Grayscale Image Encryption using Cellular Automata

Mohamed ElRakaiby
Faculty of Engineering
Egypt , Alexandria
249 ElFath Street , Janaklese

ABSTRACT

In this paper, second order cellular automata is applied on a grayscale image as block cipher using 128 bit key ,Also different security analysis are applied for variants of iterations and rounds using block identifier as an additional input to the cipher.

Keywords

Image encryption, Block cipher, Symmetric key cryptography.

1. INTRODUCTION

Image encryption shows significant need recently specially for multimedia applications .Digital images has to be treated in a different way from traditional digital data due to special characteristics of images like pixels correlation and data redundancy so, different security and statistical goals should be achieved .Cellular automata (CA) is one of these mechanisms which can be used to produce an encryption scheme and fulfills all security needs for such a cryptosystem. This paper gives an overview on basic cellular automata concepts and uses these concepts to propose a symmetric cryptosystem using reversible cellular automata (RCA) which can be used for grayscale image and can be expanded for RGB images.

In literature many image encryption schemes has been proposed using cellular automata [1] and present work makes use of different ideas presented in past proposals to study in general the impact of different attributes using a new proposal.

One of the most important ideas studied before is using a tweak or block identifier (Block ID) as a unique input for each block [2] to overcome problems produced from block redundancy in digital images.

2. CELLULAR AUTOMATA

2.1 Elementary Cellular Automata

Cellular automata (CA) composed of a grid of cells. Each cell takes one of a finite number of states, such as live/dead or on/off. The grid can be in any finite number of dimensions. For each cell, a set of cells called its neighborhood is defined relative to the specified cell position. An initial state (time t = 0) is selected by assigning a state for each cell randomly or according to predefined state. A new generation is created (at t=t+1) according to some 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 neighborhood. Typically, the rule for updating the state of cells is the same for each cell and does not change over time, and is applied to the whole grid simultaneously.

The simplest cellular automata system is one dimensional with two possible states per cell which is called elementary cellular automata with two adjacent neighbors per cell and according to cell status and neighbors status at time t=T ,the cell status at time t=T+1 is obtained andcontrolled by transition rule.

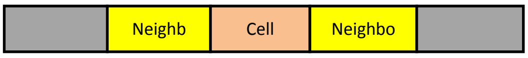


Fig 1: One cell has two adjacent neighbors

Fig 1 shows example of Rule 90 (90=01011010_2) in 1-D elementary cellular automata with 2 neighbors per cell also Fig 2 shows graphical representation of applying Rule 90 on initial state grid of 10010110000001000010010000000011 for 16 iteration.

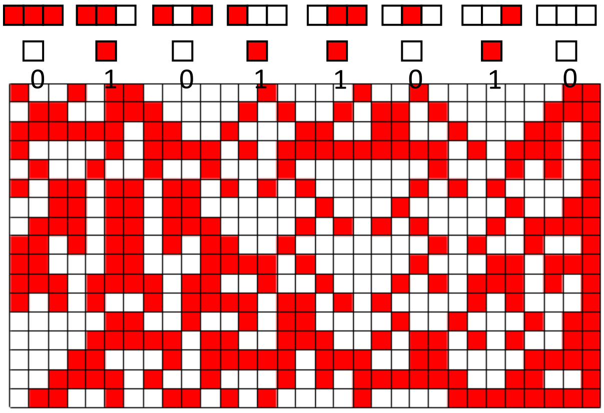


Fig 2: Applying Rule 90 for 16 iterations

2.2 Reversible Cellular Automata

A reversible cellular automaton (RCA) is a special case of CA in which every configuration has a unique predecessor. That is, RCAs are constructed in such a way that the state of each cell prior to an update can be determined uniquely from the updated states of all the cells. Several methods are known to construct cellular automata rules that are reversible. The second-order cellular automaton method invented by Toffoli and Margolus [3], in which the update rule combines states from two previous steps of the automaton permit to turn any one-dimensional binary rule into a reversible one .

If we call all cells states at specific time t: C^t ,the second order RCA is constructed by below equation :

$$C^t = F(C^{t-1}) \oplus C^{t-2}$$

Where F is applying the rule.

That way, the operation is reserved to get older states using below equation:

$$C^{t-2} = F(C^{t-1}) \oplus C^t$$

Cellular Automata has been used recently for many cryptographic applications [4-6] showing a great level of reliability and performance.

3. PROPOSED SYSTEM

As this paper is proposing an image cryptosystem, first image pixels are converted to bits; each pixel will produce only 8 bits as grayscale images pixels have the values between 0 and 255. This group of bits is fragmented into 256 bit blocks to be encrypted independently using a 128 bit key and unique block ID as system inputs then rearranged again into ciphered image Fig 3.

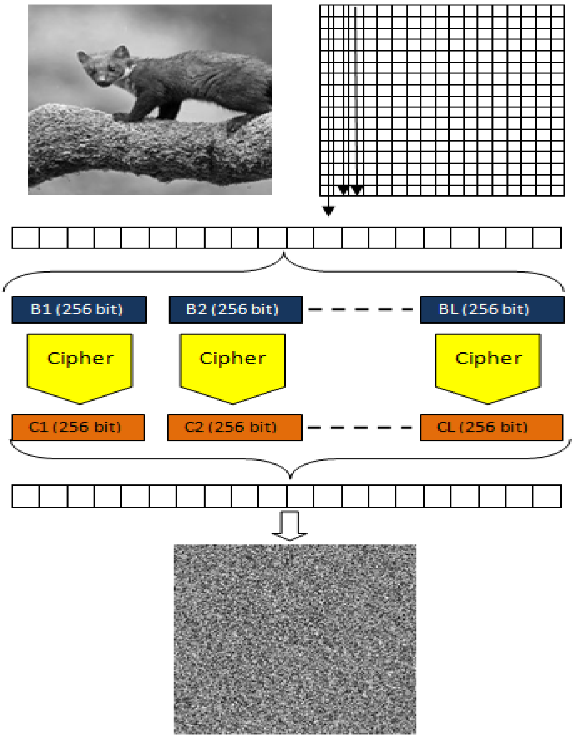


Fig 3: Overview of proposed system

Cipher mentioned in Fig 3 consists of a basic building block (round) Fig 4 which is repeated according to different configuration for proposed system.

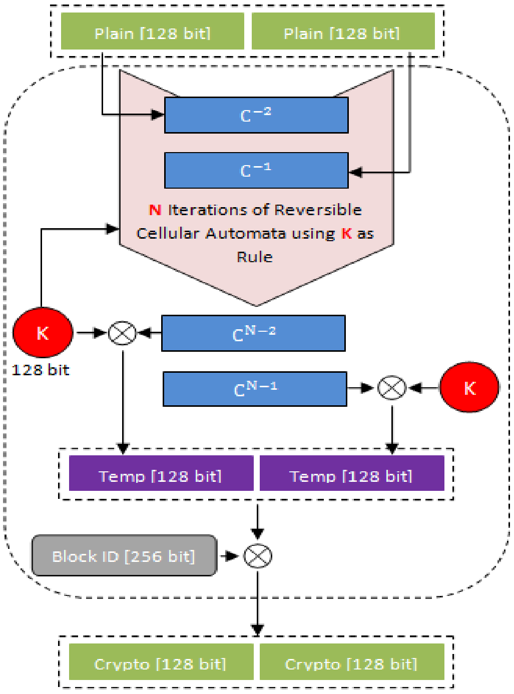


Fig 4: Overview of proposed system

The encryption process starts with dividing the 256 bit block into two 128 bits sub-blocks which represent the initial configuration for the RCA.

RCA starts with $C^{-2}$and $C^{-1}$and pass N iterations using the secret key k as the transition rule then the resulting are $C^{N-2}$and C^{N-1} XORed with the secret key.

The final step in the round is XORing with Block ID which is 256 bits consists of repeated blocks (16, 32 or 64 bit) representing the order of the plain block to be ciphered (i) represented in binary.

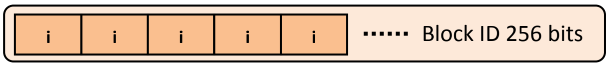


Fig 5: Block ID

Final output of this round can be fed to be input for the same system to perform another round according to cipher configuration.

4. EXPERIMENTAL RESULTS

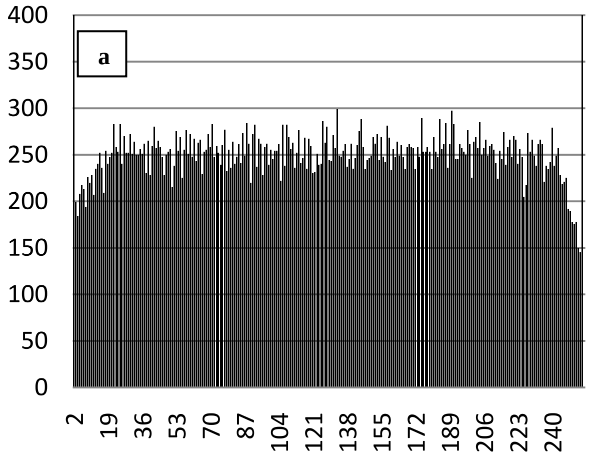
Proposed system was used to build an experiment of variable no of iterations (N) and variable no of rounds (R) for 256x256 grayscale images for all combinations of N and R shown in Table 1.

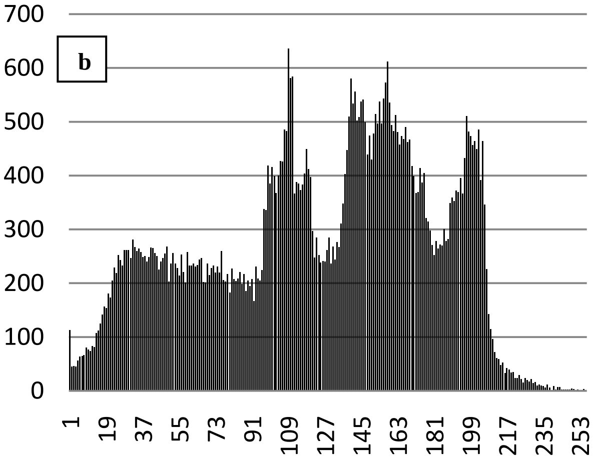
Table 1. rounds and iterations configuration

R=2,N=4	R=2,N=6	R=2,N=8	R=2,N=10
R=4,N=4	R=4,N=6	R=4,N=8	R=4,N=10
R=6,N=4	R=6,N=6	R=6,N=8	R=6,N=10

4.1 Histogram Analysis

The information given by an image histogram represents the statistical distribution of pixels values. Enciphered images must be similar to random ones and lead to a pseudo-uniform distribution (uniform histogram), unlike plain images that have irregular distributions depending on the image content.





Fi\\g 6: Histogram analysis for: a. Plain image b. ciphered image

4.2 Correlation Coefficients of Adjacent Pixels

In this part the Correlation Coefficients of adjacent pixels is presented for different configuration types for different Rounds (R) and different Iterations (N).

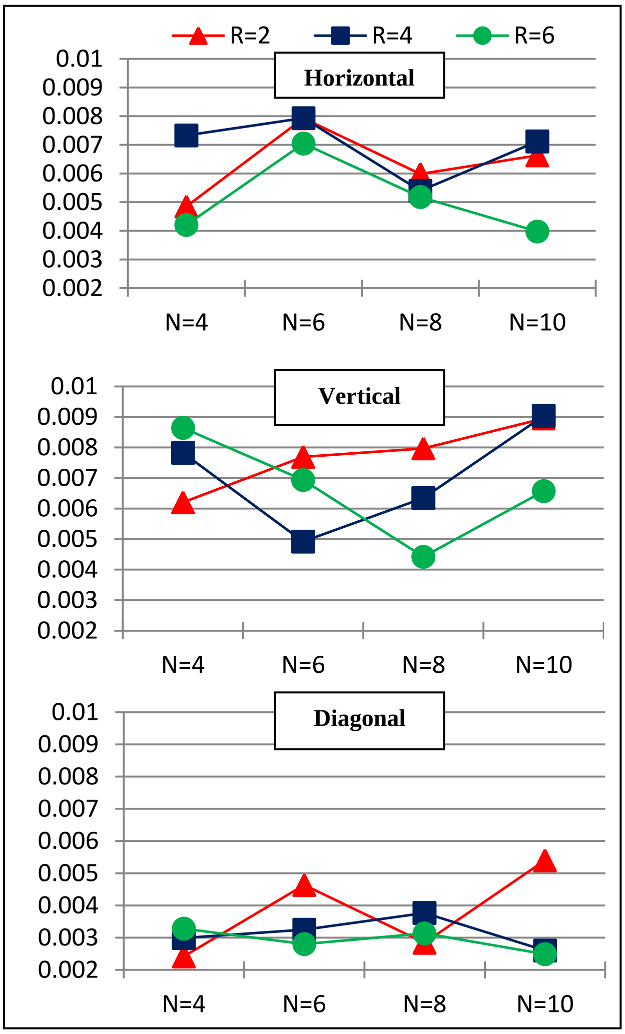


Fig 7 Correlation coefficients of ciphered image

4.3 Sensitivity to Key Variation

It is an important property of an encryption scheme to be very sensitive to little key variation in order to be robust against differential attacks. Here one bit of the key is changed randomly:

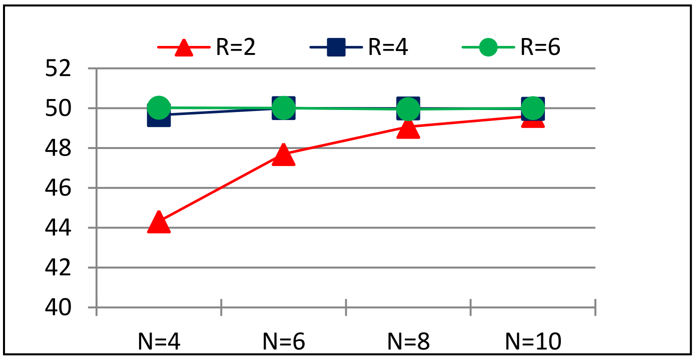


Fig 8 Percentage of changed bits after changing key by one bit

5. CONCLUSION AND FUTURE WORK

Through this paper we have introduced an encryption scheme using Reversible Cellular Automata which showed good statistical results we can start with and enhance for more robustness against different types of attacks.

Future work can be summarized in below points

- Extension of Scheme for RGB images
- Use key-dependent scramblers to enhance statistical properties of ciphered image

6. REFERENCES

[1] Seredynski M, Bouvary P.Block cipher based on reversible cellular automata. New Gener Comput 2005 ; 23: 245–58 (Ohmsha Ltd and Springer)

[2] Faraoun Kamel," Fast encryption of RGB color digital images using a tweakable cellular automaton based schema Optics & Laser Technology 64 (2014) 145–155

[3] Toffoli TT ,Margolus N.Invertible cellular automata : a review . Physica D 2001;45:229–53.

[4] Szaban , M, Seredynski ,F , and Bouvry ,P. Collective behavior of rules for cellular automata based stream ciphers ,evolutionary computation .In :Proceedings of the CEC .IEEE Congress :Jul 16–21 ,2006 .pp. 179–183..

[5] Chatzichristofis Savvas A, Mitzias Dimitris A ,Sirakoulis Georgios Ch, Boutalis Yiannis S. Novel cellular automata based technique for visual multimedia content encryption. Opt Commun 2010 ; 283(21) :4250–60.

[6] Tomassini M, Sipper M, Perrenoud M. On the generation of high quality random numbers by two-dimensional cellular automata .IEEE Trans Comput 2000 ;49 (10) :1146–51