ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

SCAN-CA Based Image Security System

Bhagyashree.S.Anantwar[1], S.P.Sonavane[2]

Student, Department of Computer Science and Engg, Walchand College of Engg, Sanli, India [1]

Asso. Professor, Department of Information Technology, Walchand College of Engg, Sangli, India [2]

Abstract: This paper presents a new methodology for image encryption. The SCAN-CA based image security system belongs to the stream cipher. Its encryption is based on permutations of image pixels and replacement of pixel values. The permutation is done with SCAN pattern generated by the SCAN methodology. SCAN patterns are developed based on the encryption specific SCAN language, which has production rule to generate a different SCAN grammar. The SCAN grammar produces a variable length scan key which is used for image encryption with CA substitution. Image pixel values are replaced using the recursive Cellular Automata substitution. Cellular Automata are dynamical systems in which time and space are discrete. The proposed image encryption method is lossless and it uses a very large number of secret keys. The pixel value permutation is key dependent. Thus, this encryption system finds a great scope in the field of security in terms of, grammar based key generation, large key space with time and space.

Keywords: Image security, Stream Cipher, SCAN methodology, Encryption and Decryption, Cellular Automata

I. INTRODUCTION

With the rapid growth in communication and computer technology, there is a huge data transaction in mobile, internet, TV, teleconferencing, telemedicine and military application. Image encryption schemes have been increasingly developed to meet the requirements for secure transmission over the communication channel. Encryption is an effective mean for reliable security. Numerous image encryption methods are available. They include SCAN-Based methods [2], chaos-based methods, tree structure-based methods and other sophisticated methods. Each method has its strengths and limitation in terms of security, speed and resulting stream size metrics. Each method has discussed above have limitation over a length of security keys. The advantage of the encryption method is with variable length security keys and its corresponding flexible encryption complexity. Therefore, this encryption method can be used by then, when users can choose a suitable security key, according to their requirement for preventing attacks.

This image security method belongs to synchronous stream cipher whose encryption method is based on the permutation of image pixel and replacement of image pixel values. Permutation of image pixel is done by scanning patterns that are generated by the SCAN approach. The pixel values are replaced using a recursive cellular Automata substitution with a generated sequence of Cellular Automata from the Cellular evolution rules. The Scan pattern generated from SCAN approach described in [4] is used because it produces a large number of Scan patterns. Some of the CA advantages are:

(1) CA has been successfully applied to several physical systems, processes and scientific problems that involve local interactions as in image processing, data encryption, byte error correcting code. (2) It has also been used in pseudorandom number generators for VLSI built-in self-test. (3) Number of CA evolution rules are very large. Hence, many techniques are available for producing a sequence of CA data for encrypting and decrypting images. (4) Recursive CA substitution only requires integer arithmetic and/or logic operations that simplifying the computation.

The security system discussed in this paper is different from the other that are described in [7]. In this work, hybrid 2-D *Von Neumann* CA was used to generate a high-quality random sequence as a key - stream, with recursive CA substitution in the encryption and decryption schemes such that the image security system was secure. The cipher systems in the cited study [7] are affine and based on 1-D CA and the encryption and the decryption schemes in [7] are non recursive. Another study [8] showed that affine cipher systems are insecure. The proposed SCAN-CA image security system is an extended and improved version of that presented in the cited study [9], because this system used SCAN techniques and four groups of CA-based recursive substitution to make the exhaustive searching attack much harder and to enhance the performance of the system.

The rest of this paper is organized as follows: Section II provides the key background in SCAN approach and CA. Section III discusses the proposed image security method. Section IV presents the possible secret keys. Section V gives simulation results. The Conclusion is finally drawn in the last section.

II. SCAN approach and Cellular Automata (CA)

A. Scanning

Definition. A scanning of two dimensional array is an order, where each element of an array is accessed exactly once. Scanning of a 2-D array is the permutation of the array elements. Thus scanning of the 2-D array is a $F_{M\times N} = \{\text{if } (i, j)\text{: } 0\leq i\leq M\text{-}1,\ 0\leq j\leq N\text{-}1\}$ is a mapping function from to the set of $\{g\ (l)\text{: } 0\leq l \leq (M\times N\text{-}1)\}$. $M \times N$ array has $(M\times N)!$ scanning paths. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can represent and generate a large

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

number of wide variety of scanning paths easily. The SCAN is a family of formal languages such as Simple SCAN, Extended SCAN and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. Fig 1. Shows an array and two different scanning of that array. One of the scanning path shown is the most widely used is raster scanning.

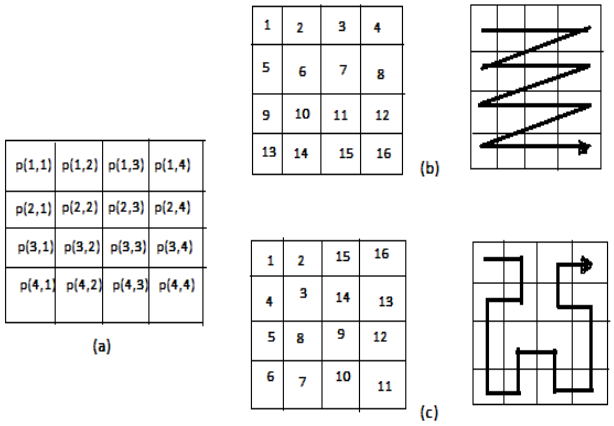


Fig 1. (a) 4×4 array, (b) Scan pattern 1 (c) Scan pattern 2 [2]

Each SCAN language is defined by the grammar. Each language has a set of basic scan patterns, a set of transformation of scan patterns and a set of rules to recursively compose simple scan patterns to obtain complex scan patterns. There are 8 different transformations of scan patterns. They are identity, horizontal reflection, vertical reflection , rotation by 90, 180, 270 and composition of these transformations [2].

In the proposed encryption method, the scanning patterns are used as the encryption keys to rearrange the pixels of the image. The scanning patterns are generated by an encryption-specific SCAN language. This SCAN language uses four basic scan patterns. They are continuous orthogonal O and Spiral S. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are the reverse of transformations 0, 2, 4, 6, respectively. The scanning is formally defined by the grammar $H= (\Gamma, A, \Pi, \Sigma)$ where, $\Gamma= \{A,S,P,U,V,T,I,W\}$ are non-terminal symbols, $\Sigma= \{0,1\}$ are terminal symbols, A is the start symbol and production rule Π are given by

$A \rightarrow S|P|I$: Process the region by a scan S or a partition P or storing image I.

$S \rightarrow 10UT$: means scan the region with basic scan pattern U and transformation T. Prefix 10 indicates basic scanning.

$P \rightarrow 11VT(A\ A\ A\ A)$: Partition the region with partition pattern V and transformation T and process each of the four sub-regions in partition order using As from the left to the right. Prefix 11 used indicates the partitioning.

$U \rightarrow 00|01|10|11$: Scan with a specific scan pattern C or D or O or S respectively.

$V \rightarrow 00|01|10$: Partition with a partition pattern B or Z or X respectively.

$T \rightarrow 000|001|010|011|100|101|110|111$: Basic eight transformations use of scanning and partitioning. Eight transformations encoded as three digit binary numbers.

$I \rightarrow 0W$: Store the original image of the region. Prefix 0 indicates storing an original image region.

$W \rightarrow$ Binary string of length 2^{2n} means, store the image of the region.

B. *Cellular automata (CA)*

Cellular Automata provides a convenient way to represent many kinds of systems in which the values of cells in an array are updated in discrete steps according to a local rule. The cells are arranged in a regular lattice structure, have a finite number of states. These states are updated in a synchronous manner according to a specified local rule of neighbourhood interaction. The neighbourhood of a cell refers to the cell and some or all of its immediate neighbours. Fig 2 shows *Von Neumann* and *Moore* neighbourhood.

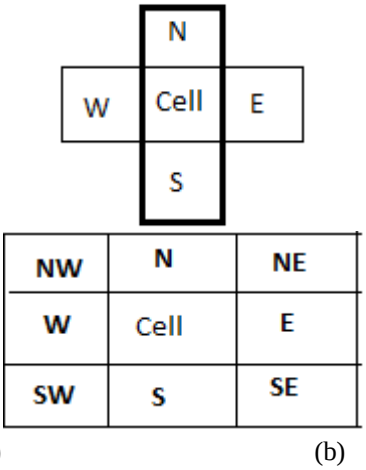


Fig 2. (a) *Von Neumann* Neighbourhood (b) *Moore* Neighbourhood [3]

The *Von Neumann* neighbourhood, which considers the set

$V^N=\{(0,0), (-1,0), (0,1), (1,0), (0,-1)\}$ and then

$V^N_{(i,j)} = \{(i,j), (i-1,j), (i,j+1), (i+1,j), (i,j-1)\}$,

i.e. the neighbourhood of a cell are the cell itself and the four cells placed in the North, South, East and West positions.

The Moore neighbourhood is defined by the set:

$V^M=\{ (0,0), (-1,0), (-1,1), (0,1), (1,1), (1,0), (1,-1), (0,-1), (-1,-1) \}$

So that each cell has nine neighbours: the cell itself, North, North-East, East, South-East, South, South-West, West and North-West. Using a specified rule of neighbourhood, the states are updated synchronously in discrete time steps

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

for all cells. For a k-state CA each cell can take any of the integer values between *0* and (*k*-1). The state of each cell

in a 2-D, k-state, *Von Neumann* neighbourhood CA, is given by the Boolean variable a = $a(i, j, t)$, $0 \le i, j, t \le N$-1. The quantity of $a(i, j, t)$ represents the state of the (i, j)th cell at discrete time t, whose four neighbours are in the states $a(i-1, j, t)$, $a(i+1, j, t)$, $a(i, j-1, t)$ and $a(i, j+1, t)$. For a 2-D *Von Neumann* 2-state CA, each cell has $(2^2)^5$ possible CA evolution , which can be expressed as

$$a(i, j, t+1) = f_B\,(a(i-1, j, t), a(i+1, j, t) , a(i, t) , a(i, j-1, t), a(i,j+1,t)) \quad \ldots\ldots(1)$$

Here $f_B(.)$ is a Boolean function defining the rule. Different cells apply different rules, making the CA hybrid. Since the evolution of the *(i,j)*th cell can be represented as a combinational logic. 2

$$a(i, j, t+1) = C_0 \oplus (C_1.\, a(i-1, j, t) \oplus C_2.\, a(i, j-1, t) \oplus C_3.\, a(i, j, t) \oplus C_4.\, a(i, j+1, t) \oplus C_5.\, a(i-1,j,t) \quad \ldots\ldots(2)$$

III. The proposed image security system

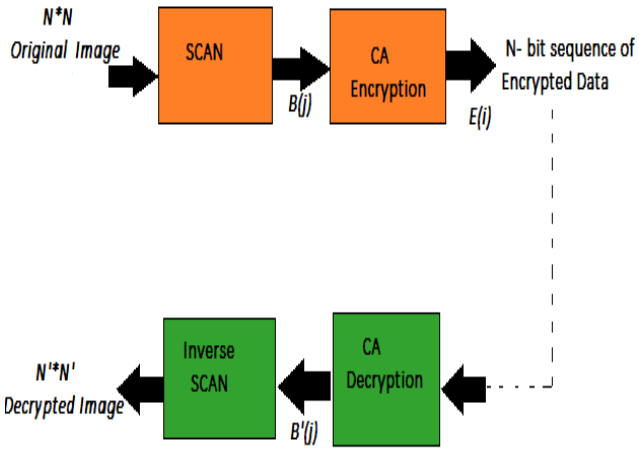
The proposed SCAN-CA based image security system belongs to the stream cipher. A stream cipher is a symmetric key cipher where the plaintext is combined with pseudorandom cipher. In a stream cipher each plaintext is encrypted one at a time with the corresponding number or text of the key stream, to give a digit or the text of the ciphertext stream. The idea of the system is:

a) Rearrange the pixels of the image using Scan keys
b) Pixel values are changed by CA substitution.

For 2-D N*N-cell dual state (0,1) *Von Neumann* Cellular Automata runs over T time steps. It has $2^{32*(N*N)}$ rules, 2^{N*N} initial conditions, 2^{4N} boundary conditions. The CA key is of variable length according to the size of 2-D CA and the number of time steps. Fig. 3 shows the SCAN-CA based image security system. Keys are used for various purposes, such as for encryption and decryption consisting two keys those are scan key and the cellular automata substitution key. Secret keys used for encryption and decryption process are randomly selected according to the requirement of the desired security strength and which are both known to the sender and receiver, before the communication of the encrypted image. The scan key is represented by the encryption-specific scan language and it is used for assigning the typical scanning pattern to the image to rearrange the pixel of the given input image. $A(k,l)$, $0 \le k, l \le N-1$.

CA key used for CA substitution consist of rule selection bits, initial or seed condition bits, boundary condition bits used to encrypt $F(i)$, $0 \le i \le L1-1$ a sequence of N-bit input data .On the sender side , suppose a single pixel is changed in $A(k,l)$, $0 \le k, l \le N-1$ then the corresponding pixel value at some location j in $B(j)$, $0 \le j \le (N*(N-1))$ has also changed. CA key generates an N bit sequence $E(i)$, $0 \le j \le L-1$, encrypted data. On the receiver side, a scan key, CA key and a sequence of *N-bit* encrypted data are required. The image can be decrypted by applying reverse CA substitution key,inverse scan key.

The final decrypted image is same in the dimension as the N*N original image because the given image security system is lossless. The selection of scan pattern is independent of image size, but the selection of 2-D cellular automata is dependent on image size.



Fig(3) SCAN-CA based image security system

IV. Possible secret keys

Let T(n) be the different scan patterns of an 2 dimensional $2^n * 2^n$ array generated by the specific SCAN key defined by the encryption-specific SCAN language. For a $2^n * 2^n$ where $n \ge 2$ images, there are eight different basic scan patterns each with eight transformations resulting in 64 basic scan-transformation patterns. When $n \ge 3$, there are additionally 24 ways to partition the image into four sub-regions of size $2^{n-1}*2^{n-1}$ each having T(n-1) recursive scan patterns. This results in T(2)=64 and $T(n)=64+24(T(n-1))^4$, $n \ge 3$. However, only a portion of scan patterns with a finite number of scan iterations shall achieve a good dispersion, the length of scan key was thus carefully determined as 46bits, meaning that only 246 scan patterns shall be used in the simulation.

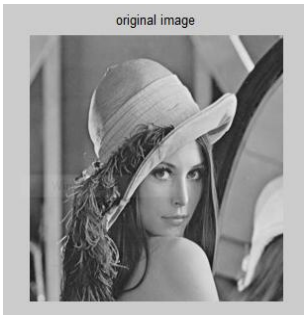
This method uses specified secret key to generate a key-stream used to encrypt the image. The length of the key-stream can be as equal as the length of original image to match the goal of security. The relationship between the image size and the minimum size of a suitable 2-D CA is described as follows. If an image with size of $2^{n1}*2^{n2}$ want to be encrypted, then the minimum size of a suitable 2-D CA is with size of $\sqrt{n1+n2+3} \times \sqrt{n1+n2+3}$ for $\sqrt{n1+n2+3} < 8$ or $\sqrt{n1+n2+4} \times \sqrt{n1+n2+4}$ for $\sqrt{n1+n2+4} \ge 8$. The length of a CA state cycle is very important in determining the suitability of the CA as a generator of random numbers. The average cycle length for 2-D N*N cell dual-state *Von Neumann* CA increases exponentially and is on the order of 2^{N*N}. Most cycle length of 2-D 8×8 cell-dual state *Von Neumann* CA will be longer than 2^{60}.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

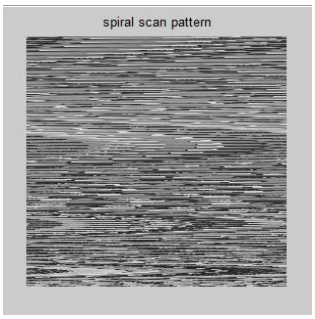
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

IV. Experiment

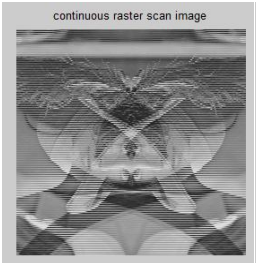
The software implementation of the proposed SCAN-CA-based image security system was performed using Matlab 2014®. The image used for the experiment is 256×256 gray scale Lena image which was used to evaluate the performance of this SCAN-CA-based image security system. Various scan keys with number of scan iterations are used to rearrange the pixels of these tested images. Fig(4) shows and original Lena image. Fig(5) shows simple spiral scan pattern using the scan grammar S5 and the corresponding scan key shown in Table I. Similarly, Fig(6) shows continuous raster scan pattern C2 and Fig(7) shows continuous diagonal scan D7 of the original image. Fig(8) shows partitioned image using scan grammar B3(S5 C2). Image is partitioned into two halfs with partition pattern B and transformation 3 and each half is then scanned using two different scanning patterns. First half scans using spiral pattern S with transformation 5 and the other half is scan using continuous raster scan pattern with transformation 2. Similarly, Fig(9) shows partitioned image using scan grammar B0(C2 S5 D7 I). The generation of grammar is based on the production rule. Table I shows the basic scan grammar and the scan key generated from the scan grammar.



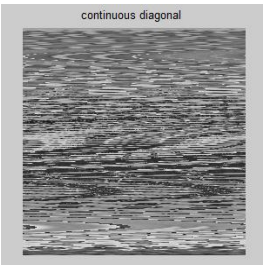
Fig(4) Original Image



Fig(5) Spiral Scan



Fig(6)RasterScan



Fig(7) Diagonal Scan

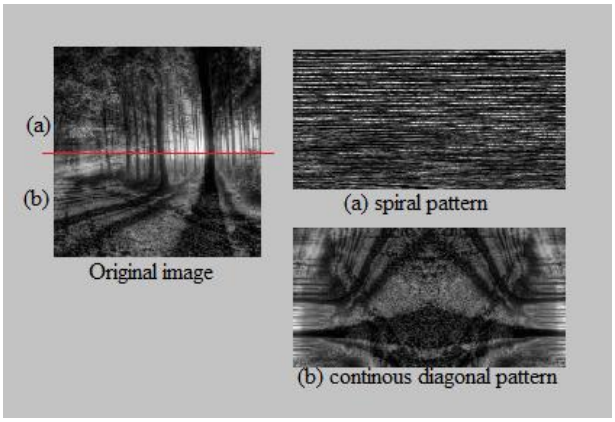
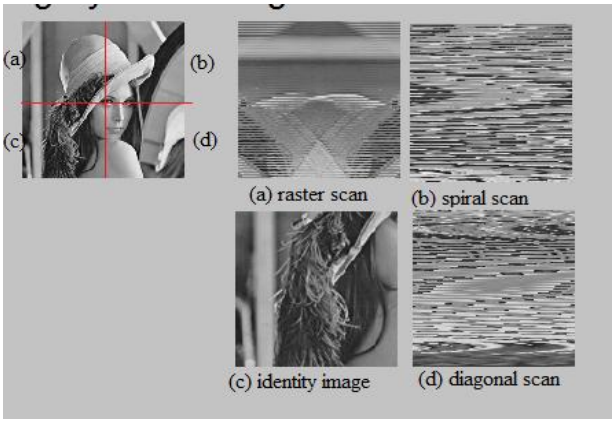


Fig (8) partitioned image using scan pattern B3(S5 C2)



Fig(9) partitioned image using scan pattern B0(C2S5D7I)

Different Scan patterns are applied for permutations of the image pixels and the same CA rule is applied to all scanned images for encryption. Decrypted image has same entropy value as that of the original image as shown in Fig(10) and its PSNR value come out to be infinity.

Table I
SCAN GRAMMAR AND SCAN KEY

Sr.no	SCAN Grammar	SCAN key
1	Basic spiral pattern S with transformation 5 (S5)	11101
2	Basic continuous raster pattern C with transformation 2 (C2)	00010
3	Basic continuous diagonal pattern D with transformation 7 (D7)	10111
4	Partition grammar1 B3(S5 C2)	110001110111011000010
5	Partition grammar2 B0(C2 S5 D7 I)	11001011000010101110110011110

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

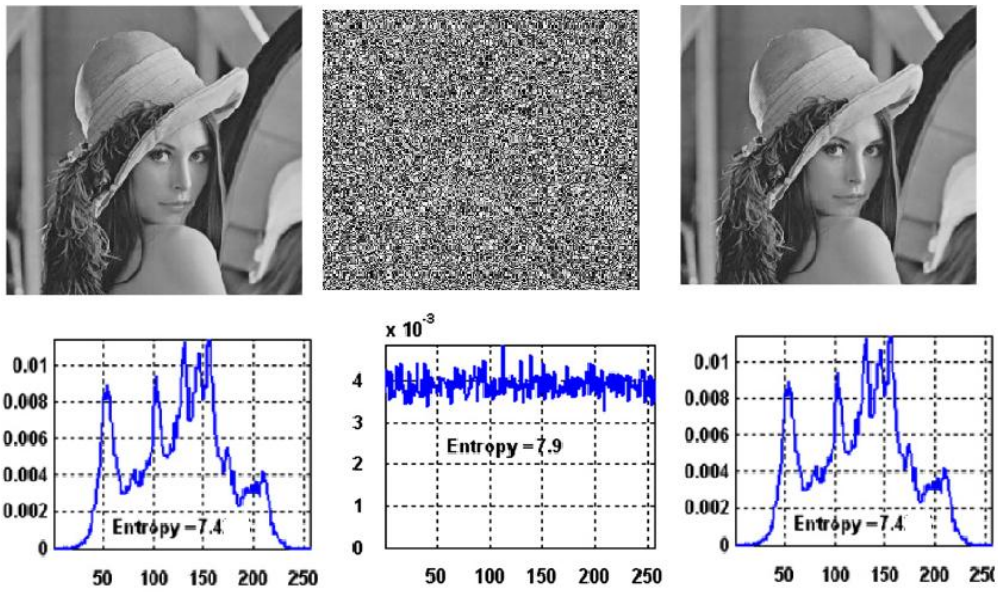


Fig (10). Original Image, Encrypted Image and Decrypted image with their corresponding pdf's and entropy

V. CONCLUSION

The image security system based on SCAN methodology and Cellular Automata have following advantages :
(1) Large number of key space.
(2) Dynamic choice CA rule to increase cryptcomplexity.
(3) Choosing a suitable size for the 2-D CA, according to the size of the image, enables the system to withstand the cropping-and-replacement attack.

REFERENCES

[1] Rong-Jian Chen, Shi-Jinn Horng " *Novel SCAN-CA-based image security system using SCAN and 2-D Von Neumann cellular automata* ",The Journal of Signal Processing :Image Communication 25(2010) 413-426.
[2] S.S. Maniccam, N.G. Bourbakis,,"*Lossless Image compression and encryption using SCAN patterns*", Pattern Recognition 35(2001) 2000 1229–1245.
[3] Saisubha V, Priyanka U , Remya K R & Reenu R "*Image Encryption Using SCAN Pattern*", Proceedings of AECE-IRAJ International Conference, 14th July 2013, Tirupati, India, ISBN: 978-81-927147-9-0.
[4] R.J. Chen, J.L. Lai," *Image security system using recursive cellular automata substitution"*, Pattern Recognition 40 (5) (2007) 1621–1631.
[5] Franciszek Seredynski, Pascal Bouvry, Albert Y , Zomaya," *Cellular automata computations and secret key cryptography*", Parallel Computing International Conference 2004 Published by Elsevier B.V. doi: 10.1016/j.parco.2003.12.014.
[6] A. Martin del Rey, G.Rodriguez Sanchez, A.del la Villa Cuenca, "*Encrypting Digital Image using cellular Automata*" , E. Corchado et al. (Eds.): HAIS 2012, part II, LNCS 7209,pp 78-88,2012 © Springer-Verlag Berlin Heidelberg 2012.
[7] Rosin P L , "Training Cellular Automata for Image Processing ", IEEE transaction Image Processing 15 (7) (2006), pp 2076-2087, ISSN 1057-7149.