Nonlinear Dyn (2016) 84:715–732
DOI 10.1007/s11071-015-2521-3

ORIGINAL PAPER

Fast and efficient randomized encryption scheme for digital images based on Quadtree decomposition and reversible memory cellular automata

Amina Souyah · Kamel Mohamed Faraoun

Received: 7 August 2015 / Accepted: 19 November 2015 / Published online: 27 November 2015

Abstract In recent years, the efficiency of cellular automata-based image cryptosystems has drawn a great interest to deal with the problematic of fast and highly secure image encryption. In this paper, we present a novel image encryption scheme that combines image's quadtree decomposition approach with reversible memory cellular automata mechanism. The proposed scheme provides high sensitivity to plain image, key bit alteration besides its competitive speed performance. With respect to exiting schemes, the proposed one permits to reach high sensitivity degrees without the need for multiple confusion/diffusion rounds. Additionally, the scheme is extended to handle randomized encryption mode, so becomes secure against chosen-plaintext attacks. Experimental tests and extensive security analysis have been performed to demonstrate security and time efficiency of the proposed scheme, and show its suitability for designing real-time and secure image's cryptosystems.

Keywords Image encryption · Memory cellular automata · Quadtree decomposition · Randomized encryption

A. Souyah · K. M. Faraoun (✉)
Computer Science Department, Djilalli Liabes University, Sidi Bel Abbès, Algeria
e-mail: kamel_mh@yahoo.fr

A. Souyah
e-mail: souyah.UDL@gmail.com

1 Introduction

Recently, the ever-increasing demand of secure image storage and transmission has become more prevalent under the rapid enlargement and development of the open networks. Real-time multimedia applications are also made possible with the advancement of mobile communication technologies. However, in public networks as the Internet, there is a potential risk of making sensitive information such as military and medical images vulnerable to unauthorized interceptions. Development of robust cryptographic schemes is thus so essential to the provision of multimedia security. For textual information, this can be handled with the direct application of several well-established encryption schemes as DES [1], IDEA [2] and AES [3]. However, the case of multimedia information such as image especially in real-time communications is different and hard to be accomplished by the revealed traditional schemes, this is because of the large computational time from a part besides the intrinsic properties of images such as large data size, bulk data capacity, strong pixel correlation and high redundancy, which decrease the encryption performance since traditional encryption schemes are not adapted to deal with modern multimedia requirements. Recently, many works have been devoted to investigate better solutions for image encryption in many concerned aspects regarding security, complexity and speed, especially under the scenario of on-line communications. In particu-

lar, application of dynamical systems for multimedia encryption is one of the main actual research directions. A new approach is suggested in this paper to design a fast and secure image encryption scheme as a solution to the aforementioned challenges in protecting image content. The main idea behind the proposed work is to encipher the image using a quadtree decomposition strategy in combination with reversible memory cellular automata mechanism, in order to construct an efficient symmetric encryption scheme for digital images. The quadtree strategy is a well-known hierarchical decomposition scheme that has been utilized in several image processing areas including image compression [4,5], image segmentation [6] and feature calculation [7]. In the present work, the quadtree decomposition strategy applies successive subdivisions to the target image into four equal quadrants (sub-images), and the size of a quadrants to be encrypted is decreased in each subdivision level. Such subdivision is continued in deep until reaching the lowest size limit that is equivalent to sub-image of 4×4 pixels block. Rather than encrypting the image using fixed block size as conventional block and stream ciphers do, we use a variable block size with hierarchical mapping in order to achieve higher security levels and avoid conventional operating modes problems. Such approach gives an implicit handling of the plain image sensitivity due to the intrinsic chaotic properties of cellular automata. Confusion and diffusion properties are verified without the need of iterated rounds, and an efficient mechanism of sub-keys generating is implemented using nonuniform cellular automata approach proposed in [8]. Besides that, the security of the proposed scheme is based on the unfeasibility of inverting a memory K-order cellular automata without knowledge of the used transition rules and at least K distinct consecutive configurations. By exploiting the high sensitivity to the plain image bit modification (i.e., diffusion), a randomized encrypting is introduced in which the use of the same key to encipher the same plain image gives in each time a different ciphered image. Such mode of enciphering which is named probabilistic encryption or nondeterministic encryption is theoretically shown to be semantically secure against chosen-plaintext attack (CPA for short). The aim of the proposed randomization technique is to provide a full probabilistic encryption without the use of any additional random data such as initialization vectors (IVs) or nonce that are generally used by conventional randomized schemes.

The remaining of the paper is organized as follows: Sect. 2 summarizes several works related to recent existing image encryption schemes. Section 3 gives essential theoretical preliminaries and definitions about cellular automata and reversible memory cellular automata, while Sect. 4 gives a detailed description of the proposed scheme. In Sect. 5, efficiency and security analysis of the scheme are performed according to several experiments and statistical measurements. Finally, conclusion is given in Sect. 6.

2 Dynamical systems for image encryption: related works

Recently, image encryption scheme, which has the aim to create a best compromise between high security and convenient speed performances, has attracted the attention of many researchers who have suggested in this way different schemes. The properties of confusion and diffusion are hard to be achieved using conventional algorithms such as DES, IDEA and AES, due to the huge amount of data carried by digital images and their specific characteristics. In this way, special enhancements may be carried out to handle such image's features, since the task of image encryption has its own requirements which differ from those of textual and usual binary data.

Among the recent works toward multimedia encryption, application of dynamical systems approaches gives promising proofs when it is used to design secure and efficient image encryption schemes. The two main paradigms of dynamical systems that have been extensively used to design image encryption schemes are: chaotic systems and discrete cellular automata models. Using the former paradigm, several chaos-based image encryption schemes were proposed, implemented and analyzed during the last decades, while several researchers noted that essential properties of dynamical chaotic systems have their corresponding equivalents in conventional cryptosystems [9,10]. Precisely, the confusion and diffusion properties of secure cryptosystems are explicitly and respectively related to the ergodicity and the high sensitivity to initial/control parameters of chaotical systems [11]. The general architecture of chaos-based image encryption schemes contains mainly two phases: confusion and diffusion. The confusion phase is generally achieved by applying permutation on the image's pixels

and shuffling the whole image using two-dimensional chaotic map, while the diffusion phase proceeds to modify pixel's values individually using a discrete version of the chaotic orbit generated using the secret key as initial condition of the system. Several variants and improvements in the aforementioned architecture were proposed in the literature, including combination of permutation–diffusion rather than using them as two separate stages for the purposes of accelerating the encryption and reducing duplicated scanning effort as proposed in [12]. Due to the superior features of bit-level operations, bit-level permutation has been also proposed in [13,14], leading to advanced improvement in both confusion and diffusion properties. An improved diffusion strategy was also proposed in [15] and [16] to meet a sufficient degree of security with fewer overall encryption rounds. A mixture strategy of either chaotic maps or introduction of other concepts as CA, DNA and genetic algorithms was recently proposed in [17–19] to achieve higher level of security with acceptable speed. In [35], the authors used two-dimensional logistic maps complicated basin structures and attractors to build a permutation–substitution-based cryptosystem for digital images, having very acceptable statistical characteristics and security levels, while the authors of [36] achieved similar competitive performances using two combined one-dimensional chaotic maps leading to larger chaotic ranges and better chaotic behaviors compared with their seed maps. A new variant has been proposed later in [37] using three-dimensional chaotic maps, in order to enlarge the key space and to defeat some common cryptanalysis attacks. However, most of chaotic-based image encryption schemes are unable to achieve satisfactory enciphering rates with respect to conventional schemes, since a relatively high number of rounds are required to reach an acceptable level of confusion/diffusion. In addition, a lot of such schemes were successfully cryptanalyzed and sometimes completely broken [39–41].

The second class of dynamical systems that has been used to encipher digital images is the cellular automata (CA for short) paradigm. Cellular automata that have been invented by Von Neumann [20] are considered as good candidate for designing fast and secure cryptosystems due to their major features including simplicity, regularity, masking of generation easily, silicon-area utilization and locality of interactions [21]. Since then, several cryptosystems have been designed to handle image encryption using CAs. In [22,23], elementary CAs with periodic boundary and unity attractors were used and led to good performances with satisfactory security level. Other improvements were suggested later in [24] using class of fractals, in [25] using SCAN-CA patterns and in [26] using recursive cellular automata substitutions. Works in [27–29] proposed stream-based approaches to deal with image encryption according to the Vernam model by using combination of several transition rules to generate secure pseudorandom sequences that were combined with the target image. Unlike CA's stream-based approaches, only few block-based ones have been proposed, like the work presented in [38] using second-order CAs to build a cryptographically secure pseudorandom permutation and use it in a parallel mode to encipher digital color images. While most of existing CA-based image encryption schemes are stream-based approaches, they are almost vulnerable to the known-plaintext attacks unless a specific mechanism of key randomization is used. While stream ciphers ensure high encryption rates, their security assumptions rely only on the statistical characteristics of the generated sequences. Hence, they fail to provide strong security requirements. Additionally, even if the mentioned schemes provide high sensitivity to elementary alterations of the secret key, their sensitivity to the plain image is poorly handled for which their vulnerability to several kinds of chosen plain-text attacks is exposed.

3 One-dimensional memory cellular automata

3.1 Elementary cellular automata

One-dimensional elementary cellular automata are special class of discrete dynamical systems formed by a finite one-dimensional array of N identical objects named cells. Each cell which is denoted by $<i>$ is characterized by its state S_i^t at time t that is defined on a finite state's set S. A cellular automaton evolves deterministically in discrete time steps, changing the states of all cells according to a local transition rule F that defines the new state S_i^{t+1} of each cell $<i>$ using its previous state and the states of its corresponding neighbors. A cell's neighborhood V_i is a specific selection of cells that are relatively chosen according to the i's position of the cell considered to be updated and its r left and right neighbors, including the cell itself. In general, a symmetric neighborhood is defined using the

aforementioned parameter r noted a radius, this later specifies the set of positions for the $2r+1$ neighboring cells by:

$$NB(i) = \{i-r, i-r+1, \ldots i-1, i, i+1, i+2, \ldots, i+r-1, i+r\} \quad (1)$$

To deal with finite size automatons boundaries, the cells of the array are concatenated together in a cyclic form to consider a periodic boundary condition. The transition rule F is then applied to each neighborhood of a given cell $<i>$ to compute and update its state to S_i^{t+1} according to the following equation:

$$S_i^{t+1} = F(V_i) = F\left(S_{i-r}^t, S_{i-r-1}^t, \ldots, S_i^t, \ldots\ldots S_{i-1+r}^t, S_{i+r}^t\right) \quad (2)$$

When the set S of possible states is equal to $\{0, 1\}$, corresponding CAs are named binary cellular automata. In such case, the transition rule is defined by the binary representation of the possible new state's values corresponding to all possible 2^{2r+1} neighborhood configurations on $2r+1$ bits, so the number of possible transition rules for a binary one-dimensional CA is then equal to $2^{2^{2r+1}}$. A configuration C^i is defined by the states of all the automaton cells by $C^i = \left(S_0^t, S_1^t, \ldots, S_{N-1}^t\right)$, while the transition rule F is extended to the global transition map Φ that describes the dynamic evolution of the CA's configurations by $C^{t+1} = \Phi(C^t)$, starting from any given initial configuration C^0. If Φ is bijective, then the corresponding CA is reversible and the backward evolution becomes possible using the inverse global transition map Φ^{-1} [30].

3.2 Memory cellular automata

Within conventional paradigm of cellular automata, we consider that the state of each cell $<i>$ at time $t+1$ is only depending on the states of its neighbor cells at time t. Nevertheless, one can consider CAs for which the state of each cell at time $t+1$ depends also on corresponding states at previous time steps $t-1, t-2, \ldots$, etc. Such class of CAs is named memory cellular automata (MCA for short) [31], having the interesting property to be reversible whatever is the used transition rule F. Specifically, in a Kth order MCA, states of new configuration C^{t+1} depend on K previous ones $C^t, \ldots, C^{t-K}$. Using K different transition rules $F_1, F_2, \ldots, F_K$, each state S_i^{t+1} of the configuration is defined by:

$$S_i^{t+1} = F_1\left(V_i^t\right) \oplus F_2\left(V_i^{t-1}\right) \oplus \cdots \oplus F_K\left(V_i^{t-K+1}\right) \quad (3)$$

where V_i^t denotes the neighborhood of the cell $<i>$ at time step t. Accordingly, the global transition map can then be defined on the set C of possible configurations by:

$$\begin{aligned} &\Psi : C \times C \cdots \times C \to C \\ &C^{t+1} = \Psi\left(C^t, C^{t-1}, \ldots, C^{t-k+1}\right) \\ &= \Phi_1\left(C^t\right) \oplus \Phi_2\left(C^{t-1}\right) \\ &\oplus \ldots . \oplus \Phi_K\left(C^{t-k+1}\right) \end{aligned} \quad (4)$$

where $\Phi_1, \Phi_2, \ldots, \Phi_{K-1}, \Phi_K$ are global transition maps corresponding to the transition rules $F_1, F_2, \ldots, F_K$.

In order to ensure reversibility of a given MCA, we can easily show that it suffices that the global transition map Φ_K be equivalent to the identity function ($\Phi_K\left(C^i\right) = C^i \forall i$). Hence, the MCA defined by the following equation:

$$C^{t+1} = \Phi_1\left(C^t\right) \oplus \Phi_2\left(C^{t-1}\right) \oplus \cdots \oplus \Phi_{K-1}\left(C^{t-K+2}\right) \oplus C^{t-K+1} \quad (5)$$

is reversible for any set of the transition functions and admits as a reverse the MCA defined by the following equation:

$$B^{t+1} = \Phi_{K-1}\left(B^t\right) \oplus \Phi_{K-2}\left(B^{t-1}\right) \oplus \cdots \oplus \Phi_1\left(B^{t-K+2}\right) \oplus B^{t-K+1} \quad (6)$$

where the B_i's denotes the possible configurations of the inverse MCA.

The proof of this proposition is trivial. Let's consider the configurations $(C^{t+1}, C^t, \ldots, C^{t-K+1})$ generated using the Kth order MCA defined by Eq. (5). We show that the configuration C^{t-K+1} can be recovered by applying the MCA defined in Eq. (6) on the configurations $(C^{t+1}, C^t, \ldots, C^{t-K+2})$.

When running the inverse MCA, configurations are handled in reverse order such that: $B^{t-k+2} = C^t, \ldots, B^t = C^{t-K+2}$ and $B^{t+1} = C^{t-K+1}$. Hence, using Eq. (6) we have:

$$B^{t+1} = \Phi_{K-1}\left(B^t\right) \oplus \Phi_{K-2}\left(B^{t-1}\right) \oplus \cdots \oplus \Phi_1\left(B^{t-K+2}\right) \oplus B^{t-K+1}$$

$$
\begin{aligned}
&= \Phi_{K-1}\left(C^{t-K+2}\right) \oplus \Phi_{K-2}\left(B^{t-K+3}\right) \oplus \cdots \\
&\quad \oplus \Phi_1\left(C^t\right) \oplus C^{t+1} \\
&= \Phi_1\left(C^t\right) \oplus \Phi_2\left(C^{t-1}\right) \oplus \cdots \\
&\quad \oplus \Phi_{K-1}\left(C^{t-K+2}\right) \oplus C^{t+1} \qquad (7)
\end{aligned}
$$

By substituting the term C^{t+1} in Eq. (7) using Eq. (5) we obtain:

$$
\begin{aligned}
B^{t+1} &= \Phi_1\left(C^t\right) \oplus \Phi_2\left(C^{t-1}\right) \oplus \cdots \\
&\quad \oplus \Phi_{K-1}\left(C^{t-K+2}\right) \oplus \Phi_1\left(C^t\right) \\
&\quad \oplus \Phi_2\left(C^{t-1}\right) \oplus \cdots \\
&\quad \oplus \Phi_{K-1}\left(C^{t-K+2}\right) \oplus C^{t-K+1} \\
&= \left[\Phi_1\left(C^t\right) \oplus \Phi_1\left(C^t\right)\right] \\
&\quad \oplus \left[\Phi_2\left(C^{t-1}\right) \oplus \Phi_2\left(C^{t-1}\right)\right] \oplus \cdots \\
&\quad \oplus \left[\Phi_{K-1}\left(C^{t-K+2}\right) \oplus \Phi_{K-1}\left(C^{t-K+2}\right)\right] \\
&\quad \oplus C^{t-K+1} = 0 \oplus 0 \oplus \cdots \oplus 0 \oplus C^{t-K+1} \\
&= C^{t-K+1} \qquad (8)
\end{aligned}
$$

Consequently, the MCA defined by Eq. (6) can always recover the configuration C^{t-K+1} from the configurations $(C^{t+1}, C^t, \ldots, C^{t-K+2})$. As a result, it is the inverse of the MCA defined by Eq. (5).

In the present work, reversible memory cellular automat of 4th order are combined with the quadtree image decomposition strategy in order to construct the proposed image enciphering scheme. Corresponding details are presented in the following sections.

4 The proposed encryption scheme

The main purpose of the proposed scheme is to provide a highly secure image encryption mechanism with optimal runtime performance. With respect to existing chaos-based and CA-based schemes, the proposed one uses a specific strategy to deal with image's content, by applying a hierarchical decomposition mechanism which avoids the need for classical operating modes that are based on fixed-length block decomposition or elementary pixel's transformations. In the following, we give details of the enciphering/deciphering schemes with the full description of the used key scheming mechanism. Note that the transition rules used to evolve MCAs in the proposed scheme use a neighborhood radius $r = 3$, so they are coded on 128 bits.

4.1 The image encryption/decryption scheme

In the proposed scheme, the whole plain image is firstly decomposed into four equal quadrants according to the quadtree decomposition strategy. These four blocks are considered as four initial configurations $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$ of a 4th order MCA that is defined according to Eq. (5) from the previous section. The transition rules of this MCA are derived from the secret key using an efficient key scheming mechanism as will be explained in the next section. Before applying the constructed MCA during four iterations, the resulting four new configurations $(C^4)_0$, $(C^5)_0$, $(C^6)_0$ and $(C^7)_0$ (that are blocks of the same size as the plain ones) undergo a mixing phase in order to introduce a sufficient dependence between the image's pixels. These dependencies are amplified later by the MCA evolution mechanism to achieve high plain image sensitivity and avoid the use of several confusion/diffusion rounds. The resulting configurations are then combined to form a new image. The upper left resulting bloc $(C^4)_0$ is recursively subdivided into four equal size quadrants that define new configurations $(C^0)_1$, $(C^1)_1$, $(C^2)_1$ and $(C^3)_1$ for a 4th-order MCA constructed using a new set of transition rules derived from the secret key. This new MCA is iterated to produce new configurations $(C^4)_1$, $(C^5)_1$, $(C^6)_1$ and $(C^7)_1$ that replace the sub-blocks of $(C^4)_0$. This process is repeated recursively by dividing the block $(C^4)_i$ at each level i until reaching the deepest possible level m where the size of the block $(C^4)_m$ is equal to 4×4 pixels. At this level, and since the size is equal to 16 bytes (128 bits), the corresponding block $(C^4)_m$ is simply combined using the Xor operator with the last generated sub-key. According to the presented process, three transition rules (sub-keys) are needed at each level, so the total number of required sub-keys is equal to $3^*m + 1$. Details of the enciphering scheme are presented in Fig. 1.

The mixing phase of pixels uses the simple modular addition operator to introduce related dependencies between the pixels of each initial configuration $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$ (the four sub-quadrants of the plain image). This phase combines the bytes of each configuration in both forward and backward direc-

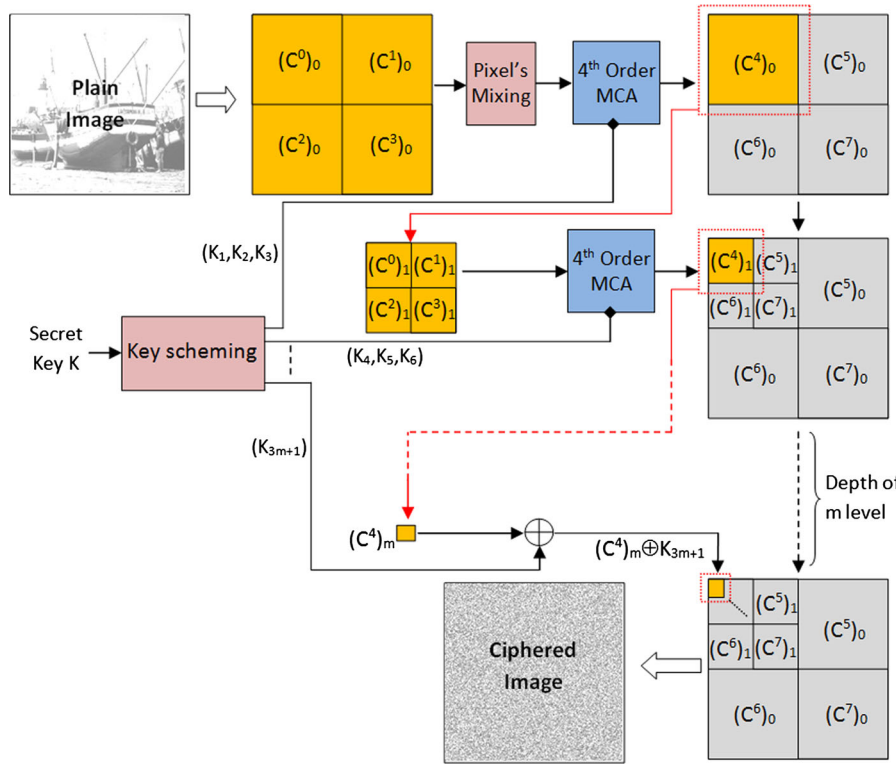

Fig. 1 Descriptive diagram of the proposed enciphering scheme

tions to propagate elementary possible alterations of any single bit of the plain image to several locations of the same configuration. Such propagation is easily amplified later by the MCA evolution mechanism and leads to a high avalanche of changes in the produced ciphered image. This mechanism avoids using several consecutive rounds of confusion as it is generally used by chaotic-based image cryptosystems, so leads to a great enhancement of the enciphering/deciphering runtime. The following pseudo-algorithm illustrates details of the pixels's mixing phase, where each configuration is considered as an array of n bytes A[0…$n-1$]. The same procedure is applied during the deciphering process on the last derived configurations in order to reverse the mixing effect and recover the correct plain image.

By inverting the encryption steps, decryption is performed in a deterministic way to recover the plain image from the ciphered one. After generating the sub-keys using the same scheme, the upper left block of 4×4 pixels is extracted from the ciphered image and combined with the sub-key K_{3m+1} to recover the configuration $(C^4)_m$. This obtained configuration is fed conjointly with the three other 4×4 neighborhood blocks used as configurations $(C^5)_m$, $(C^6)_m$ and $(C^7)_m$, respectively, into the inverse 4th-order MCA that uses the sub-keys K_{3m}, K_{3m-1} and K_{3m-2} (on 128 bit each one) as transition rules. At each reconstruction level, the set of used transition rules matches the set of sub-keys that are derived by the key scheming mechanism. The inverse MCA generates the configurations $(C^0)_m$, $(C^1)_m$, $(C^2)_m$ and $(C^3)_m$ corresponding to the

```
Procedure MixConfiguration;
Input : configuration A      // that can be either be (C^0)_0,(C^1)_0,(C^2)_0 or (C^3)_0
Output : a mixed version of the configuration A
For i:=1 to n-1 do A[i]:=(A[i]+A[i-1]) mod 256;    // mixing in the forward direction
For i:=n-2 dowto 0 do A[i+1]:=(A[i+1]⊕A[i]) mod 256;  // mixing in the backward direction
End
```

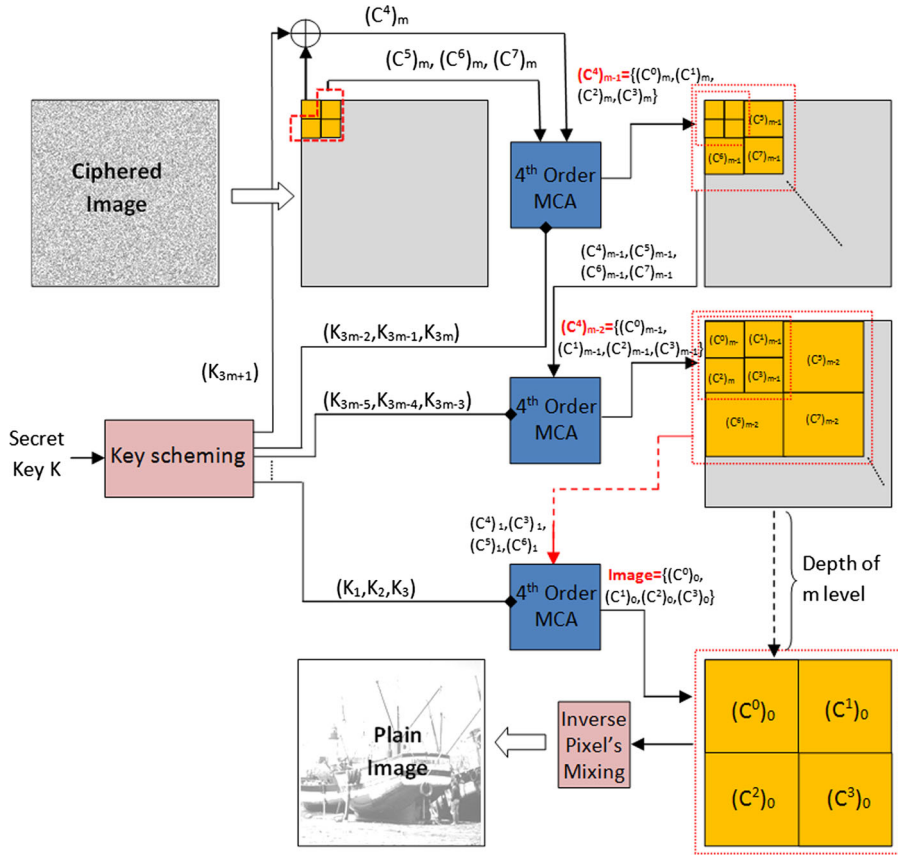

Fig. 2 Descriptive diagram of the proposed decryption scheme

quadtree decomposition depth of the mth level, which gives when combined the configuration $(C^4)_{m-1}$ of the $(m-1)$th level. This process is continued recursively in a bottom-up manner until reaching the configurations $(C^0)_0$, $(C^1)_0$, $(C^2)_0$ and $(C^3)_0$ that undergo finally the inverse pixel's mixing phase and are combined to form the plain image. Figure 2 illustrates the diagram of the decryption process.

4.2 Key expansion mechanism

According to the encryption/decryption scheme, several sub-keys are required during the quadtree decomposition steps to define the transition rules of related MCAs. Since the used MCAs are of 4th order, three different transition rules are used by each MCA, so we need three different sub-keys at each decomposition level. The quadtree decomposition depth depends on the image's size: For a square image of $L \times L$ pixels, the exact number m of decompositions is equal to $[\log_2(L)]-1$. Hence, the number of required sub-keys is equal to $3.([\log_2(L-2)])+1$.

In the proposed scheme, the sub-keys are derived from the secret key K (128 bits) using a nonuniform class of cellular automata that alters transition rules at each position using a pair of control bits extracted from the key. The secret key is considered as an initial configuration, and then a set of four transition rules, namely 90, 105, 150 and 165, is used to update the state of each cell's position and is stored in a table T_i that is updated after each iteration by applying a cyclic left rotation. For a given cell at a position $<i>$, the choice of the rule to apply is made based on an index value derived from the current cell state and the state of its right neighbor, so four possible values are 00, 01, 10 and 11. If we consider T_j the rules table state at iteration j, then the state S_i^{t+1} at the position $<i>$ of a new configuration is determined using the following equation:

$$\begin{aligned} S_i^{t+1} &= T_j\left[S_i^t + 2.S_{i+1}^t\right](V_i) \\ &= T_j\left[S_i^t + 2.S_{i+1}^t\right]\left(S_{i-1}^t, S_i^t, S_{i+1}^t\right) \end{aligned} \tag{9}$$

By evolving the nonuniform CA, each new configuration defines a new generated sub-key. The process

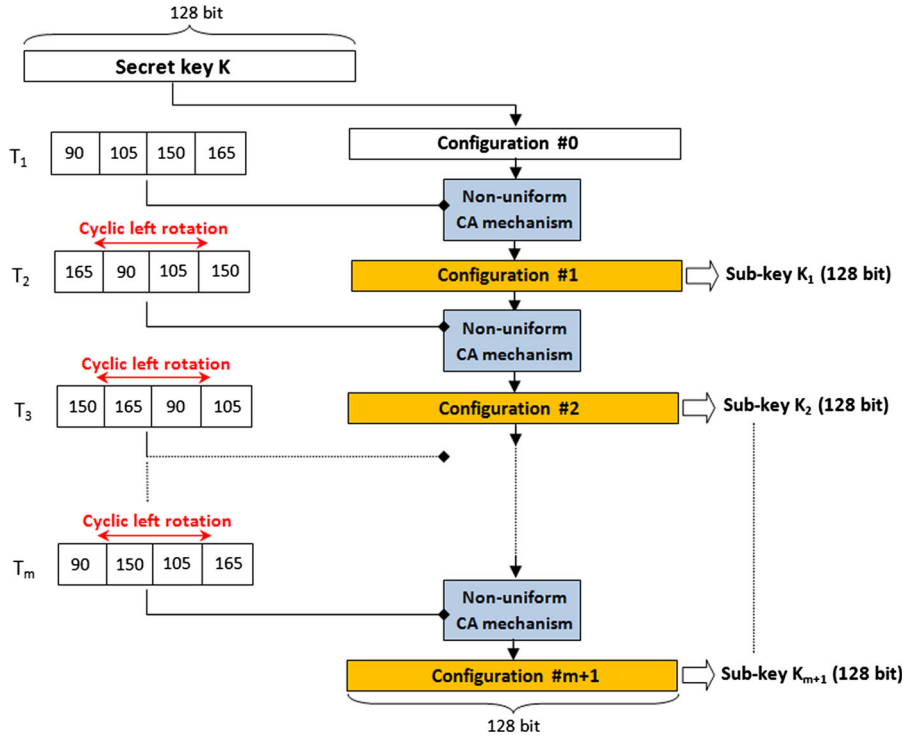

Fig. 3 Key expansion and sub-keys derivation scheme

is continued until all sub-keys are generated. Figure 3 illustrates details of the key expansion mechanism. As illustrated in obtained experimental results, the proposed key scheming ensures a high confusion of the cryptosystem when the resulting ciphered image is high sensitive to elementary bit's flipping of the secret key.

5 Experiments and obtained results

In order to show the robustness and efficacy of the proposed scheme, a number of experiments have been performed using common statistical tests and measurements. In the following we present the corresponding different obtained results, including statistical analysis and differential analysis, which demonstrate the satisfactory security and the robustness of the proposed scheme with respect to several attacks. Experiments are performed using gray scale images of 512×512 pixels, and extension for handling colored images is trivial.

5.1 Statistical analysis

For clarifying robustness of the proposed scheme against statistical attacks, several experiments are performed according to the criterions of histogram distribution, pixel's correlation and entropy measurements. The obtained ciphered image should ensure a high level of randomness to avoid possible deduction of information using known ciphertext attacks. It is also important to guarantee that the enciphered and its corresponding plain images do not share any statistical properties.

5.1.1 Histogram analysis

The histogram analysis of a given image permits to deduce information about the statistical distribution of its pixels's values. While the histogram of the plain image can have an arbitrary form depending on the image content, the histogram of a ciphered one should follow a uniform distribution that reflects a random behavior to avoid any possible information deduction. Figure 4 illustrates the (512×512) images used for experiments with corresponding ciphered images, and Fig. 5 shows corresponding histograms. It is clear that histograms of all ciphered images are pseudo-uniform. Hence, no statistical attack can reveal any information about the plain image using only the corresponding ciphered one.

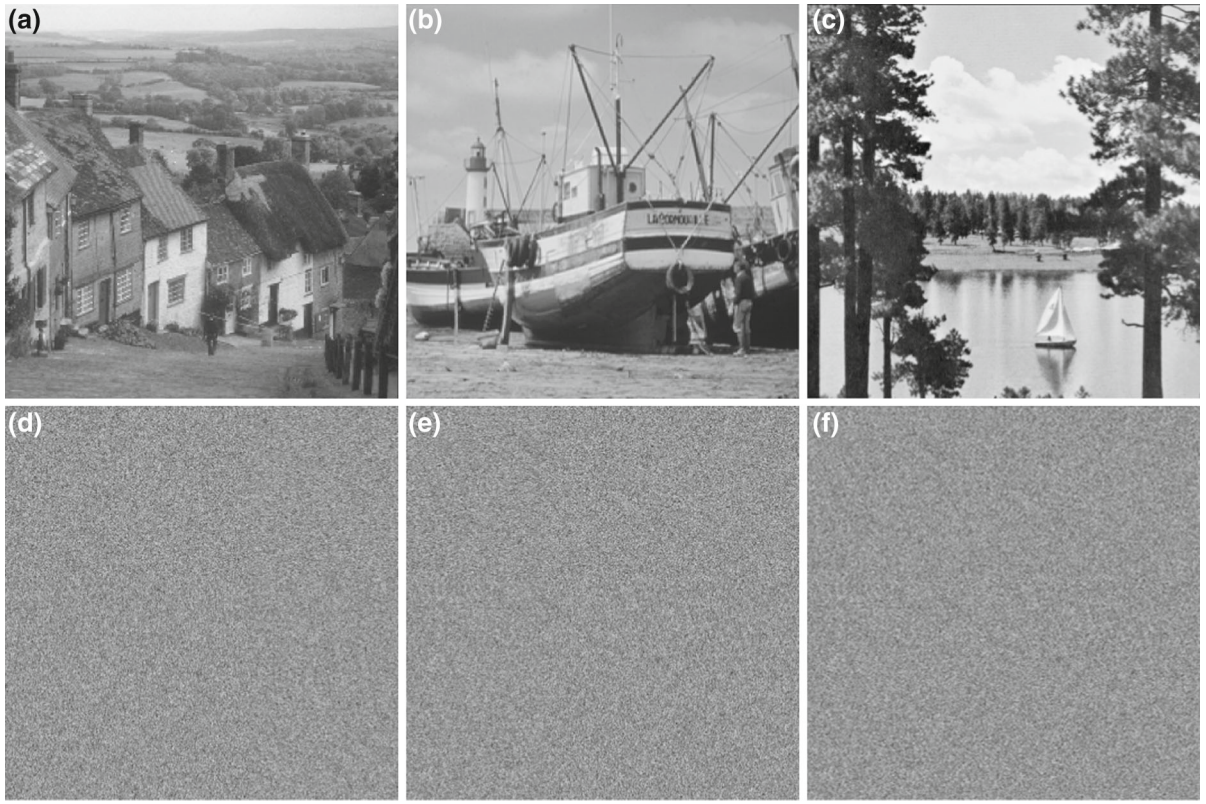

Fig. 4 Plain images used for experiments with their corresponding ciphered images: **a** Goldhill, **b** Boat and **c** Lake

5.1.2 Entropy analysis

Entropy was introduced firstly by Shannon in his paper [32]. Since then, Shannon's entropy has been commonly used in information sciences. It is a measure of the uncertainty associated with a random variable. The entropy $H(S)$ of a source S is defined by:

$$H(S) = -\sum_{n=1}^{L} P(m_i) \log_2 P(m_i) \tag{10}$$

where L represents the number of distinct symbols released by S, and $P(m_i)$ is the probability of symbol's m_i occurrence in S. In the context of digital images, the utmost possible entropy of a source emitting 256 symbol (a grayscale images) is 8. Given that, the computed entropy for the ciphered images should be very close to the theoretical value 8 in order to confirms their high degree of unpredictability (randomness). Results of Shannon's entropy of Boat, Goldhill and Lake grayscale images are shown in Table 1.

Conventional usage of Shannon entropy aforementioned is referred to as global Shannon entropy. Due to some weaknesses in such global entropy that are cited in [33], and to its failure to measure the true randomness of an image, we used another measurement of randomness that computes the sample mean of Shannon entropy to a number of non-overlapping and randomly selected image blocks using local Shannon entropy proposed in [33]. The local entropy simulations are performed under the case that 30 non-overlapping blocks are randomly selected with 1936 pixels per block, using exactly the same set of parameters as pointed in [33]. Local entropy of the three images used for experiments is illustrated in Table 2.

From illustrated results, we point out that each global entropy of enciphered image is very close to the theoretical value of 8, and each local entropy also belongs to the acceptance interval at 5 % of significance level. Hence, results demonstrate the satisfaction of both local and global entropies by the enciphered images.

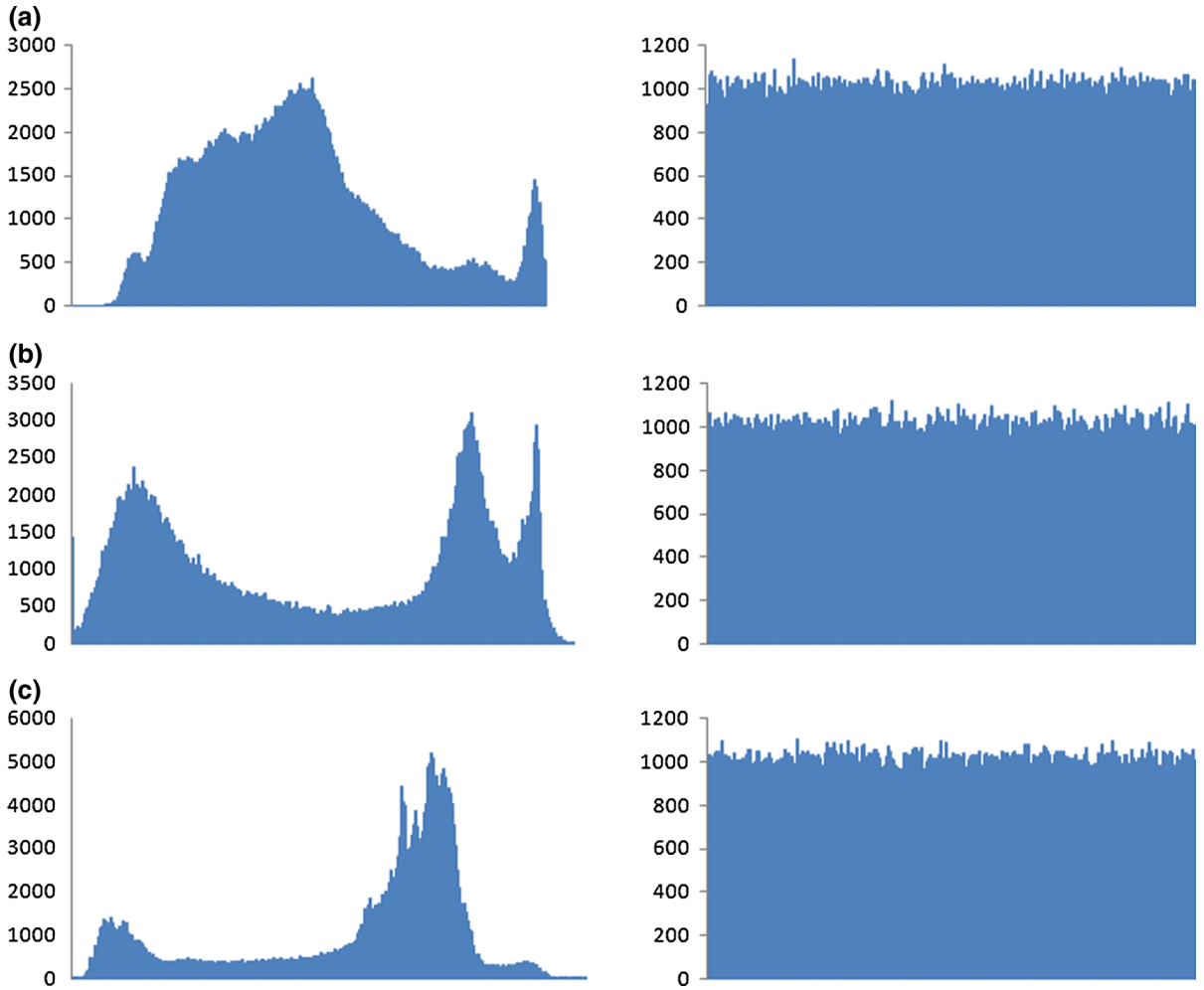

Fig. 5 Histograms of plain/ciphered images: **a** Goldhill, **b** Lake and **c** Boat

Table 1 Shannon's entropy of Boat, Goldhill and Lake grayscale images

Image	Plain image	Ciphered image
Boat	7.0931	7.9976
Goldhill	6.5724	7.9987
Lake	6.2387	7.9992

5.1.3 Analysis of adjacent pixels correlation

In plain images, there is a strong correlation between adjacent pixels in horizontal, vertical and diagonal directions. However, a ciphered image that should have a random aspect must provide extremely low correlation between adjacent pixels. In order to evaluate correlation of adjacent pixels in every direction (vertical, diagonal and horizontal), the subsequent procedure is performed: A set of 10,000 pairs of adjacent pixels is randomly chosen in every direction from both plain and corresponding ciphered images. The correlation coefficient for each image is then computed using the following equations:

$$r_{xy} = \frac{\mathrm{Cov}(x, y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

$$\text{where} \quad \mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \text{ and } E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \, , \, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (11)$$

Table 2 Local entropy results for the test images using 30 blocks of 1936 pixels, with parameters $h_{\text{left}}^{l^{*}0.05} = 7.901901305$ and $h_{\text{right}}^{l^{*}0.05} = 7.903037329$

	Boat		Goldhill		Lake	
	Plain	Ciphered	Plain	Ciphered	Plain	Ciphered
Block #1	4.4393	7.8956	6.7892	7.9133	6.8712	7.9719
Block #2	4.1816	7.9131	5.6581	7.9002	7.0480	7.7952
Block #3	4.7889	7.9029	6.9812	7.8877	6.9741	7.8547
Block #4	7.2377	7.9115	6.6874	7.9076	6.9875	7.9147
Block #5	4.5124	7.9116	7.2180	7.9035	6.2478	7.9243
Block #6	4.8562	7.9004	6.9982	7.9038	7.0215	7.9021
Block #7	5.8472	7.8841	7.2105	7.9102	7.2369	7.8974
Block #8	7.4121	7.8997	6.0125	7.9025	7.0129	7.8812
Block #9	4.9891	7.9147	5.3897	7.8877	6.1035	7.9046
Block #10	5.4989	7.8941	5.6871	7.8929	7.3869	7.9201
Block #11	6.6024	7.8987	4.3329	7.9033	7.1258	7.9963
Block #12	7.0316	7.9017	5.2758	7.8795	6.3256	7.8952
Block #13	4.6006	7.9114	5.6835	7.9038	7.0155	7.9107
Block #14	4.8567	7.9095	5.5572	7.9085	7.1276	7.8749
Block #15	6.7455	7.9086	6.6877	7.9118	6.0422	7.9044
Block #16	5.1793	7.9052	5.9632	7.8836	6.5149	7.9113
Block #17	5.0005	7.9087	5.5873	7.8991	6.2358	7.9001
Block #18	5.7355	7.8889	4.0155	7.8858	6.0462	7.9097
Block #19	6.2735	7.8887	4.6986	7.9124	7.0154	7.9120
Block #20	7.0549	7.9044	6.3971	7.9085	7.5587	7.9119
Block #21	7.3383	7.9085	6.1287	7.9038	7.2365	7.9087
Block #22	7.3352	7.8991	5.9851	7.9079	7.3557	7.9054
Block #23	6.3976	7.9164	5.1227	7.9106	6.1574	7.8897
Block #24	5.0160	7.8846	5.2130	7.8932	7.5475	7.9035
Block #25	5.0005	7.9087	4.0157	7.9049	7.0154	7.9089
Block #26	5.7355	7.8889	5.9963	7.9038	6.0453	7.9201
Block #27	6.2735	7.8887	5.9245	7.8932	5.9991	7.9147
Block #28	7.0549	7.9044	6.3248	7.898	7.2487	7.8994
Block #29	6.2111	7.9048	6.2305	7.8836	6.5687	7.9033
Block #30	5.1449	7.9054	6.8841	7.8912	7.0368	7.8974
Mean value	5.8784	7.9021	5.8885	7.8998	6.8036	7.9047

Here, $E(x)$ is the estimation of mathematical expectations of x, $D(x)$ is the estimation of variance of x, and $\text{cov}(x, y)$ is the estimation of covariance between x and y. x and y are grayscale values of two adjacent pixels in the image, and N is the number of selected pixels.

Table 3 lists the different obtained mean values of the correlation coefficients for plain and ciphered images used for experiment. It is clear that ciphered images provide very low correlation in all directions, meaning that they provide a high randomness degree. Further illustrations are shown in Fig. 6 using the correlation diagram in vertical, diagonal and horizontal directions of the image Goldhill and its corresponding ciphered image.

5.2 Sensitivity analysis

One of the most important security aspects of an image's cryptosystem is to be resistant against differ-

Table 3 Correlation coefficient of adjacent pixels in the plain images Boat, Barbara and child and their corresponding cipher-images

Image	Plain			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Goldhill	0.9809	0.8811	0.9056	0.0013	0.0017	0.0014
Lake	0.9691	0.9647	0.9458	−0.0025	0.0022	0.0038
Boat	0.9279	0.7516	0.8726	0.0016	0.0015	−0.0024

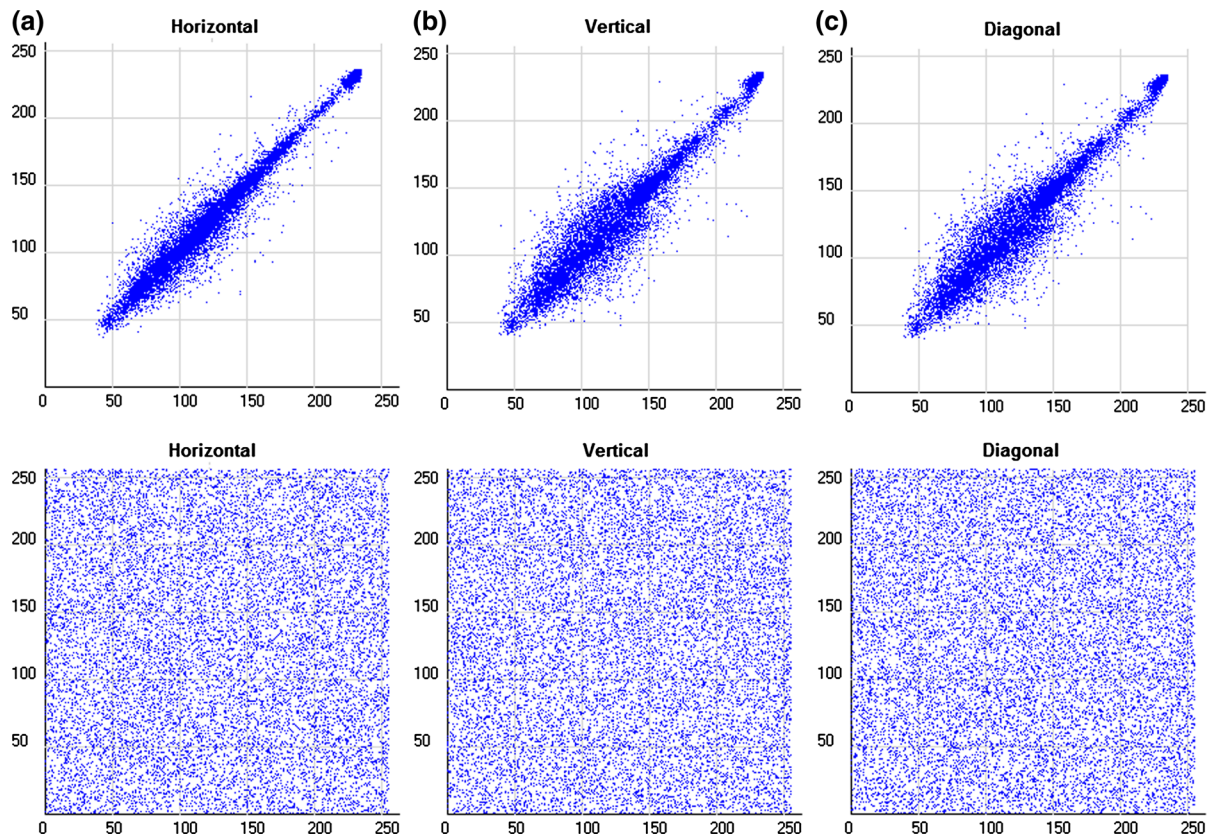

Fig. 6 Correlation diagrams for plain/ciphered images: **a** diagonal, **b** vertical and **c** horizontal

ential and linear attacks. These two attacks exploit the influence of elementary changes in the system's inputs (the key and the plain image) on the corresponding output (the ciphered image) in order to deduce information about the secret key. A secure cryptosystem must ensure a high sensitivity to elementary changes of its inputs to ensure best confusion/diffusion properties. In the following, we present several performed experiments to evaluate the sensitivity of the proposed encryption scheme to both key and plain image elementary alterations.

5.2.1 Sensitivity of secret key

The sensitivity of the proposed encryption scheme to its secret key variation is measured using percentage of difference between two ciphered images of the same plain image, using two keys K_1 and K_2 that are slightly different (a one bit difference only). The following experiment was conducted to evaluate key's sensitivity with respect to all the 128 key's bits: A plain image is firstly ciphered using a randomly generated key K_1 to obtain the ciphered image C_1. After that, we carried out

128 bits changes on the key K_1 to get each time a key K_2 that differs only on one bit with respect to K_1. The key K_2 is then used to encipher the same plain image for obtaining the ciphered image C_2. The percentage of difference is then calculated between C_1 and C_2 using the following equation:

$$\text{diff} = \left(\frac{1}{512.512} \sum_{i=1}^{L} \sum_{j=1} \text{sg}(C_1[i, j] - C_2[i, j]) \right). 100 \text{ where } \text{sg}(x) = \begin{cases} 1 \text{ if } x \neq 0 \\ 0 \text{ otherwise} \end{cases} \quad (12)$$

Similarly, sensitivity of the decryption scheme to the secret key alterations can be evaluated by decrypting C_1 for each test image using a modified key K_2 and then reporting the percentage of difference between the resulting image and the original plain one. A high sensitivity to the key leads to a high percentage of difference with respect to all key's bit positions.

The above two experiments have been performed using the three test images, and results are reported in Fig. 7. It is clear from obtained results that an extremely high sensitivity is ensured by the proposed scheme with respect to all the 128 bits of the secret key, leading to a high robustness to differential and linear cryptanalysis.

5.2.2 Sensitivity to plain image alterations

One of the main advantages of the proposed scheme is its extreme sensitivity to elementary variations of the plain image. Unlike almost all existing CA-based image cryptosystems, the proposed one is highly sensitive to elementary changes that affects a plain image. When ciphering with the same key, a single bit flipping from the whole image produces a completely different ciphered image with a different percentage equal at least to 99 %. Such important characteristic denotes a high diffusion rate of the scheme. It is generally achieved only by chaos-based approaches using multiple enciphering rounds, whereas the proposed scheme achieves equivalent performances using only one enciphering round. In addition, it has been established that a cryptosystem that provides such plain image's high sensitivity is robust against differential cryptanalysis.

In order to evaluate the sensitivity of the scheme to a minor plain image modification, we used the two common measurements: NPCR and UACI. The NPCR stands for the number of pixels change rate when one bit from a randomly selected pixel of the plain image is changed, while the UACI stands for unified average changing intensity that measures the average intensity of differences between the plain and ciphered image. If we denote by C_1 and C_2 two ciphered images corresponding to two plain images that differ in only one bit, and we define the bipolar matrix D at each pixel position (i, j) by $D[i, j] = 0$ if $C_1[i, j] = C_2[i, j]$ and $D[i, j] = 1$ otherwise, then the corresponding NPCR value is computed using the following equation:

$$\text{NPCR} = \left(\frac{1}{N \cdot M} \sum_{i=1}^{M} \sum_{j=1}^{M} D[i, j] \right) \times 100\,\% \quad (13)$$

where N is the width of the image. The UACI measurement which computes the average intensity of difference between plain and ciphered images is computed using the following equation:

$$\text{UACI} = \frac{1}{N \cdot M} \left(\sum_{i=1}^{M} \sum_{j=1}^{M} \frac{|C_1[i, j] - C_2[i, j)]|}{255} \right) \times 100\,\% \quad (14)$$

Using the three test images, we computed the average of both NPCP and UCAI when changes of each pixel's bit of the plain image are applied. The obtained values of the NPCR were 99.59, 99.72 and 99.51 % for the images Boat, Goldhill and Lake, respectively, while the UACI values were 33.52, 33.53 and 33.49 % for the same image, respectively. These results show that even small change in the original image results in a significant change in the ciphered one. Hence the proposed scheme has a good ability to resist differential attack.

In order to further illustrate the effectiveness of the proposed scheme with respect to the plain image's sensitivity, we performed an evaluation of the NPCR and UACI using multiple enciphering rounds. Unlike existing schemes, the proposed one provides a high sensitivity with only one enciphering round, leading to best speed performance with equivalent resistance to differential attack. Figure 8 illustrates evolution of both measurements with respect to the performed enciphering rounds.

5.3 Randomized encryption and resistance against chosen-plaintext attack

In order for an encryption scheme to be resistant against chosen-plaintext attack (to be CPA secure), it should provide the property of randomized encryption. This

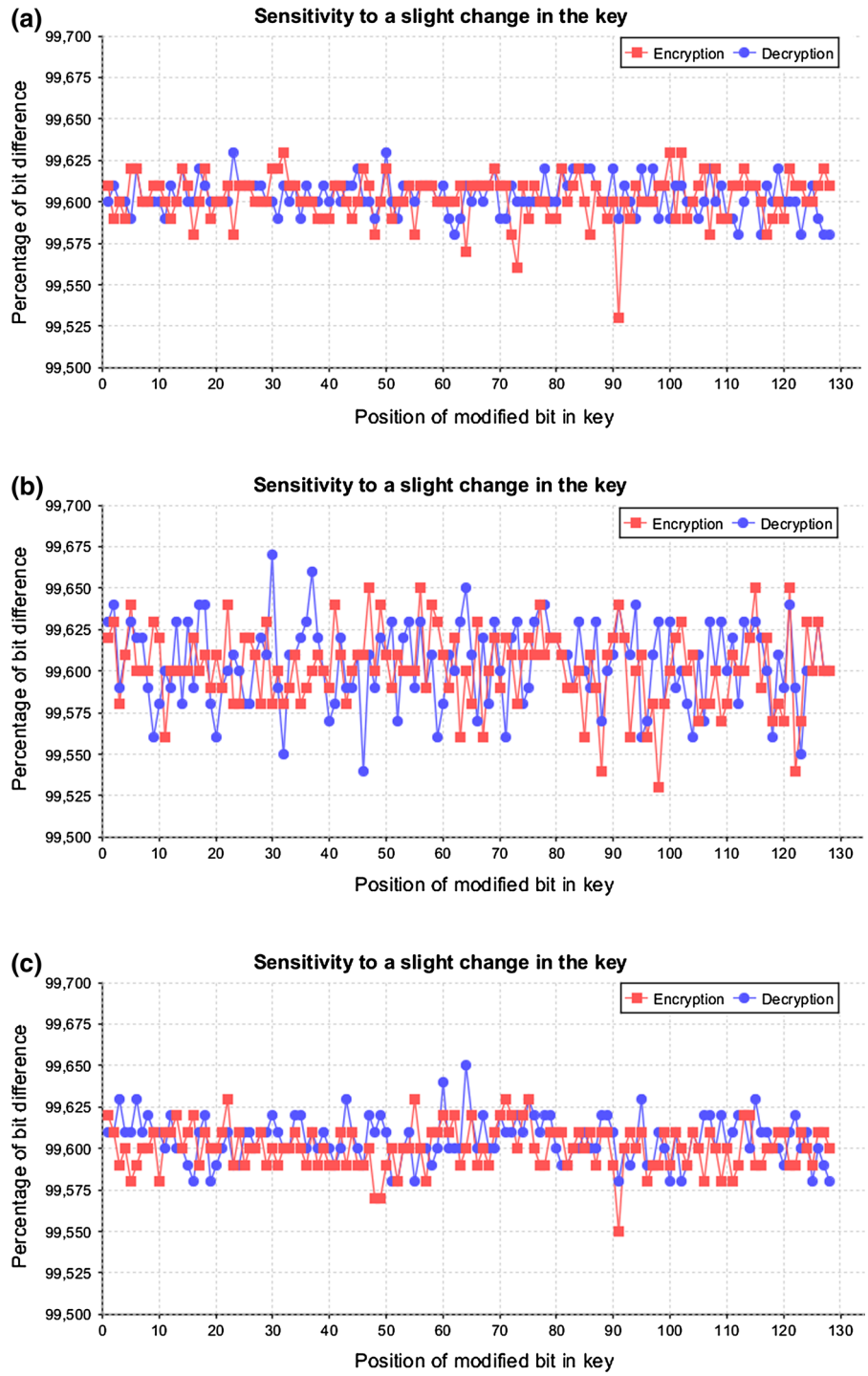

Fig. 7 Results on secret key's sensitivity to elementary bit alterations: **a** using the image Goldhill, **b** using the image Lake and **c** using the image Boat

property is satisfied by each enciphering system that produces two different ciphered images when ciphering the same plain image with the same secret key. Hence, an attacker cannot use previous information about a given plain image to break the semantic security of the system and reveal any useful information about the key.

The high diffusion property provided by the proposed scheme permits to use it easily in a randomized

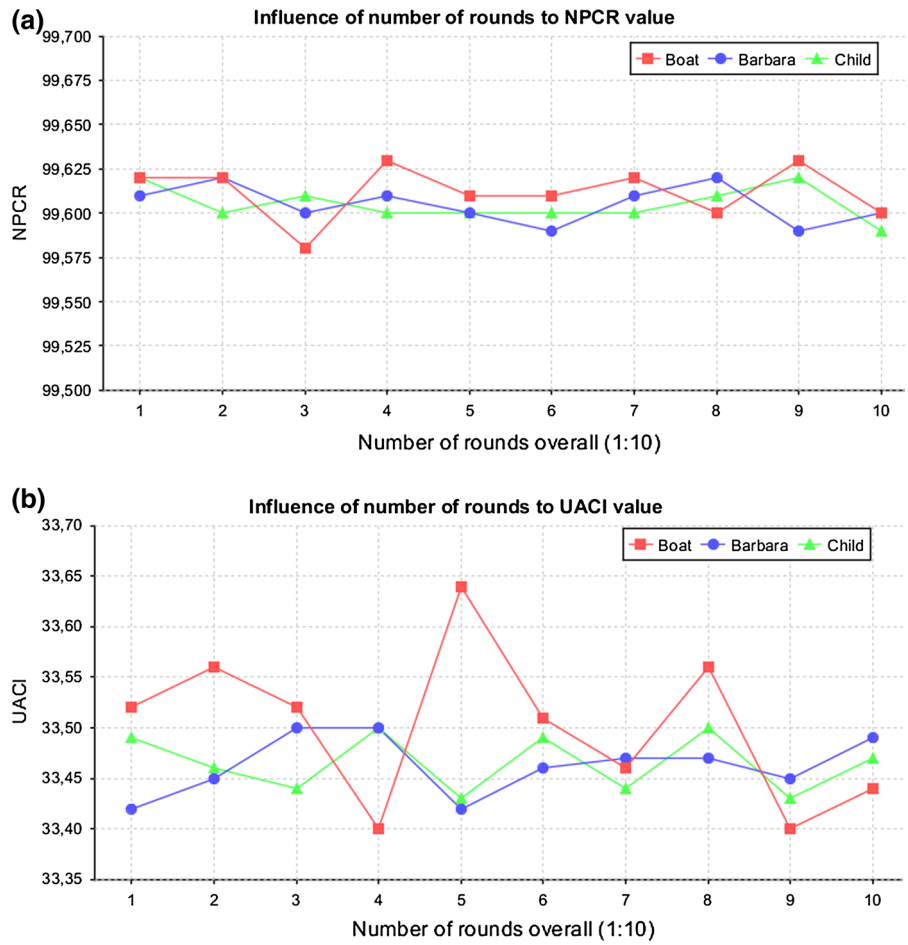

Fig. 8 Evaluation of the plain image's sensitivity with respect to enciphering rounds: **a** NPCR evolution, **b** UACI evolution

encryption mode. Since the plain image is highly sensitive to elementary bit variations, it undergoes an elementary bit modification at each encryption using the same key, so the resulting ciphered image will be totally different due to high sensitivity of the scheme. When deciphering, the resulting plain image is exactly the same as the original one except on one bit difference, which is negligible with respect to the size of the image and visually imperceptible.

Since a grayscale image with size $M \times N$ contains $M \cdot N$ pixels on 8 bits each one, the total number of possible ciphered image for a given plain one with a fixed secret key is equal to $2^{8^*M \cdot N}$. For an image of 256×256 pixels, this number is equal to 2^{131072} which is extremely huge, and the probability to get the same ciphered image after two consecutive ciphering operations is negligible. Figure 9 illustrates two ciphered versions of the Boat image using the same secret key. The second enciphering is performed after flipping a randomly selected bit from the image. Figure 9d shows the difference image between the two ciphered versions, while corresponding difference is equal to 99.01 %. This will ensure that the proposed scheme is extremely robust against chosen-plaintext attacks.

5.4 Performances and statistical analysis comparisons

As mentioned above, one of the main advantages of the proposed scheme is the extremely high encryption/decryption rates provided with respect to existing recent schemes that use cellular automatons and chaotic systems. According to the NPCR and UACI analysis, only one enciphering round is required by the proposed scheme to achieve same sensitivity degree as existing schemes using multiple rounds. Hence, the overall run time for both encryption and decryption procedure is considerably reduced.

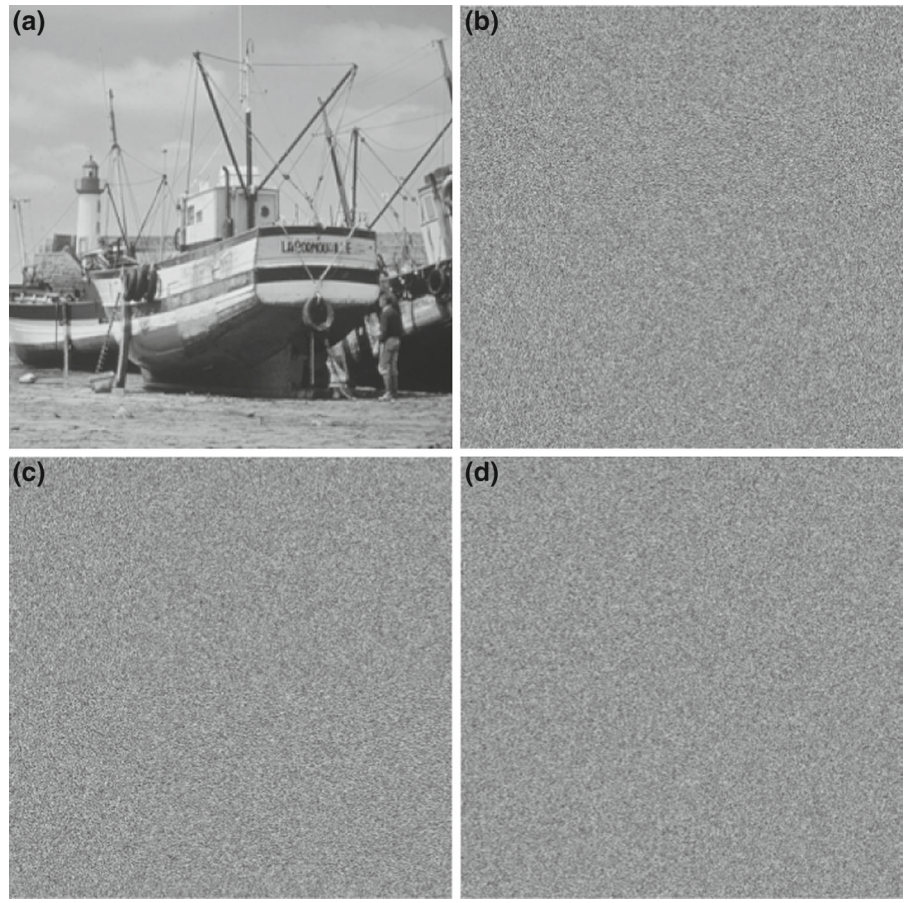

Fig. 9 Randomized encryption using the proposed scheme: **a** plain image, **b** ciphered image C_1 using a key K, **c** ciphered image C_2 using the same key, **d** difference image $|C_1 - C_2|$ between C_1 and C_2

Implementation of the proposed scheme was realized using C programming language, and experiments were performed on an Intel(R)Core (TM)i7-CPU of 3Ghz with 8GB of memory. The resulting performance outperforms almost all existing CA-based and Chaos-based approaches used for image encryption. Table 4 illustrates obtained enciphering/deciphering rates in comparison with some existing schemes. Since decryption and encryption times are generally equivalent, only encryption times are presented.

In order to evaluate statistical performances of the proposed schemes and demonstrate its advantage with respect to existing chaos-based and CA-based ones, we present a statistical comparative study in Table 5. After implementing approaches referenced in [35–38], we benchmarked using the three images of Fig. 4, and averaged results with respect to entropy, sensitivity, UACI and NPCR are reported. Obtained results show that the scheme outperforms most of the existing ones with respect to several statistical criterions. Besides, the security assumption of the proposed scheme is much stronger than the others, since it is relaying on the impossibility to reconstruct previous configurations of an M-order MCA without knowledge of at less M consecutive configurations.

6 Conclusions

This paper proposes a new image encryption scheme based on one-dimensional reversible memory cellular automata and hierarchical quadtree decomposition. The plain image is recursively decomposed into four equal quadrants that define four configurations to be evolved using a 4th-order memory cellular automaton. Resulting configurations replace the initial image's blocks, while one of them is recursively divided in a quadtree scheme until reaching a lower decomposition limit. Security of the proposed scheme is relied on the impossibility to reconstruct 4th-order MCA's config-

Table 4 Encryption time performances comparison for different image sizes

Plain image size	Encryption time (in ms)					
	Ref. [34]	Ref. [35]	Ref. [36]	Ref. [37]	Ref. [38]	Proposed
256×256	569	7641	178	120	189	93
512×512	2251	34468	663	475	758	327
1024×1024	8986	151709	3142	1951	3097	1264

Table 5 Statistical and sensitivity measurements comparison with some existing schemes

	Ref. [34]	Ref. [35]	Ref. [36]	Ref. [37]	Ref. [38]	Proposed
Averaged entropy	7.9912	7.9984	7.9987	7.9993	7.9973	7.9991
Averaged sensitivity measurement (eq. 12)	99.326	99.417	99.546	99.612	99.512	99.623
UACI	99.147	99.524	99.587	99.598	99.441	99.606
NPCR	33.478	33.498	33.481	33.507	99.498	33.513

uration without knowledge of the transition rules and at least four consecutive configurations. Such security assumption is stronger than the one used by existing CA-based schemes, and obtained confusion/diffusion performances outperformed those of existing chaos-based and CA-based ones. Runtime performance is greatly enhanced since only one enciphering round is required to achieve optimal sensitivity to both key and plain image alterations. Such optimal sensitivity permits to use the proposed scheme in a randomized encryption mode that is very resistant against chosen-plaintext attacks. Besides, the key space defined by secret keys on 128 bits is sufficiently large to defeat possible brute force attacks. Therefore, the scheme is particularly suitable for real-time Internet image encryption and transmission applications.

In future works, we plan to enhance the proposed scheme to handle encryption of non-square images using an adaptive quadtree variant. In order to achieve higher security levels, we also plan to extend the proposed scheme using two-dimensional cellular automata.

References

1. Howard, Ralph: Data encryption standard. Inf. Age **9**(4), 204–210 (1987)
2. Lai, X., Massey, J.L.: A proposal for a new block encryption standard. In: Damgård, I. B. (ed.) Advances in Cryptology—EUROCRYPT'90, pp. 389–404. Springer, Berlin (1991)
3. Daemen, Joan, Rijmen, Vincent: The Design of Rijndael: AES-The Advanced Encryption Standard. Springer, Berlin (2002)
4. Suk, Tomáš, Höschl, Cyril, Flusser, Jan: Decomposition of binary images–a survey and comparison. Pattern Recognit. **45**(12), 4279–4291 (2012)
5. Chang, Ji-Ying, Chang, Ruey-Feng, Kuo, Wen-Jia: Edge-based motion compensated classified DCT with quadtree for image sequence coding. Signal Process. Image Commun. **11**(3), 187–197 (1998)
6. Tseng, S.-Y., Yang, Z.-Y., Huang, W.-H., et al.: Object feature extraction for image retrieval based on quadtree segmented blocks. In: 2009 WRI World Congress on Computer Science and Information Engineering, pp. 401–405. IEEE (2009)
7. Salari, E., Li, W.: A fast quadtree motion segmentation for image sequence coding. Signal Process. Image Commun. **14**(10), 811–816 (1999)
8. Tomassini, M., Perrenoud, M.: Nonuniform cellular automata for cryptography. Complex Syst. **12**(1), 71–82 (2000)
9. Guo, J.-I., et al.: A new chaotic key-based design for image encryption and decryption. In: Proceedings of Circuits and Systems, 2000. The 2000 IEEE International Symposium on ISCAS 2000 Geneva, pp. 49–52. IEEE (2000)
10. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(08), 2129–2151 (2006)
11. Zanin, M., Pisarchik, A.N.: Gray code permutation algorithm for high-dimensional data encryption. Inf. Sci. **270**, 288–297 (2014)
12. Wang, Y., Wong, K.-W., Liao, X., et al.: A new chaos-based fast image encryption algorithm. Appl. Soft Comput. **11**(1), 514–522 (2011)
13. Zhu, Z., Zhang, W., Wong, K., et al.: A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf. Sci. **181**(6), 1171–1186 (2011)

14. Zhang, W., Wong, K., Yu, H., et al.: A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun. Nonlinear Sci. Numer. Simul. **18**(3), 584–600 (2013)
15. Chen, J., Zhu, Z., Yu, H.: A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme. Opt. Int. J. Light Electron Opt. **125**(11), 2472–2478 (2014)
16. Fu, C., Chen, J., Zou, H., et al.: A chaos-based digital image encryption scheme with an improved diffusion strategy. Opt. Express **20**(3), 2363–2378 (2012)
17. Behnia, S., Akhshani, A., Mahmodi, H., et al.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**(2), 408–419 (2008)
18. Enayatifar, R., Abdullah, A.H., Isnin, I.F.: Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Lasers Eng. **56**, 83–93 (2014)
19. Bakhshandeh, A., Eslami, Z.: An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Opt. Lasers Eng. **51**(6), 665–673 (2013)
20. Von Neumann, J., Burks, A.W., et al.: Theory of self-reproducing automata. IEEE Trans. Neural Netw. **5**(1), 3–14 (1966)
21. Chatzichristofis, S.A., Mitzias, D.A., Sirakoulis, G.C., et al.: A novel cellular automata based technique for visual multimedia content encryption. Opt. Commun. **283**(21), 4250–4260 (2010)
22. Abdo, A.A., Lian, S., Ismail, I.A., et al.: A cryptosystem based on elementary cellular automata. Commun. Nonlinear Sci. Numer. Simul. **18**(1), 136–147 (2013)
23. Jin, J.: An image encryption based on elementary cellular automata. Opt. Lasers Eng. **50**(12), 1836–1843 (2012)
24. Alexopoulos, C., Bourbakis, N.G., Ioannou, N.: Image encryption method using a class of fractals. J. Electron. Imaging **4**(3), 251–259 (1995)
25. Maniccam, S.S., Burbakis, N.G.: Image and video encryption using SCAN patterns. Pattern Recognit. **37**(4), 725–737 (2004)
26. Chen, R.-J., Lai, J.-L.: Image security system using recursive cellular automata substitution. Pattern Recognit. **40**(5), 1621–1631 (2007)
27. Tomassini, M., Perrenoud, M.: Stream cyphers with one- and two-dimensional cellular automata. In: Schoenauer, M., Deb, K., Rudolph, G., Yao, X., Lutton, E., Merelo, J.J., Schwefel, H.-P. (eds.) Parallel Problem Solving from Nature PPSN VI, pp. 722–731. Springer, Berlin (2000)
28. Tomassini, M., Sipper, M., Zolla, M., et al.: Generating high-quality random numbers in parallel by cellular automata. Future Gener. Comput. Syst. **16**(2), 291–305 (1999)
29. Xuelong, Z., Qianmu, L., Manwu, X., et al.: A symmetric cryptography based on extended cellular automata. In: 2005 IEEE International Conference on Systems, Man and Cybernetics, pp. 499–503. IEEE (2005)
30. Wolfram, S.: A New Kind of Science. Wolfram media, Champaign (2002)
31. Alonso-Sanz, R.: One-dimensional r=2 cellular automata with memory. Int. J. Bifurc. Chaos **14**(09), 3217–3248 (2004)
32. Shannon, C.E.: A mathematical theory of communication. ACM SIGMOBILE Mob. Comput. Commun. Rev. **5**(1), 3–55 (2001)
33. Wu, Y., Zhou, Y., Saveriades, G., et al.: Local Shannon entropy measure with statistical tests for image randomness. Inf. Sci. **222**, 323–342 (2013)
34. Liao, X., Lai, S., Zhou, Q.: A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process. **90**(9), 2714–2722 (2010)
35. Wu, Y., Yang, G., Jin, H., et al.: Image encryption using the two-dimensional logistic chaotic map. J. Electron. Imaging **21**(1), 013014-1–013014-15 (2012)
36. Zhou, Yicong, Bao, Long, Chen, C.L.Philip: A new 1D chaotic system for image encryption. Signal Process. **97**, 172–182 (2014)
37. Kanso, A., Ghebleh, M.: A novel image encryption algorithm based on a 3D chaotic map. Commun. Nonlinear Sci. Numer. Simul. **17**(7), 2943–2959 (2012)
38. Mohamed, F.K.: A parallel block-based encryption schema for digital images using reversible cellular automata. Eng. Sci. Technol. Int. J. **17**(2), 85–94 (2014)
39. Wang, X., Xu, D.: A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn. **75**(1–2), 345–353 (2014)
40. Zhu, C., Xu, S., Hu, Y., et al.: Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn. **79**(2), 1511–1518 (2015)
41. Zhu, C., Liao, C., Deng, X.: Breaking and improving an image encryption scheme based on total shuffling scheme. Nonlinear Dyn. **71**(1–2), 25–34 (2013)