Engineering Science and Technology, an International Journal 17 (2014) 85–94

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: http://ees.elsevier.com/jestch/default.asp

Full length article

A parallel block-based encryption schema for digital images using reversible cellular automata

Faraoun Kamel Mohamed*

Computer Sciences Department, Djilalli Liabbes University, Sidi Bel Abbès, Algeria

ARTICLE INFO

Article history:
Received 2 November 2013
Received in revised form
6 April 2014
Accepted 6 April 2014
Available online 5 May 2014

Keywords:
Reversible cellular automata
Images encryption
Pseudorandom permutations
Parallelism

ABSTRACT

We propose a novel images encryption schema based on reversible one-dimensional cellular automata. Contrasting to the sequential operating mode of several existing approaches, the proposed one is fully parallelizable since the encryption/decryption tasks can be executed using multiple processes running independently for the same single image. The parallelization is made possible by defining a new RCA-based construction of an extended pseudorandom permutation that takes a nonce as a supplementary parameter. The defined PRP exploit the chaotic behavior and the high initial condition's sensitivity of the RCAs to ensure perfect cryptographic security properties. Results of various experiments and analysis show that high security and execution performances can be achieved using the approach, and furthermore, it provides the ability to perform a selective area decryption since any part of the ciphered-image can be deciphered independently from others, which is very useful for real time applications.

1. Introduction

Due to the huge expansion of images and multimedia use in current nowadays applications, the need for fast and secure representation, transmission and storage schemas become more and more crucial, especially because digital images can contain private and confidential information that may be associated with financial, medical or personal interest. Unlike traditional types of data such as texts and binary flows, digital images have different and specific characteristics that make their encryption using classical standard encryption schemas (like AES, DES and others) fail to achieve best efficacy and performances. Redundancy, bulky data capacity and high correlation across blocks of pixels make digital images a specific kind of data that need dedicated encryption algorithms to handle such particularities and provide better performances especially in term of encryption speed and security.

Recently, many images encryption techniques and approaches have been proposed in the literature, using different models and theories including chaos-based encryption that use confusion/diffusion techniques [1–4] to provide resistance against known-plaintext and chosen-plaintext attacks. Cellular automatons (CA) are another kind of dynamical systems that has been successfully and widely used to build robust images cryptosystems by exploiting their dynamical and randomness properties, with the capacity to exhibit complex and unpredictable behavior.

Since the first work proposed by Wolfram [5] to build a CA-based stream cipher, many techniques and approaches emerged using different classes and models of CAs. Works in Refs. [6–8] propose variants of CA-based stream ciphers for image encryption using combination of several rules to generate pseudo-random numbers sequences and combining them to the target image using the Vernam model. Even if stream ciphers are generally considered to be the fastest class of cryptosystems, they are vulnerable to known-plaintext attacks unless specific mechanism of key randomization is used (i.e. the same key must never be used more than one time).

Block-ciphers are another category of cryptosystems where the plain-data is considered as a sequence of fixed length blocks. Enciphering is performed using some specific operation mode such like CBC, CTR or OCB. In such encryption schema, each block is ciphered independently, and the result is used as input to encipher the next one in an iterative way. Block-ciphers are generally resistant to both known and chosen plaint-text attacks, and permit to deal perfectly with the redundant nature of digital images since same blocks are never encrypted in the same way. However, they are generally sequential and iterative (except the CTR mode that act like a stream-cipher), and as a result slow with respect to stream-ciphers and chaotic confusion/diffusion approaches. Many cellular automaton block-ciphers have been proposed using reversible

* Tel.: +213 775323650.
E-mail address: kamel_mh@yahoo.fr.
Peer review under responsibility of Karabuk University.

http://dx.doi.org/10.1016/j.jestch.2014.04.001

cellular automatons [9–11] but with a specific operation mode designed to handle block-encryption enchainment since standardized operation modes have not been yet used with CA's based cryptosystems. Existing CA-based approaches are almost all sequential and as a result, the parallel implicit nature of CAs is not effectively exploited.

In the present paper, we propose a completely new CA-based encryption model that act like a block-cipher but in a fully parallel mode. Using second-order cellular automatons, a pseudo-random permutation (PRP) is first constructed, and then injected into a parallelizable encryption schema that act on the different blocks of a digital image independently. The proposed system is robust against know-plaintext and chosen-plaintext attacks unlike stream-based CAs approaches, and has the main advantage to be fully parallel unlike existing block-based CA's approaches. A nonce-based technique is introduced to deal with the ECB (electronic code book) problem, so that two block of the same content are never encrypted in the same way. This technique prevents the need for block dependency like standard block operating modes does, so allows a coherent parallelization of the encryption. The remaining of the paper is organized as follow: related works on images encryption are firstly presented. A theoretic background about cellular automata and the second-order reversible class is presented in Section 2. The Section 3 describes the construction of the proposed PRP permitting to encipher individual blocks, when Section 4 gives details of the full parallel implementation of the proposed encryption schema. Security analysis and encryption performances with experimental results are presented in Sections 5 and 6, when conclusions are finally drawn in Section 7.

2. Related works

Recently, many researchers address the images encryption problem using two main approaches: chaos theory and cellular automata. Using chaos-based techniques, designing the diffusion function can be quite challenging. This should be done in such a way that resistance to known-plaintext and chosen-plaintext attacks are achieved [12,13]. In Ref. [13] the security of Ref. [14] is analyzed and some weaknesses are found which are mainly caused by infirm diffusion architecture. Li and Chen [15] analyze the diffusion function of the schemes of [16,17] altogether and found some problems including a serious flaw of the diffusion function. In Ref. [35], the authors employ cryptographic primitive operations with a non-linear transformation function within encryption operation, and adopt round keys for encryption using the chaotic tent map. In Ref. [36], the same authors propose an enhancement of the RC5 block cipher using chaotic transformation to build a robust images cryptosystem.

Ever since Wolfram studied the first secret key process based on cellular automata [5], many researchers had explored variants cryptology based on them. Especially in recent years, CAs has been already used largely for image cryptography [18,19,32], image processing [20,21], authentication and security [22,23] and so on. Methods exploiting other techniques to encipher images have been proposed also in Refs. [24–28].

3. Reversible cellular automata

A Cellular Automata consist of a number of cells arranged in a regular lattice, each cell has its own state that can change in a discrete time step. States of the whole CA's cells are updated synchronously using a local transition rule that defines each new cell's state using its old state, and the states of the corresponding neighbors. The neighbors are a specific selection of cells relatively chosen with respect to a given cell's position that can be defined for each cell i using a radius r on the lattice. This will gives $n = 2r + 1$ different neighbor including the cell i itself. The boundaries cells of the lattice are concatenated together in a cyclic form to deal with the finite size automatons.

Formally, if we define the state of a cell i at the time t with q^t_i, its state on time $t + 1$ will depend only on the states of the corresponding neighborhood at the time t, by applying a transition rule that defines the way states are updated. If the neighborhood radius is r, and only two cell states are defined, the length of each transition rule is then 2^{2r+1} bit, and the number of possible rules is $2^{2^{2r+1}}$. For one dimensional binary CAs, a transition rule is generally coded using the integer value of the corresponding binary representation. In the present work, we consider one-dimensional binary CAs with radius $r = 3$, so that we have 2^{128} possible rule.

Unlike elementary cellular automata, a reversible cellular automaton is a specific 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 automata method invented by Ref. [29], in which the update rule combines states from two previous steps of the automaton permits to turn any one-dimensional binary rule into a reversible one using the fact that the state of a cell at time t depends not only on its neighborhood at time t-1, but also on its state at time t-2. This is achieved by combining the ith cell state at time t with the state of the same cell in time $t - 2$ using the *xor* operator.

If we define the configuration state of a given CA at each time step t by C^t, we can build a second-order RCA using any elementary CA by the following equation:

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

when the map "F" denote the global evolution map of the used basic CA. The defined RCA can then be reversed trivially using the following equation:

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

Second-order RCAs defined using Equation (2) are always reversible even if the basic used CA defined by the map F is not. We can so construct as mush RCAs as possible existing CAs. Reversibility is performed using the same transition rule in both directions, raising qualitatively the same behavior of one-order CAs as pointed by Wolfram [30], which makes the use of such defined RCAs very appropriate for cryptosystems building.

Instead of using one initial configuration like standard one-dimensional CA, two initial configurations are used to evolve a second-order RCA. Starting from two configurations C^{-1} and C^0 it gives after n time step tow configurations C^{2n-1} and C^{2n}. By running the RCA backward starting from C^{2n-1} and C^{2n} as initial configurations, we can recover the two configurations C^{-1} and C^0 after exactly n iteration using the same transition rule and the same principle of combining with the $(t-2)^{\text{th}}$ state at each time step t. Security of RCA-based cryptosystems is assured by the impossibility to reconstruct initial conditions pair from any given pair of consecutive configurations without the knowledge of the transition rule used initially.

4. The proposed encryption schema

As stated in the introduction, the proposed encryption schema is a symmetric block-based one, so the same secret key K is used by both encryption and decryption process. The key is 128 bit size

which ensures a sufficiently large key space robust against exhaustive key search attacks. Plain-images to be enciphered are decomposed into blocks of 256 bit size that are encrypted in parallel unlike sequential existing block-based that perform encryption of the ith block B_i after encryption of all blocks from B_0 to B_{i-1}. In order to build such parallel encryption mode, a keyed PRP is defined on 256 bit blocks that take a key, a nonce and a data block as input to produced a ciphered block of same size as output. We detail the construction of the PRP and the construction of the general parallel image encryption schema in the following sections.

4.1. Construction of the proposed PRP using second-order CAs

Let first give some basic definitions about permutations and pseudo-random permutations (PRPs). A function Φ defined on the set of all binary strings of length n into the same set Φ:{0,1}^{n} → {0,1}^{n} is said to be a permutation if and only if it is a bijection (i.e. Φ^{-1} exist and is efficiently computable).

A family of permutation Φ_k defined by:

$$\Phi_k : Kx\{0,1\}^n \rightarrow \{0,1\}^n$$

$$(k,x) \rightarrow y = F(k,x) \tag{3}$$

is said to be a pseudorandom permutation family if it cannot be distinguished from a truly random permutation selected randomly from the set of all permutations on functions domain for any value of k [31]. Given the output of the function Φ_k and the output of a truly random function, no polynomial algorithm that can distinguish between the two outputs must exit. A pseudorandom permutation family can be considered as a collection of pseudorandom permutations, where a specific one may be chosen using a key. In the following, we use the term PRP to refer to any pseudo-random permutation family Φ_k. Formally, a PRP is said to secure if the advantage of any distinguishing algorithm from a truly random permutation is negligible.

Pseudorandom permutations have been largely studied and analyzed to be used for cryptographic purposes. Almost all block ciphers can be considered as PRPs such like the standards DES or AES. Many PRPs construction algorithms have been proposed in the literature, where the most known and used is the standardized Lubby–Rackoff construction using Feistel networks [34]. In the following, we define a new construction of PRPs using second-order reversible cellular automata, and we show in later sections that it can achieve very promising performances competitive to those of the standard ones.

Let define the proposed PRP as a function Φ that transform an input plaintext block PB_i of 256 bit size into a ciphered block CB_i of same size. We extend the definition of a PRP by defining three parameters as inputs instead of two in the standard definition. The function Φ takes a key K (the secret key of encryption), a nonce n_i (specific for each block PB_i) and the block PB_i to produce the ciphered block CB_i. If we note by $I = \{0,1\}$ the set of possible binary values, and I^n the set of possible binary stings with size n, the function Φ can be defined by:

$$\Phi : I^{128} \times I^{32} \times I^{256} \rightarrow I^{256}$$

$$(K, n_i, PB_i) \rightarrow CB_i = F(K, n_i, PB_i) \tag{4}$$

The second parameter n_i is introduced to prevent the ECB encryption problem, such that same plaintext blocks are never ciphered in the same way since a nonce n_i is different and specifics for each block B_i, and do never repeat for the same key. We have considered in the present work that the value of n_i is simply the order i of the block B_i represented on 32 bit, so that we can deal with 2^{32} different blocks of the same plain-images, and be able to encipher images of size $32*2^{32} = 2^{37}$ byte, which is largely sufficient for nowadays applications.

As explained in Section 2, second order RCAs start evolving from two different configurations: an initial configuration C^0 and a pre-initial configuration C^{-1}, to gives after m iteration using the same transition rule R two corresponding configurations C^{2m-1} and C^{2m}. This mechanism is used to build the proposed PRP that act like the following: first, a plain-block B_i is split into two 128 bit length sub-blocks BL_i and BH_i (standing for the low and high order parts of B_i). The two sub-blocks are first combined each one using a xor with a sub-key Sk_i derived by altering the key K using the nonce n_i. This alteration is performed in a simple but effective way illustrated in Fig. 1. After the xor combination, the resulting pair of configurations (the two sub-blocks) undergoes five rounds of 8 iterations each one. At the end of each round, the two resulting configurations are exchanged and used as input of the next round. During each round, the input configurations are evolved using a different transition rule. The first, third and fifth round are performed using the master key K as transition rule, when the second and fourth rounds use the sub-key Sk_i as transition rule. Totally, 40 iterations are performed, and at the last, the resulting configuration C^{79} and C^{80} are combined newly with the sub-key Sk_i using a Xor, then concatenated to form the final ciphered block CB_i. Fig. 1 illustrates the details of the PRP described mechanism.

Since second-order RCA's initial conditions are very sensitive to variations, only one bit modification of the key is sufficient to produce a completely different evolution behavior. This ensure that even if the sub-key's derivation process is trivial, it ensure the modification of at less one bit of the key K when using any nonce n_i, and so all sub-keys Sk_i are different and produces a completely different behavior when used to encipher different plaintext blocks PB_i that have same content.

Decryption using the proposed PRP is performed using exactly the same schema and the same parameters. If the input of the function is the key K, the nonce n_i and the ciphered block CB_i, the output will be automatically the plain-block PB_i. This is a great advantage of the proposed PRP, since this will permit to use the same hardware circuits for both encryption and decryption if hardware implementation is used and the same programming code if software implementation holds.

The proposed PRP Φ is experimentally shown to be indistinguishable from a random permutation, and very sensitive to small variations of each parameter PB_i, n_i and the key K. These two properties make the PRP enough secure and suitable for cryptographic applications. Analysis of the proposed PRP with corresponding experiments and results are presented in the next sections.

4.2. The parallel images encryption schema

Unlike most existing image encryption schemas using confusion/diffusion, sequential block ciphering or stream ciphering, the proposed approach is completely parallel and there is no need for multiple iterations to ensure a complete avalanche criterion satisfaction. Input color or gray-scale plain-image is considered as a set of independents 256 bit blocks that can be ciphered independently from one another using the proposed PRP. Blocks can be ciphered by groups or independently depending on the parallelism level of the used platform, and the number of used processors or threads.

The input image to be enciphered is first decomposed in equal length 256 bit blocks PB_0,…PB_L, when a padding schema can be used if the size of the image is not multiple of 256. Each block PB_i is transmitted to the PRP Φ with the secret key K and its

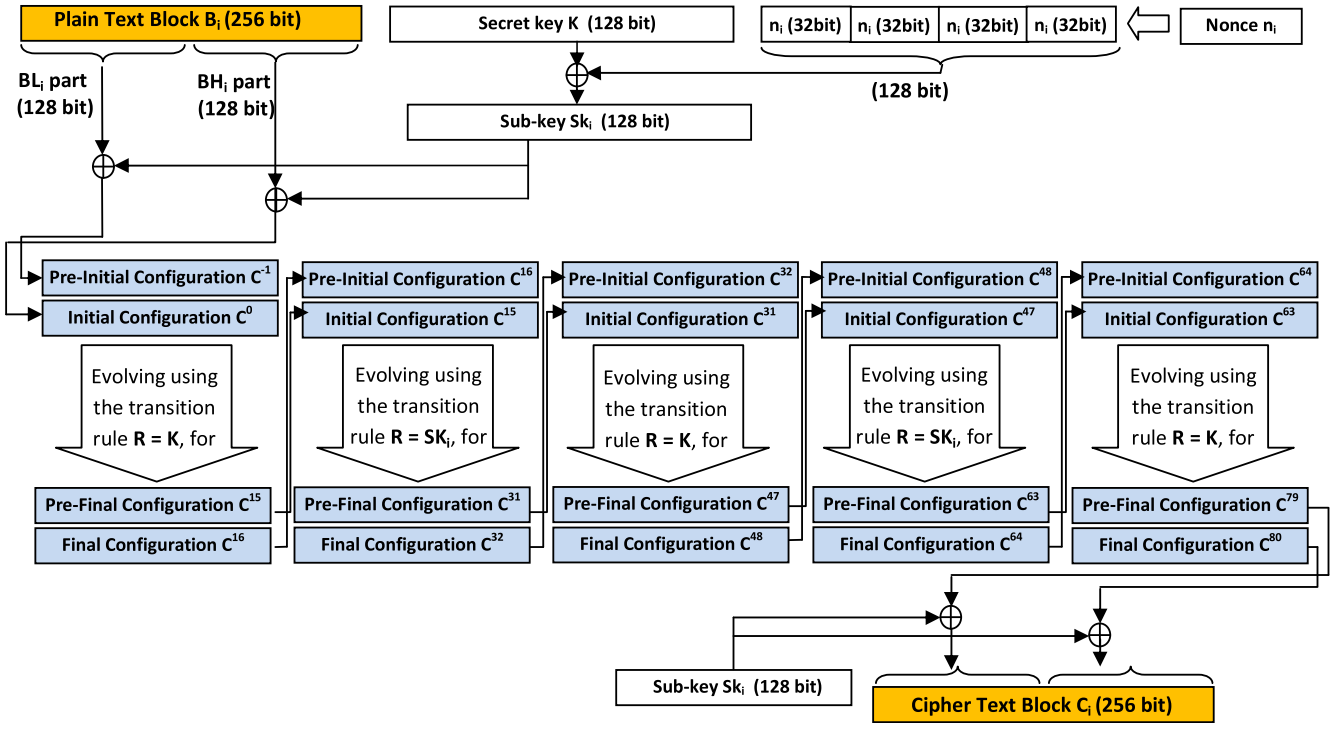

Fig. 1. Proposed RCA's based PRP, used for encryption/decryption of a single 256 bit block.

corresponding range i used as nonce. The output of Φ will be the corresponding ciphered block $CB_i = \Phi(K,i,PB_i)$. After all plain-text blocks are processed, corresponding ciphered block $CB_0,\ldots,CB_L$ are combined using the same ranges to form the final ciphered image. Since enciphering of each block is independent from the others, it clear that the task is be fully parallelized. Fig. 2 illustrate the proposed enciphering process.

It is important to note that plain-text blocks that have same content can never be ciphered in the same way since the nonce is different and never repeated for the same image of size lower than 2^{37} byte. The introduction of the nonce in the proposed PRP is provided to solve the ECB enciphering problem and remove the need for sequential block enchaining or iterative confusion/diffusion that are time consuming. The security and efficacy of the proposed schema is based upon the extreme sensitivity of the proposed PRP to any small variation of the nonce value, which is proven experimentally in the following section.

Since Φ is self-invertible ($\Phi = \Phi^{-1}$), the decryption process is performed in the same way. The enciphered image is inputted to the same system using the same key, and the output will be

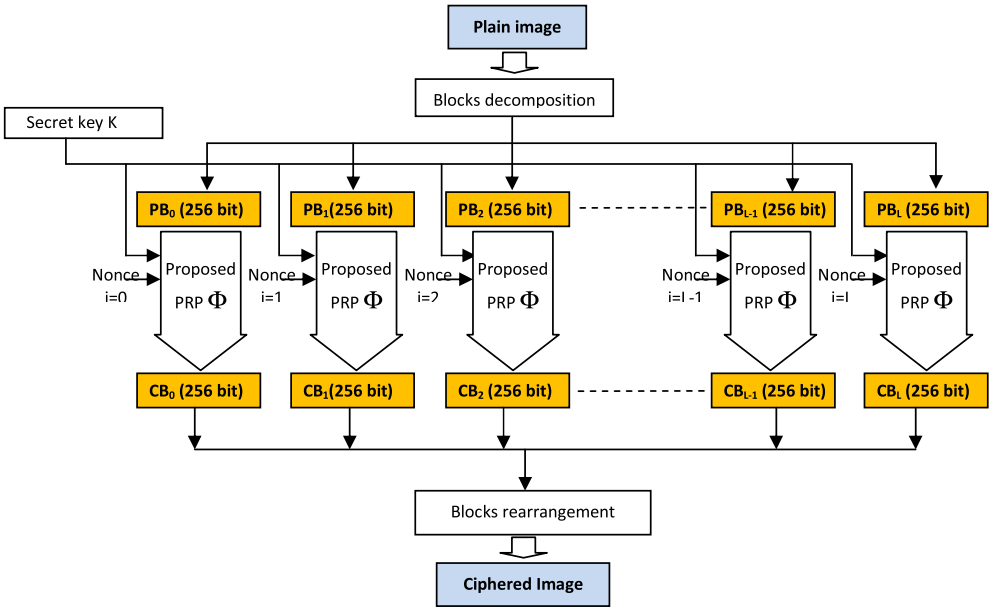

Fig. 2. Proposed parallel image encryption/decryption schema.

imperatively the original plain-image. Decryption is also parallelizable, and the same code or circuit that performs encryption can also perform decryption without any supplementary modifications.

5. Security analysis and experimental results

In this section, several experiments and tests are performed to evaluate the security and robustness of the proposed approach. We first analyze the security aspects of the proposed PRP with respect to the randomness and sensitivity criterions. Then, the second experiments part evaluates the different security aspects of the proposed cryptosystem using statistical tests, including its robustness against major cryptanalysis attacks classes.

5.1. Analysis of the PRP performances

As stated in Section 4.1, a secure PRP must satisfy two main criterions: to be indistinguishable from a random permutation, and to be very sensitive to small variations of its inputs. The former criterion is shown experimentally by evaluating the pseudo-randomness degrees of the PRP's output during enciphering of plain-images. The later criterion is demonstrated by evaluating the sensitivity degree of the PRP's output with respect to small variations of the three inputs: plain-block, nonce and the secret key.

Sensitivity to plain-block variation is measured by comparing the PRP's outputs (in term of percentage of different bits) when using a fixed key and fixed nonce values with the 256 possible different one-bit-modified copies of a given plain-block, and taking the averaged result on 10^6 such experiment performed using a set of 10^6 random generated plain-block. For any plain-block PB, if PB' is its modified version by flipping the ith bit then the corresponding percentage of difference d_i is computed by:

$$d_i = \left(H\left(\Phi(\mathrm{PB}),\ \Phi\left(\mathrm{PB}'\right)\right)\Big/256\right)*100\%,\quad \forall 1 \le i \le 256 \text{ and } \mathrm{PB}' = \mathrm{PB}\ xor\ 2^{i-1} \tag{5}$$

when H is the hamming distance between two 256 bit blocks. The average of bit difference percentage is then computed by taking the average of d_i values for the set of 10^6 different plain-blocks used for experimentation (generated randomly). Same experiment is performed for the nonce input with a fixed plain-block and a fixed key (using 10^6 random generated nonce and measuring bit difference with the 32 possible one-bit-modified copies), and for the key input with fixed nonce and fixed plain-block (using 10^6 random generated key and measuring the bit difference each time with the 128 possible one-bit-modified copy). Obtained results for the three experiments are illustrated in Fig. 3(a), (b) and (c). It is clear that averaged bit difference is always close to the optimal value (50%) for the three inputs which proof that the PRP's output is very sensitive to any elementary one bit modification of any input. This characteristic ensures the robustness of the proposed PRP against both linear and differential cryptanalysis, and grantee that avalanche criterion is perfectly satisfied.

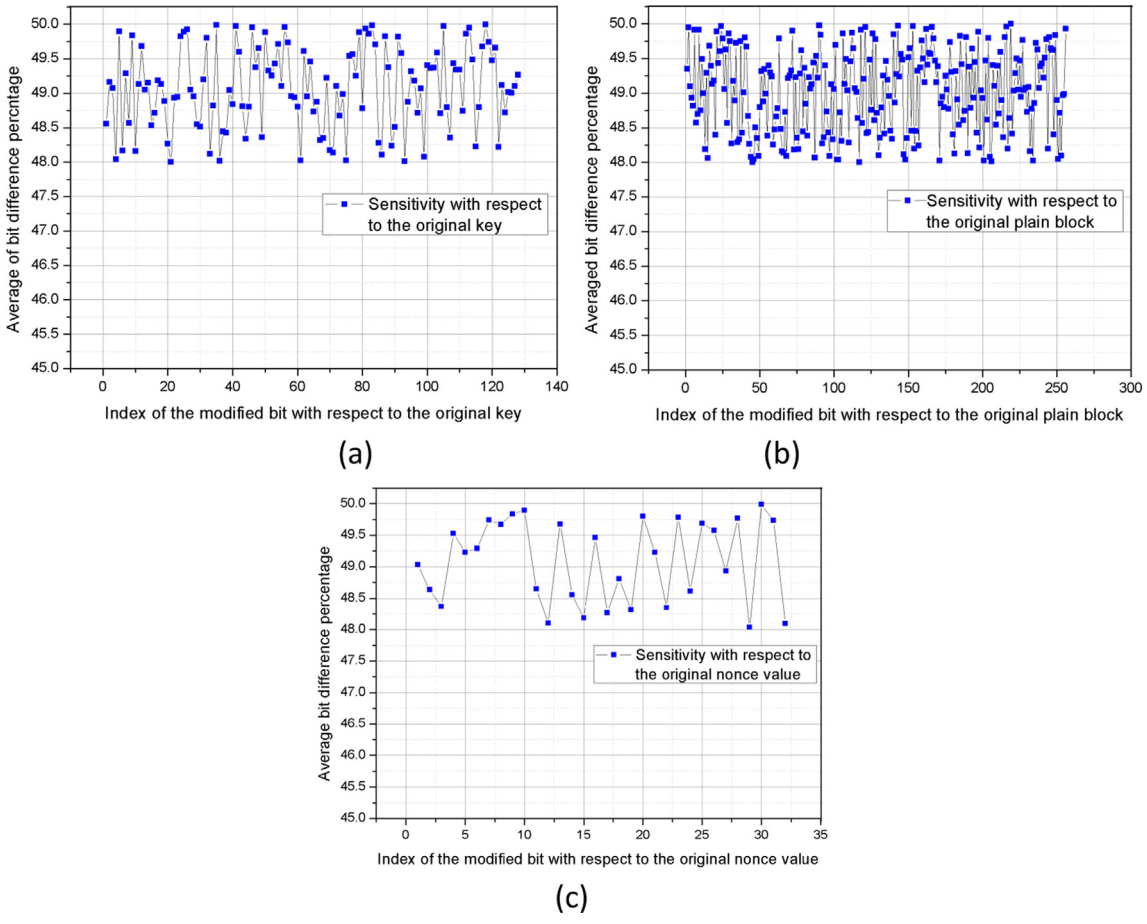

Fig. 3. Sensitivity of the proposed PRP to elementary input's changes: (a) key sensitivity, (b) plain-block sensitivity and (c) nonce sensitivity.

5.2. Security analysis of the proposed image's parallel cryptosystem

In order to evaluate performances and security of the proposed cryptosystem, different statistical tests and measurements are performed using three 512 × 512 gray-scale images: Lena, Peepers and boat illustrated in Fig. 4(a), (b) and (c). Corresponding ciphered images using a 128 bit random key are presented in Fig. 4(e), (f) and (g). The following sections illustrate different obtained results with respect to several security aspects.

5.2.1. 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. We can see from Fig. 5 that histogram of the three ciphered images is uniform and so no statistical attack can reveal any information about the plain-image without knowledge of the secret key.

5.2.2. Information entropy and image correlation

According to Shannon's theory, information entropy is one of the main randomness measurements of information. High entropy values express a high degree of randomness and for any message coded on m bit, the upper bound of the entropy is m. Since gray-level images are coded on 8 bits, the optimal entropy value is 8, and the entropy of ideally random image should be very close to this bound. The entropy is calculated using the following formula:

$$H = -\sum_{i=0}^{2^m-1} p_i \mathrm{Log}_2(p_i) \tag{6}$$

when p_i is the probability distribution of different gray-level values of an image (from 0 to 255) that can be approximated by their frequency.

Table 1 illustrates different entropy values obtained for plain and ciphered images. The results are also compared to those obtained by two existing CA-based and chaos-based cryptosystems proposed in Refs. [31,32]. It is clear that ciphered images has near to optimal entropies and so has random a good random properties that prevent any statistical cryptanalysis attacks since no significant information can be derived from the ciphered image without the secret key.

Another important statistical test that permits to show the high quality of the diffusion and confusion properties of the proposed cryptosystem is correlation among images pixels. Since digital images have generally redundant content, they present a strong correlation between adjacent pixels unlike ciphered images that should have a near to zero correlation to avoid any possible information deduction that lead to a possible statistical attack. To perform a pixel's correlation test on an image, a set of 20,000 random pairs of adjacent pixel is chosen (in vertical, diagonal and horizontal directions) and the correlation coefficient is then calculated and plotted in a correlation diagram using the formula stated in Ref. [33]. As an example, Fig. 6 illustrates the correlation distribution of horizontally, vertically and diagonally adjacent pixels for the plain and ciphered versions of the Lena image. Table 2 List the corresponding correlation values calculated for the three used images Lena, Peppers and Boat.

5.2.3. Key sensitivity

An important security aspect of block-based cryptosystems is to be resistant against differential and linear attacks. Such aspect can be satisfied if the encryption result is very sensitive to small elementary variations of the used secret key. To evaluate the key sensitivity degree of the proposed approach, the following experiment is performed: for a given plain-image, enciphering using a random key K is first performed to obtain a reference ciphered image. Then, 128 one-bit modifications are performed on each of the 128 different bits of K followed by enciphering of the plain-image using the resulting modified key. We can then compute the percentage of difference between the resulting ciphered-image and the reference ciphered-image obtained using the original key K using the following equation:

$$\mathrm{diff} = \left(\frac{1}{512*512}\sum_{i=1}^{512}\sum_{j=1}^{512} sg\left(C[i,j] - C'[i,j]\right)\right)*100 \tag{7}$$

when C is the reference ciphered image, C' is the resulting ciphered-image (using the modified key), and sg is the function defined by:

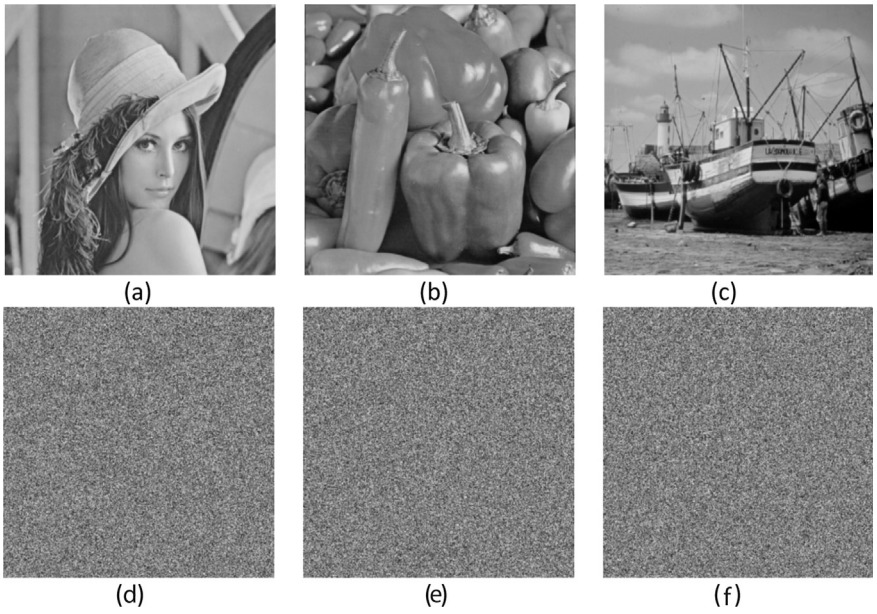

Fig. 4. Gray-level images used for analyzing the cryptosystem: (a) Lena, (b) Peeper and (c) Boat, and Corresponding ciphered images (e), (f) and (g) respectively.

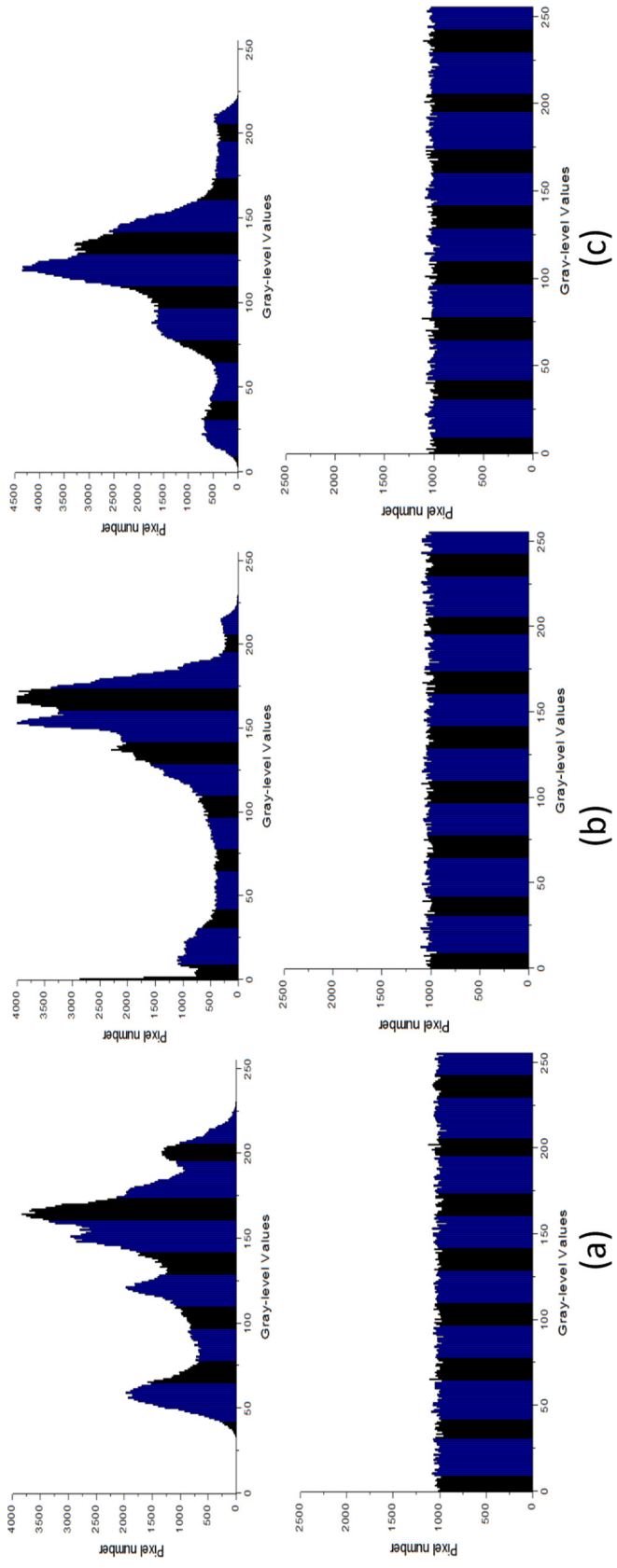

Fig. 5. Histograms of plain/ciphered images: (a) Lena, (b) Boat and (c) Peepers.

Table 1
Entropy of plain/cipher images for proposed and existing cryptosystems.

Image	Plain-image	Ciphered-image	Ref. [32] (ciphered)	Ref. [3] (ciphered)
Lena	7.2103	7.9999	7.9368	7.9997
Boat	7.3415	7.9998	7.9643	7.9957
Peppers	7.0325	7.9987	7.9487	7.9961

Table 2
Correlation coefficients of adjacent pixels of different images.

Image	Plain			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9832	0.9725	0.9620	0.0012	0.0031	0.0022
Peppers	0.9691	0.9789	0.9601	0.0037	−0.0020	0.0079
Boat	0.9701	0.9821	0.9510	0.0029	0.0049	0.0027

$$sg(x) = \begin{cases} 1 & if x \neq 0 \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

This experiment was performed using 1000 different random keys, and the averaged results are illustrated by Fig. 7(a). We can easily notes that difference's rates are very high for each bit position modification and so the enciphering key is very sensitive to modifications. Another way to show key sensitivity is to compare the deciphered image using a wrong key (that differ only on one bit to the correct one) with the correct deciphered key and compute the percentage of difference between the correct and the wrong decrypted images. Results of this experiments using Lena image are presented in Fig. 7(b) and proof that decryption is also very sensitive to small key variations.

6. Performances analysis and comparison

As mentioned above, the main advantage of the proposed parallel approach is that it permits very high encryption/decryption rates with respect to existing sequential models due to parallelized nature of the schema. We have implemented the cryptosystem using MMX assembly instruction on Delphi 6 programming environment and experimenting using an i7-2600 3.40 GHz platform. Multi-threading model is used to exploit the inherent parallelism by decomposing the plain-images in different sets of blocks that are ciphered independently by different threads. The resulting performances outperform almost all sequential approaches, as illustrated by results reported in Table 3 comparing the proposed schema to chaotic confusion/diffusion approach [33], existing CA-based approach [32], block-based AES CBC and CTR operating mode and A5/1 algorithm.

We note that obtained encryption/decryption rates depend on the used platform and the number of possible threads and processors. Fig. 8 illustrate the evolution of encryption time with respect to the number of used threads for a given 2900 × 2500 gray-scale image. Upper bounds of the encryption speed is only limited by the platform characteristics and the number of possible computation units. If hardware implementation is used, an additional level of parallelism can be exploited since cellular automatons can ran asynchronously for each block which will lead to a further enhancement of the overall encryption/decryption performances.

7. Conclusion

The present paper proposes a novel image encryption schema that is completely parallelizable unlike existing models. The task of enciphering/deciphering of any plain-image can be executed in

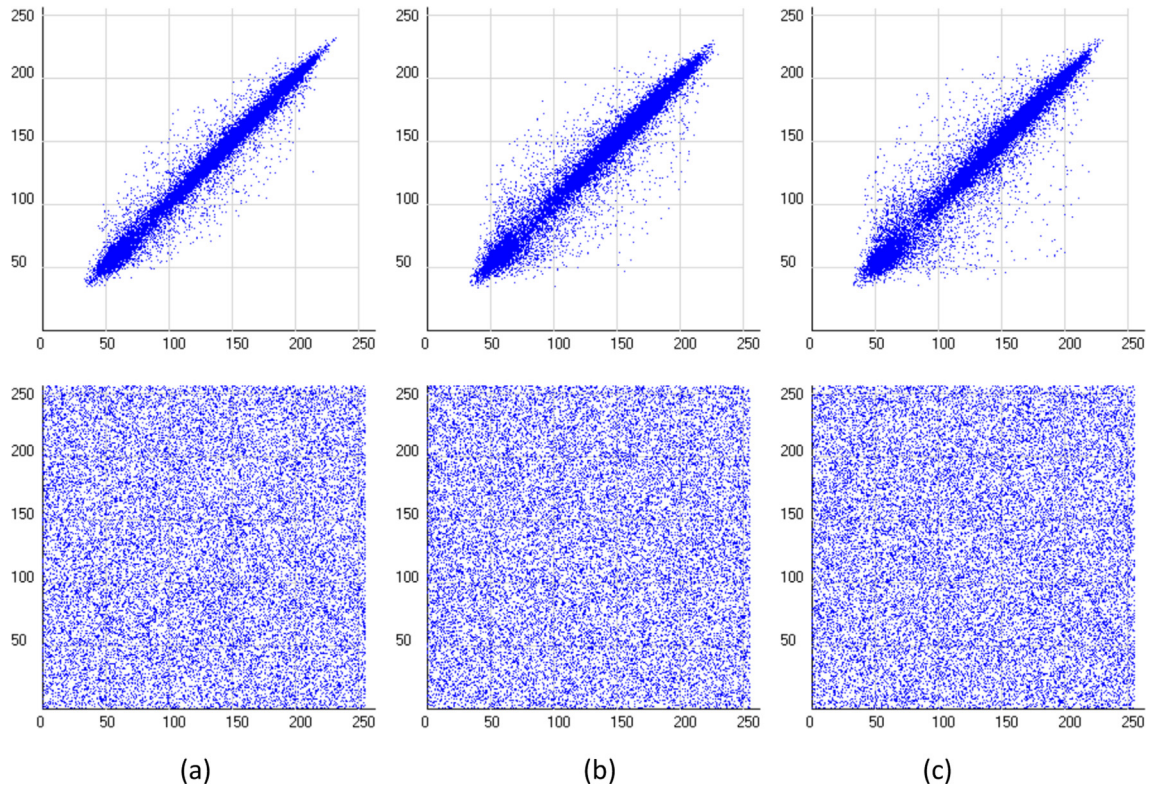

Fig. 6. Correlation distribution for plain/ciphered Lena image: (a) horizontal, (b) vertical and (c) diagonal.

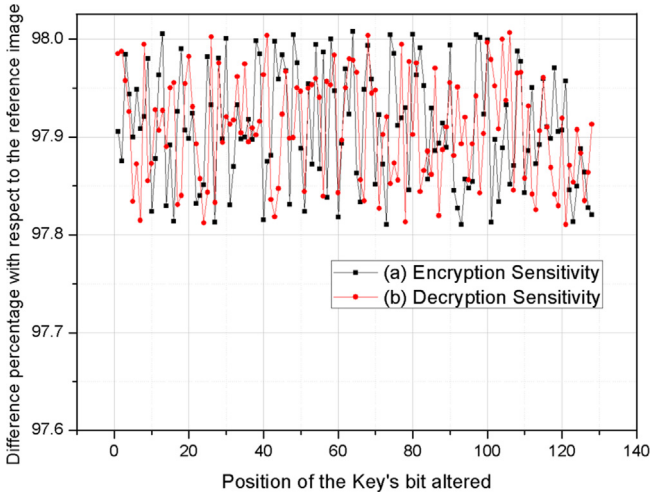

Fig. 7. Secret key sensitivity to elementary one-bit modifications: (a) encryption sensitivity; (b) decryption sensitivity.

Table 3
Encryption time performances comparison for different image sizes.

Plain-image size	Encryption time (in ms)					
	Ref. [32]	Ref. [33]	AES (CBC)	AES (CTR)	A5/1	Proposed
256 ko	1785	3352	1212	987	1456	761
1 Mo	7234	13,124	4431	3891	4321	3102
4 Mo	14,612	26,523	9025	7625	8278	6320

parallel using multiple threads/processors without affecting the security and coherence of the cryptosystem. Such parallelism has been made possible by defining an extended new PRP using reversible second-order automata mechanism. The PRP can be applied independently on each image block such that encryption of any block relay only on its content and its index in the image without the need for anterior enciphered block information. Unlike existing CA-based and classical block based schemas, no block enchaining is needed to solve the ECB encryption problem. The security of the proposed approach is induced by the dynamical and chaotic behavior of RCA, and their high sensitivity to small initial conditions and evolution key variations.

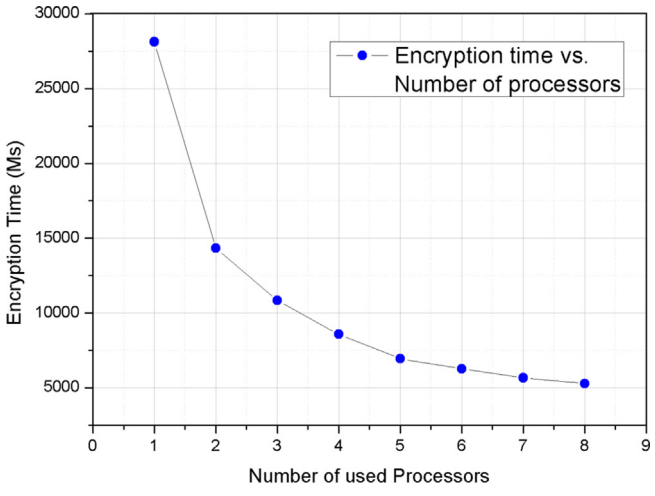

Fig. 8. Encryption time with respect to the used threads (on an 8 processors machine).

The two main advantages of the proposed approach are first the parallel mode of operation for encryption and decryption that lead to great performances enhancement on multi-processor platforms, and second, the selective area deciphering such that any specific image's area can be deciphered without knowledge of the full ciphered-image. The approach is also very robust to data deterioration or nosy transmission, since any ciphered-data corruption will affect only the corrupted block without influencing the decryption result of prior or posterior blocks. Obtained results show the robustness and high performance degree of the proposed schema even with a non-optimized code. We assume that better performances can be achieved if hardware implementation is used.

References

[1] X. Wang, J. Zhao, H. Liu, A new image encryption algorithm based on chaos, Opt. Commun. 285 (2012) 562–566.
[2] M. Francois, T. Grosges, D. Barchiesi, R. Erra, A new image encryption scheme based on a chaotic function, Signal Process. Image Commun. 27 (2012) 249–259.
[3] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simulat. 17 (7) (2012) 2943–2959.
[4] R.S. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun. 284 (22) (2011) 5290–5298.
[5] S. Wolfram, Random sequence generation by cellular automata, Adv. Appl. Math. 7 (2) (1986) 123–169.
[6] M. Szaban, F. Seredynski, P. Bouvry, Collective Behavior of Rules for Cellular Automata-Based Stream Ciphers, Evolutionary Computation, in: CEC.IEEE Congress, July 16–21, 2006, pp. 179–183.
[7] S.A. Chatzichristofis, A.D. Mitzias, G.C. Sirakoulis, S. Yiannis, A novel cellular automata based technique for visual multimedia content encryption, Opt. Commun. 283 (21) (2010) 4250–4260.
[8] M. Tomassini, M. Sipper, M. Perrenoud, On the generation of high quality random numbers by two-dimensional cellular automata, IEEE Trans. Comput. 49 (10) (2000) 1146–1151.
[9] M. Seredynski, P. Bouvary, Block cipher based on reversible cellular automata, New Gener. Comput. 23 (2005) 245–258. Ohmsha Ltd and Springer.
[10] Peter Anghelescu, Silviu Ionita, Emil Safron, Block Encryption Using Hybrid Additive Cellular Automata, in: 7th International Conference on Hybrid Intelligent Systems, IEEE, 2007.
[11] A. . Ray, D. Das, Encryption algorithm for block ciphers based on programmable cellular automata, Inf. Process. Manag. (2010) 269–275.
[12] C. Cokal, E. Solak, Cryptanalysis of a chaos-based image encryption algorithm, Phys. Lett. A 373 (2009) 1357–1360.
[13] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image Vis. Comput. 27 (2009) 1371–1381.
[14] N. Pareek, V. Patidar, K. Sud, Discrete chaotic cryptography using external key, Phys. Lett. A 309 (2003) 75–82.
[15] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, Int. J. Bifurcat. Chaos 14 (2004) 3613–3624.
[16] J. Shen, X. Jin, C. Zhou, A color image encryption algorithm based on magic cube transformation and modular arithmetic operation, Lect. Notes Comput Sci. 3768 (2005) 270–280.
[17] X. He, Q. Zhu, P. Gu, A new chaos-based encryption method for color image, Lect. Notes Artif. Int. 4062 (2006) 671–678.
[18] Jin Jun, Zhi-Hong Wu, A secret image sharing based on neighborhood configurations of 2-D cellular automata", Opt. Laser Technol. 44 (3) (2012) 538–548.
[19] W. Zhang, J. Peng, H. Yang, P. Wei, A Digital Image Encryption Scheme Based on the Hybrid of Cellular Neural Network and Logistic Map, in: Advances in Neural Networks, Lecture Notes in Computer Science vol. 3497, 2005, pp. 860–867.
[20] L. Cappellari, S. Milani, C. Cruz-Reyes, G. Calvagno, Resolution scalable image coding with reversible cellular automata, IEEE Trans. Image Process. 20 (5) (2011) 1461–1468.
[21] L. Rosin Paul, Image processing using 3-state cellular automata, Comput Vis. Image Understand 114 (7) (2010) 790–802.
[22] Claude Kauffmann, Nicolas Piché, N.D. Seeded, Medical image segmentation by cellular automaton on GPU, Int. J. Comput. Assist. Radiol. Surg. 5 (3) (2010) 251–262.
[23] Rong-Jian Chen, Shi-Jinn Horng, Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata, Signal Process. Image Commun. 25 (6) (2010) 413–426.
[24] Z. Eslami, J. Zarepour Ahmadabadi, A verifiable multi-secret sharing scheme based on cellular automata, Inf. Sci. 180 (15) (2010) 2889–2894.
[25] J. Lang, Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation, Opt. Laser Eng. 50 (7) (2012) 929–937.

[26] Sudheesh K. Rajput, Naveen K. Nishchal, Image encryption and authentication verification using fractional nonconventional joint transform correlator, Opt. Laser Eng. 50 (10) (2012) 1474–1483.
[27] Z. Liu, M. Gong, Y. Dou, F. Liu, S. Lin, M. Ashfaq Ahmad, et al., Double image encryption by using Arnold transform and discrete fractional angular transform, Opt. Laser Eng. 50 (2) (2012) 248–255.
[28] S. Banerjee, S. Mukhopadhyay, L. Rondoni, Multi-image encryption based on synchronization of chaotic lasers and iris authentication, Opt. Laser Eng. 50 (7) (2012) 950–957.
[29] T. Toffoli, N. Margolus, Invertible cellular automata: a review, Phys. D. 45 (2001) 229–253.
[30] S. Wolfram, A New Kind of Science, Wolfram Media, 2002, ISBN 1-57955-008-8, pp. 437–440.
[31] M. Bellare, P. Rogaway, Chapter 3: Pseudorandom Functions, Introduction to Modern Cryptography, retrieved 30.09.07.
[32] A.A. Abdo, S.G. Lian, I.A. Ismail, M. Amin, H. Diab, A cryptosystem based on elementary cellular automata, Commun. Nonlinear Sci. Numer. Simulat. 18 (1) (2013) 136–147.
[33] G. Chen, Y.B. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solit. Fract. 12 (2004) 749–761.
[34] M. Luby, C. Rackoff, How to construct pseudorandom permutations from pseudorandom functions, SIAM J. Comput. 17 (2) (April 1988) 373–386.
[35] Mohamed Amin, Osama S. Faragallah, Ahmed A. . Abd El-Latif, A chaotic block cipher algorithm for image cryptosystems, J. Commun. Nonlinear Sci. Numer. Simulat. 15 (11) (November 2010) 3484–3497.
[36] Mohamed Amin, Ahmed A. . Abd El-Latif, Efficient modified RC5 based on chaos adapted to image encryption, J. Electron. Imaging 19 (1) (Jan 2010).