 neighbourhood beyond one.

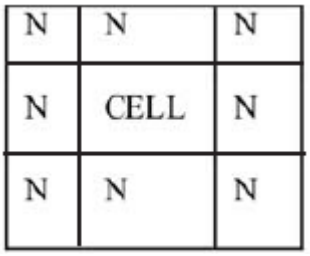

Figure 2: 2D Moore Neighbourhood

Figure 2 shows the structure of two dimensional cellular automata neighbourhood cells respectively. In both of these figures, central cell is denoted by CELL and all of its 9 neighbourhood are denoted by 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 neighbours at time t-1.For two-dimensional 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 neighbourhood nine cells are considered (as shown in figure 2). The 2D CA rules as Boolean functions are

64	128	256
32	1	2
16	8	4

Figure 3: 8-neighborhood CA rules

Figure 3 shows all the rules of two dimensional cellular automata. In 2-D eight neighbourhood CA the next state of a particular cell is affected by the current state of itself and eight cells in its nearest neighbourhood (Table). 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 neighbours 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 neighbour 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 neighbouring cells, the rule number will be the arithmetic sum of the numbers of the relevant cells, which gives the linear rules of cellular automata. For example the 2D CA rule 150 (=2+4+16+128) refers to the 4 neighbourhood dependency of the central cell on right, bottom, left and top. The number of such rules is 8C0+8C1+....+8C8=256.Rule-150 will be applied uniformly applied to each cell.

III. LITERATURE SURVEY

Stephen Wolfram [1] stated that a stream cipher based on a simple one dimensional cellular automata. For this the author derives a rule to update or find the next or new values. i.e. $a_i^1=a_{i-1}$ XOR (a_i OR a_{i+1}). Here a_i contains the values 0 or 1.So in this process the author converts the plain text into cipher text by using the statement. $C_i=P_i$ XOR a_i. The plain text can be recovered by repeating the same operation, but only if the sequence a_i is known. No systematic algorithm for its solution is currently known. The CA can be implemented efficiently on an integrated circuit. It requires less than gate delay times to generate each output bit, and can potentially be used in variety of high band width cryptographic applications. Stephen Wolfram [2] stated that CA may be used as mathematical models for physical, biological and computational systems. In this paper the author analyses the CA and has described some generic features of this behaviour, such as the formation of some patterns. To get the patterns the author describes a set of rules. These rules are applied synchronously to each cell. Olivier Martin et al. [3] stated that Cellular Automata is complex and has a varied behaviour. CA are discrete dynamical systems of simple construction. The complete structure of a state transition diagrams are derived in the terms of number and algebraic quantities. To give an extensive analysis of global properties the algebraic techniques are used. The systems are usually irreversible and contains large number of configurations and cycles. Stephen Wolfram [4] stated that self-organizing in cellular automata is discussed as a computational process. Formal language theory is used to extend dynamical systems theory descriptions of cellular automata. The sets of configurations generated after a finite number of time steps of cellular automaton evolution are shown to form regular languages. Many examples are given. The sizes of the minimal grammars for these languages provide measures of the complexities of the sets. This complexity is usually found to be non-

decreasing with time. The limit sets generated by some classes of cellular automata they appear to correspond to more complicated languages. Many properties of these sets are then formally non-computable. It is suggested that such un decidability is common in these and other dynamical systems. Norman H. Packard and Stephen Wolfram [5] stated that a largely phenomenological study of two-dimensional cellular automata is reported. Qualitative classes of behaviour similar to those in one-dimensional cellular automata are found. Growth from simple seeds in two-dimensional cellular automata can produce patterns with complicated boundaries, characterized by a variety of growth dimensions. Evolution from disorder states can give domains with boundaries that execute effectively continuous motions. Some global properties of cellular automata can be described by entropies exponents. Other are undecidable. Stephen Wolfram [6] stated that cellular automata are discrete dynamical systems with simple construction but complex self-organizing behaviour. Evidence is presented that all one-dimensional cellular automata fall into four distinct universality classes. Characterizations of the structures generated in these classes are discussed. Three classes exhibit behaviour analogous to limit points, limit cycles and chaotic attractors. The fourth class is probably capable of universal computations, so that properties of its infinite time behaviour are undecidable.

IV. IMAGE ENCRYPTION AND DECRYPTION USING 2D CELLULAR AUTOMATA RULES

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 (nonlinear 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 nonlinear (confusion)operations or rules .But if we use more number of nonlinear 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 nonlinear 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 5 shows the encryption and decryption for eight number of rounds whereas Figure 7 and Figure 9 show operations involved in one round encryption and one round decryption using cellular automata rules.

1) STEPS OF ENCRYPTION ALGORITHM

a) Nonlinear 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 nonlinear cellular automata rule (complement) to each bit of the plain texts. Similarly we write the 128-bits key in a 4x4 matrix and apply nonlinear CA rule (complement) to each cell of the key matrix. After the complementation we apply PB CA rule8 separately. Figure 4 shows the use of Periodic Boundary CA rule-8 to the matrix[7].

Figure 4: 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.

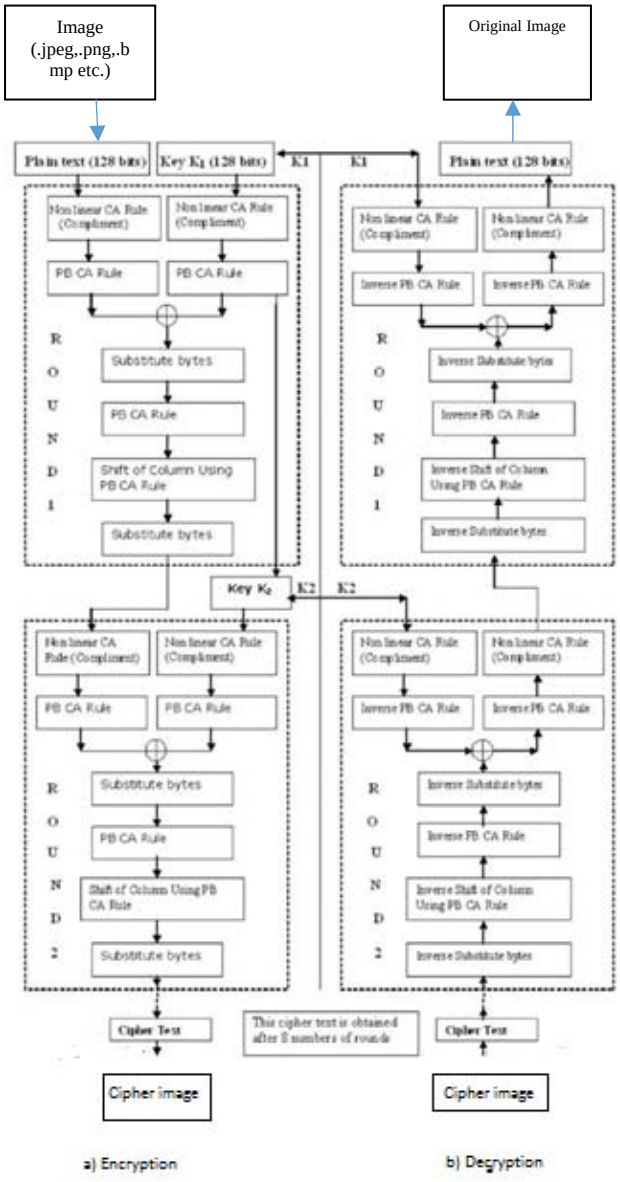

Figure 5: Encryption and Decryption algorithm applying CA rule

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 6 shows an example of the Sub Bytes transformation. Figure 7 shows the general form of Substitute byte transformation.

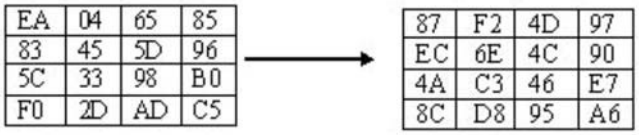

Figure 6: Sub Bytes transformation

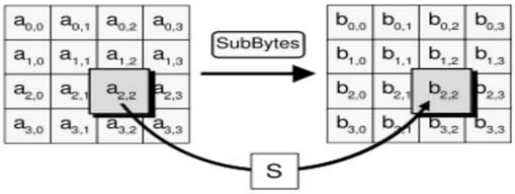

Figure 7: General form of Substitute byte transformation

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 8) 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
0	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

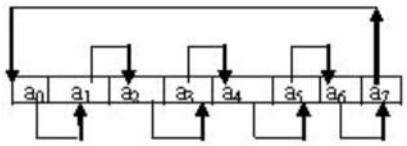

Figure 8: PB CA rule-32 on each cell of plaintext

e) Substitute Bytes Transformation(S-Box):

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

2) STEPS OF DECRYPTION ALGORITHM

Since nonlinear CA rule (compliment), PB CA rule8 (linear), XOR (linear), S-Box (nonlinear), 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.

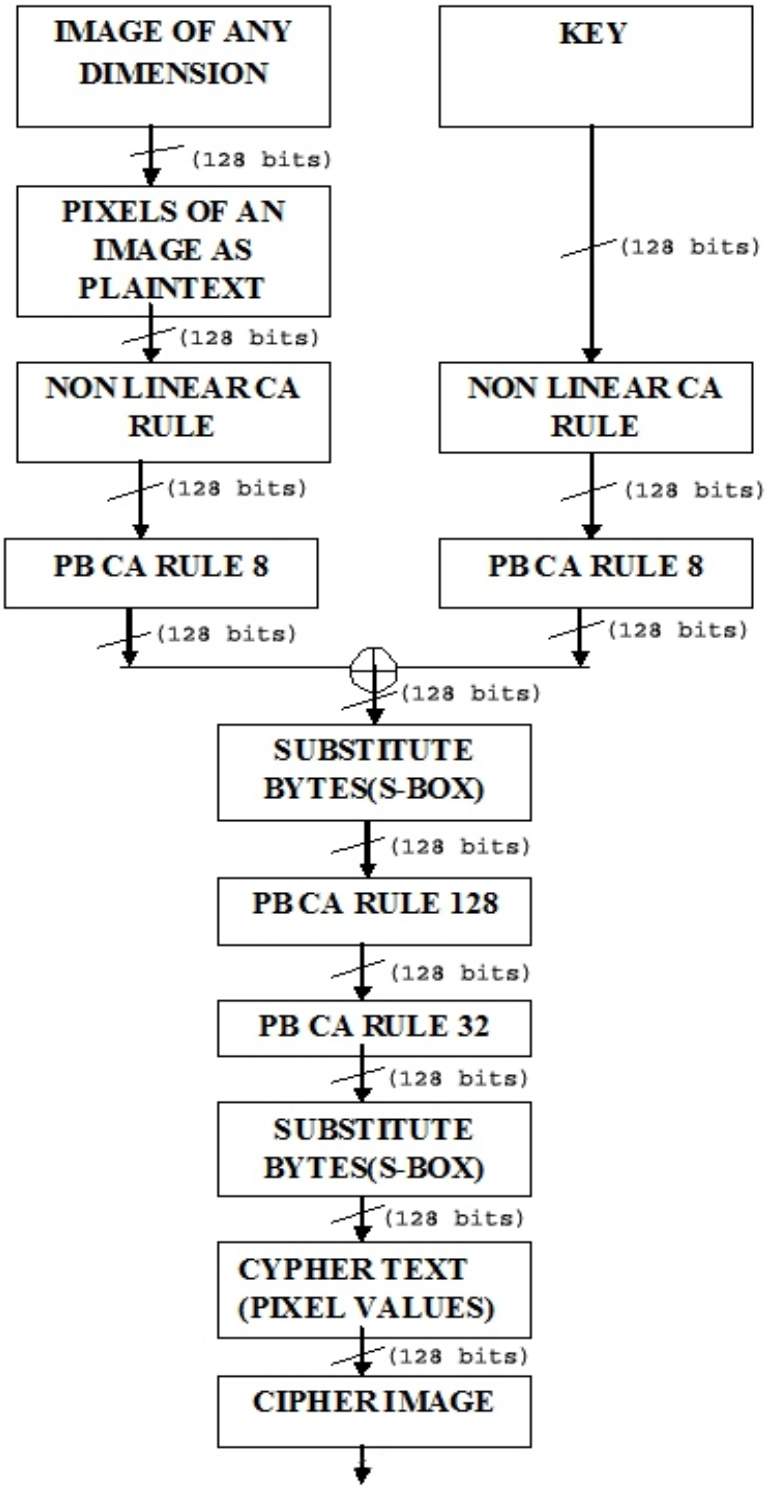

Figure 9: One round of Encryption algorithm

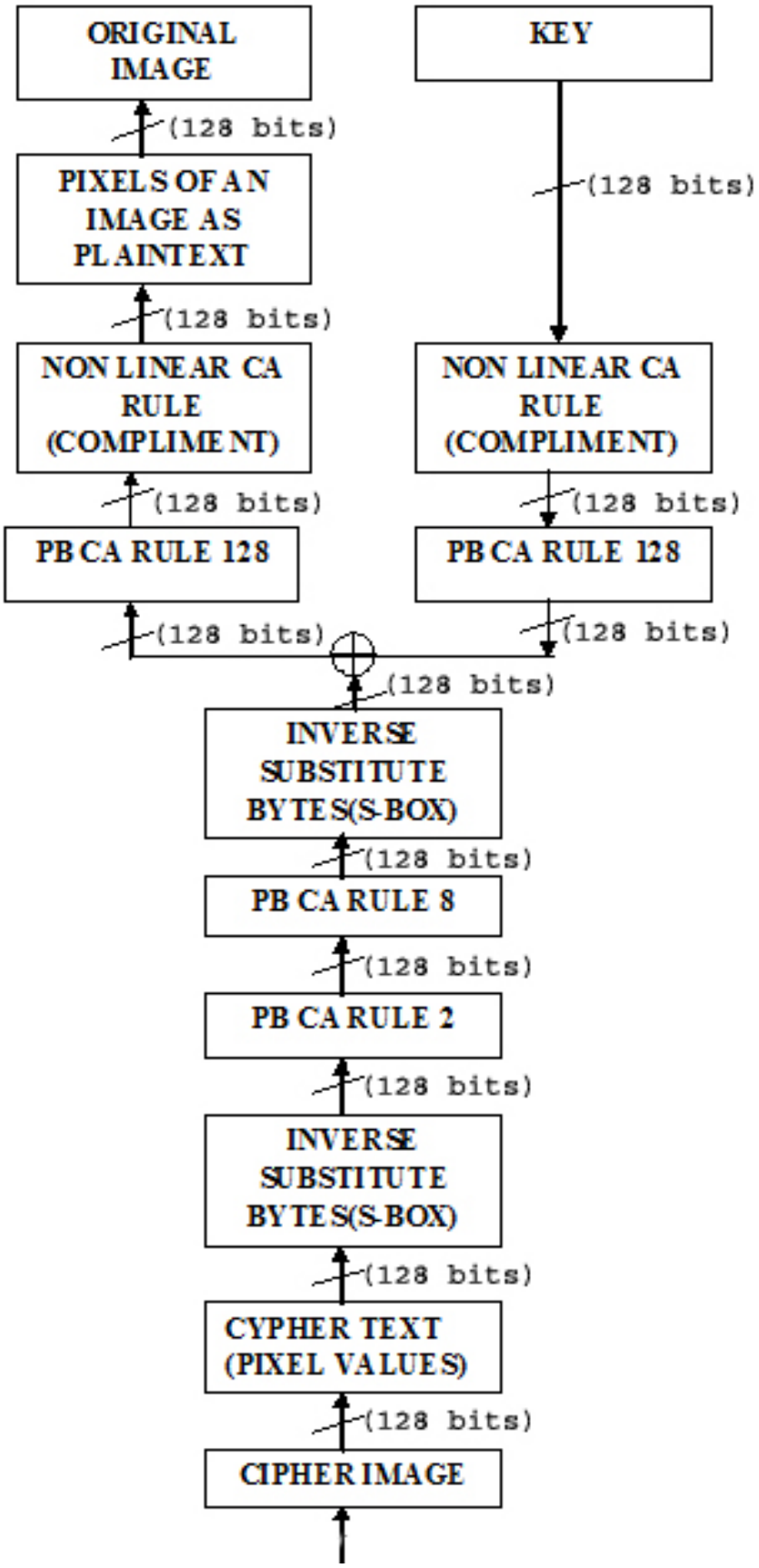

Figure 10: One round of Decryption algorithm

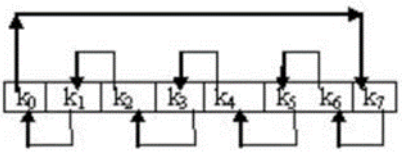

Figure 11: Shifting of rows by PB CA rule-2

Figure 10 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

V. REFERENCES

[1] Stephen Wolfram, “Cryptography with Cellular Automata”, Advances in Cryptology: Crypto '85 Proceedings, Lecture Notes in Computer Science, volume 2 18, pages 429-432 (Springer-Verlag, 1986).

[2] Stephen Wolfram, “Cellular Automata as Simple Self-organizing Systems”, July 1982; revised November 1982.

[3] Olivier Martin, Andrew M. Odlyzko and Stephen Wolfram, “Algebric Properties of Cellular Automata”, Commun. Math. Phys. 93, 219-258 (1984).

[4] Stephen Wolfram, “Computation Theory of Cellular Automata”, Commun. Math. Phys. 96, 15-57 (1984).

[5] Norman H. Packard and Stephen Wolfram, “Two-Dimensional Cellular Automata”, Journal of Statistical Physics, Vol. 38, Nos. 5/6, 1985.

[6] Stephen Wolfram, “Universality and Complexity in Cellular Automata”, Elsevier Science Publishers B .V. (North-Holland Physics Publishing Division), 1984.

[7] Panda, Sambhu Prasad, et al. "Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography." International Journal of Communication Network & Security 1 (2011): 18-23.