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