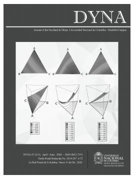
UNIVERSIDAD
NACIONAL
DE COLOMBIA
SEDE MEDELLÍN
FACULTAD DE MINAS



DYNA
http://dyna.medellin.unal.edu.co/

Composite cellular automata based encryption method applied to surveillance videos

Luis Miguel Cortés-Martinez, Luz Deicy Alvarado-Nieto & Isabel Amaya-Barrera

Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. lmcortesm@correo.udistrital.edu.co, lalvarado@udistrital.edu.co, iamaya@udistrital.edu.co

Received: August 23th, 2019. Received in revised form: March 17th, 2020. Accepted: April 15th, 2020

Abstract
This work is part of the research project "Encryption Models Based on Chaotic Attractors" institutionalized in the Research and Scientific Development Center of the Universidad Distrital Francisco José de Caldas. In this paper, a symmetric encryption method for surveillance videos is presented, based on reversible composite cellular automata developed for this purpose. This method takes advantage of reversible cellular automata and elementary rule 30 properties, for efficient regions of interest encryption in surveillance video frames, obtaining an algorithm which experimental results of security and performance are consistent with those reported in current literature. In addition, it allows decryption without loss of information through a fixed size key for each video frame.

Keywords: cryptosystem; reversible composite cellular automata; video encryption; region of interest encryption.

Método de encriptación basado en autómatas celulares compuestos aplicado a videos de vigilancia

Resumen
Este trabajo se enmarca en el proyecto de investigación "Modelos de Encriptación Basados En Atractores Caóticos" institucionalizado en el Centro de Investigaciones y Desarrollo Científico de la Universidad Distrital Francisco José de Caldas. En este documento, se presenta un método de encriptación simétrico para videos de vigilancia a partir de autómatas celulares compuestos reversibles desarrollados para este propósito. Este método aprovecha las propiedades de los autómatas celulares reversibles y de la regla elemental 30, para el cifrado eficiente de regiones de interés en fotogramas de videos de vigilancia, obteniendo un algoritmo cuyos resultados experimentales de seguridad y desempeño son consistentes de acuerdo con los reportados en la literatura actual. Además, permite el descifrado sin pérdida de información mediante una llave de tamaño fijo por cada fotograma de video.

Palabras clave: criptosistema; autómatas celulares compuestos reversibles; cifrado de videos; cifrado de regiones de interés.

1. Introduction

Technological and communication advances, together with the social need for protection and intruder detection, have triggered the massive installation of video surveillance systems in recent years. Due to the large amount of information that is currently captured, stored and transmitted in image, audio and video formats, new cryptography techniques have been presented, and they have received the attention from a scientific and academic community with a view to generating more sophisticated, secure and faster proposals for these format types, since traditional cryptography methods are not effective for this purpose [1,2].

Cryptography schemes that have arisen for image, audio and video formats take advantage of several theories such as elliptic curves [3], DNA sequences [4], quantum computing [5,6], discrete transforms [7,8], chaos theory [1,8-12] and cellular automata [6,11-18].

Connection between cryptography and nonlinear dynamic systems theory has given rise to a line of research called

How to cite: Cortés-Martinez, L.M, Alvarado-Nieto, L.D. and Amaya-Barrera, I, Composite cellular automata based encryption method applied to surveillance videos. DYNA, 87(213), pp. 212-221, April - June, 2020.

Revista DYNA, 87(213), pp. 212-221, April - June, 2020, ISSN 0012-7353
DOI: http://doi.org/10.15446/dyna.v87n213.81859

chaotic cryptography, which approaches have been on the rise in recent years [10]. These approaches take advantage of intrinsic properties of continuous and discrete chaotic dynamic systems, that provide inherent strengths in information masking and have proven to be a security alternative for image, audio and video encryption. Nevertheless, reported disadvantages of chaotic cryptography in literature refer to the high computational cost and the required numerical precision of those algorithms to ensure high sensitivity [19].

Cellular Automata (CAs) were introduced in the late 1940's by von Neumann [20], as a mathematical model with a set of transformation rules that operate on a rectangular mesh formed of a finite number of cells, that interact and evolve in discrete time steps according to a local transition rule and may exhibit complex behaviors. In the last years, CAs have been used in several biological contexts [21,22]. Currently, CAs are an interest technique in the designing of image encryption methods, since it is possible to interpret and treat an image as the initial state of a Layered Cellular Automaton (LCA) and define encryption mechanisms based on its evolution [13,14]. Efficient and robust methods use CAs for image [14-17], audio [18] and video encryption [13]. Several cryptosystems merge CAs with other several approaches such as chaos theory [11,12] and quantum computing [6].

According to the amount of information that is encrypted, two categories of video encryption have emerged: In the first, the frames that constitute the video are fully encrypted [23]; and in the second, only the regions of interest (RoIs) are considered, defined as the frame segments that contain sensitive information [13]. The second category is more efficient since the size of sensitive information is reduced. In [24-27], different methods of detection and extraction of RoIs have been proposed, which consider movement, people's faces, text, among others, as a kind of sensitive information.

In this paper, LCAs and chaos inherent properties are used for the construction of a surveillance video encryption method that uses Composite Cellular Automata (CCAs), one-dimensional CAs designed for this method, which rules are constructed with the reversible elementary rules defined by Wolfram [28]. The proposed encryption method is symmetric and applicable to grayscale and color videos. The sender uses fixed size keys for the encryption of rectangular RoIs defined by motion perceptions in video frames. Encrypted RoIs conserve their original size.

On the other hand, the receiver uses the same keys to recover the original video from the encrypted RoIs and the video frames with hidden RoIs coming from the sender.

This paper is organized as follows. In Section 2, theoretical bases of this work are described. In Section 3, the developed encryption method is described in detail. In Section 4, experimental tests and performance analysis of the implemented cryptosystem are performed. Finally, Section 5 lists the conclusions and contributions of this paper.

2. Theoretical framework

Theoretical principles that support the work presented in this paper relate properties of cryptographic systems to the characteristics of one-dimensional CAs, to contribute in the information security field with a proposal applied on surveillance videos.

2.1. Cryptographic systems

Cryptography arises from the need to ensure confidentiality, integrity and availability of information. Consequently, cryptographic systems are designed and implemented, with the aim of transforming meaningful information into unintelligible data through a hiding mechanism that uses secret cipher keys and allows exclusive access of authorized users to the original information by a decryption process. On the other hand, cryptanalysis seeks to detect vulnerabilities in cryptosystems in order to retrieve or supplant information [29].

There are two types of cryptosystems: symmetric and asymmetric. In symmetric type, the same key is used at both ends of a communication channel, while in asymmetric type each user has a public and a private key [29]. Algorithms based on CAs or chaos that have been proposed for image and video encryption are usually of symmetric type.

In this work, density of periodic points, topological transitivity, and sensitive dependence on initial conditions of the combination of CAs pseudo-random behavior among with additional operations of integer numbers are used to induce the confusion and diffusion properties that should be part of a cryptographic method [30-32].

The confusion property seeks to ensure that the cryptosystem evolution in time is independent of the encrypted text and the cipher key, that is, that the relationship between text and password is sufficiently complex to guarantee security. On the other hand, the diffusion property seeks that small changes in the original text should generate completely different encrypted text [30].

2.2. Cellular Automata

Cellular Automata (CAs) are massively parallel homogeneous discrete dynamic systems [20] with the capability to exhibit complex behaviors. They are represented by an n-dimensional matrix with a finite number of cells, where each cell i has a state s_i from a set of possible states S and evolves, synchronously with the other cells of the matrix, in discrete time steps according to a local transition rule or evolution function. The updated state of each cell depends on the entries of this function, which are the previous states of a set called neighborhood, that is conformed of the cell itself and some adjacent [11,33].

The number of possible evolution rules N_R for a one-dimensional CA is calculated by using eq. (1), where k is the cardinality of S, and n is the number of cells that compose its neighborhood [21].

$$N_R = k^{k^n} \tag{1}$$

Boundaries of CAs can be periodic, reflecting or fixed [22]. Periodic boundaries are used in the proposed method.

Elementary Cellular Automata (ECAs) are one-dimensional, each cell in an ECA has three neighbors and the set of possible states is $S = \{0, 1\}$. According to eq. (1), there are $2^{2^3} = 256$ different transformation rules for ECAs, called elementary rules, that are identified by integer numbers in the interval from 0 to 255 [28]. The next state for a cell i in an ECA in function of a given elementary rule f is calculated by eq. (2), which is defined in terms of neighboring cells.

$$s_i(t+1) = f[s_{i-1}(t), s_i(t), s_{i+1}(t)] \tag{2}$$

Fig. 1 schematizes the evolution of an i_{th} cell in an ECA.

Wolfram [28,33] classified elementary rules into four types according to behavior of CAs in space-time diagrams: homogeneous stable (class I), periodic stable (class II), chaotic (class III) and complex (class IV). Rule 30 is classified as class III and has been used as a pseudo-random number generator [28]. Unpredictable behavior with rule 30 increases when the number of cells is large and odd [34], and when avoiding the use of ECA's entire rows or columns.

An ECA presents reversibility when it is possible to obtain information about its past states through the current state of its cells, that is, when the state of each cell depends on the previous state of a single cell in the neighborhood [33].

Only six elementary rules achieve reversibility on an ECA [28,33], called reversible elementary rules and listed on Table 1. For convenience, in the proposed encryption method an alternative notation for these rules is used in this paper, with respect to the value that takes each cell in the ECA based on its only predecessor in the neighborhood.

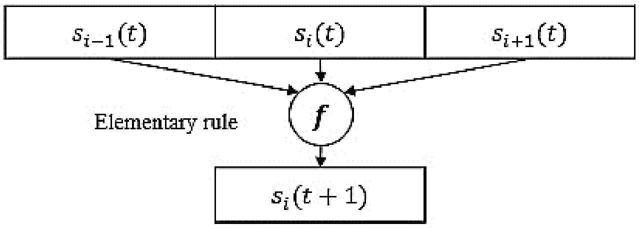


Figure 1. Cell evolution in an ECA.
Source: The Authors.

Table 1.
Reversible elementary rules.

Reversible elementary rule	Alternative notation	Behavior description	Reversible pair rule
240	A	Shift-right	170 (C)
204	B	Identity	204 (B)
170	C	Shift-left	240 (A)
15	$\overline{A}$	Shift-right and complement	85 ($\overline{C}$)
51	$\overline{B}$	Complement	51 ($\overline{B}$)
85	$\overline{C}$	Shift-left and complement	15 ($\overline{A}$)

Source: The Authors.

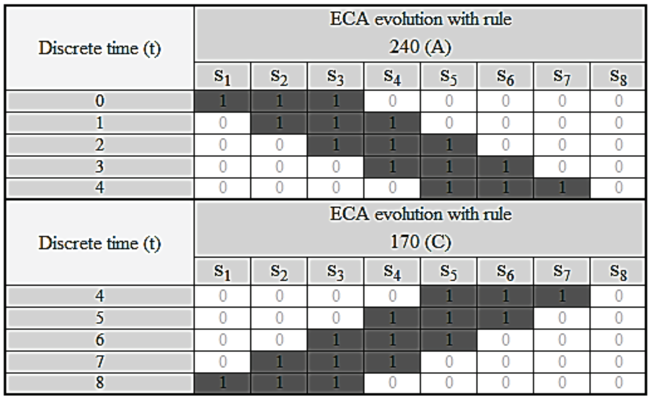
These rules can also be classified into two types: Self-Reversible (SRR) and Non-Self-Reversible Rules (NSRR). SRR are those rules that are reversible with themselves; and NSRR are those that do not achieve this property. ECAs have four NSRR (15, 85, 170 and 240) noted as 'A', 'C', '$\overline{A}$' and '$\overline{C}$'; and two SRR (51 and 204), noted as 'B' and '$\overline{B}$'.

Reversibility property of CAs is useful in cryptosystems design. In one dimension, this reversibility can be determined, although in the literature it has been shown that this property is undecidable for two or more dimensions [20].

Fig. 2 shows the behavior of an ECA that evolves four times with rule 240 ('A'), and four times with rule 170 ('C') to return to its initial state '11100000'.

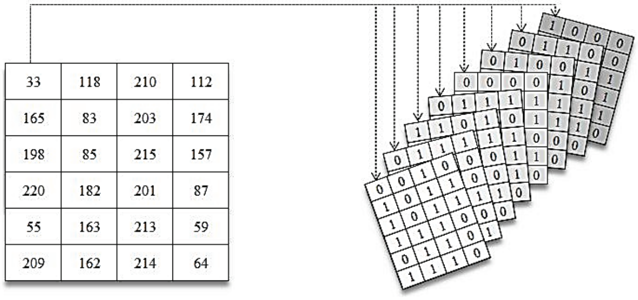
In CAs context, it is possible to interpret an image I with size $M \times N$ as a Layered Cellular Automaton (LCA), since it is a matrix with values in the interval from 0 to 255 (black to white), reason why each value can be represented with a byte [13,14]. If I is a grayscale image, the LCA that represents is an 8-layer CA, that is, a matrix of $M \times N \times 8$ bits as shown in Fig. 3. If I is a color image, it is possible to represent it by three adjoined 8-layer CAs that form a 24-layer CA.

In the proposed method, each row or column that constitutes any layer in the LCA is considered as the initial state of a one-dimensional CA. The maximum number of one-dimensional CAs that constitutes a LCA obtained from I is given by eq. (3), where the function $max(M, N)$ returns the maximum value between M and N, and the L value is 8 in grayscale images or 24 in color images.



Discrete time (t)	ECA evolution with rule 240 (A)							
	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
0	1	1	1	0	0	0	0	0
1	0	1	1	1	0	0	0	0
2	0	0	1	1	1	0	0	0
3	0	0	0	1	1	1	0	0
4	0	0	0	0	1	1	1	0
Discrete time (t)	**ECA evolution with rule 170 (C)**							
	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
4	0	0	0	0	1	1	1	0
5	0	0	0	1	1	1	0	0
6	0	0	1	1	1	0	0	0
7	0	1	1	1	0	0	0	0
8	1	1	1	0	0	0	0	0

Figure 2. ECA evolution with rules 240 and 170.
Source: The Authors.



33	118	210	112
165	83	203	174
198	85	215	157
220	182	201	87
55	163	213	59
209	162	214	64

Figure 3. Interpretation of image as LCA.
Source: The Authors.

$$N_S(I) = L \times max(M, N) \tag{3}$$

3. Proposed cryptographic method

In the following subsections, the key generation technique, the RoI extraction mechanism and the structure of the proposed cryptographic method are described. The central axis of this method is a kind of reversible one-dimensional CA.

3.1. Composite Cellular Automata definition

The kind of CAs formulated in this paper are named Composite Cellular Automata (CCAs). They are one-dimensional and ECA-based, since their transition rules are a combination of elementary rules. They are called composite rules, with which new possible behaviors emerge that cannot be obtained independently through ECAs.

Formally, a composite rule **F** is given by expression in eq. (4), where f_i is an elementary rule and r is the number of elementary rules that constitute **F**.

$$\mathbf{F} = \{f_1, f_2, \dots f_i, \dots\ f_r\} \tag{4}$$

In turn, each f_i defines the state for a set of r cells in the CCA from i to $i + r - 1$ through the expressions in eq. (5). The number of bits that represent a composite rule is $8 \times r$ because an elementary rule is identified by eight bits.

$$\begin{gathered} s_i(t+1) = f_1[s_{i-1}(t), s_i(t), s_{i+1}(t)] \\ s_{i+1}(t+1) = f_2[s_i(t), s_{i+1}(t), s_{i+2}(t)] \\ \vdots \\ s_{i+r-1}(t+1) = f_r[s_{i+r-2}(t), s_{i+r-1}(t), s_{i+r}(t)] \end{gathered} \tag{5}$$

Fig. 4 shows a 6-cell periodic boundaries CCA that evolves with a composite rule with $r = 2$.

Utilization of CCAs has several advantages: a greater number of rules, the possibility of establishing new reversible rules, and an efficiency that resembles ECAs homogeneity.

3.2. Reversible composite rules classification

A reversible CCA evolves with a composite reversible rule, that consists exclusively of elementary reversible rules. The number of cells of a CCA must be multiple of r to ensure that every f_i on **F** is used the same number of times.

For simplicity purposes, alternative notation presented in Table 1 is used to identify any reversible composite rule as a string of r characters, each one has six possible values (‘A’, ‘Ā’, ‘B’, ‘B̄’, ‘C’, ‘C̄’). Nevertheless, not all possible combinations of these values identify a reversible composite rule. In the proposed method, the r value is equal to 8.

In the CCAs environment, new NSRR arise, that involve displacement in the same direction, labeled as Composite Shift Rules (CSR), and formed exclusively of the elementary rules ‘A’ and ‘Ā’, or ‘C’ and ‘C̄’. Fig. 5 shows the behavior of a CCA with initial state ‘11100000’ that evolves four times with rule ‘AAAAAĀAA’ and other four with rule ‘CCCCC̄CCC’ to return to its initial state.

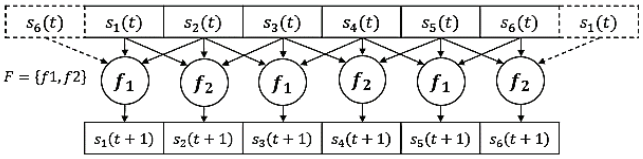
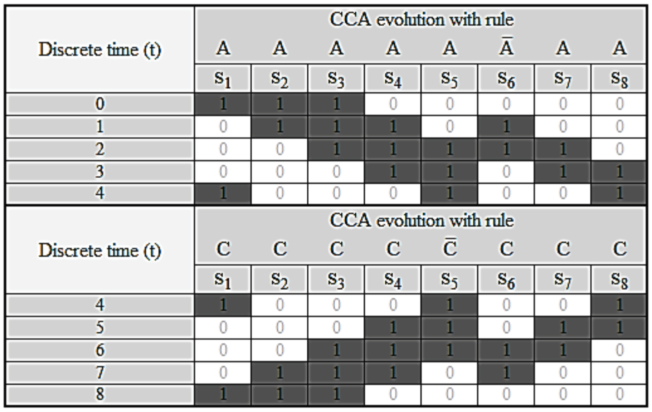


Figure 4. CCA evolution with r=2.
Source: The Authors.



Discrete time (t)	CCA evolution with rule							
	A	A	A	A	A	Ā	A	A
	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
0	1	1	1	0	0	0	0	0
1	0	1	1	1	0	1	0	0
2	0	0	1	1	1	1	1	0
3	0	0	0	1	1	0	1	1
4	1	0	0	0	1	0	0	1

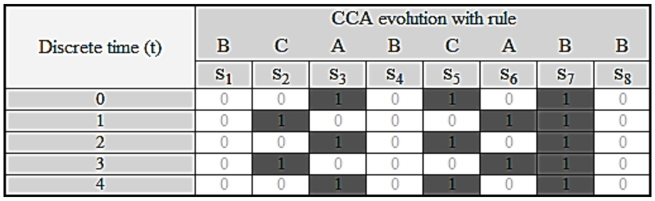
Discrete time (t)	CCA evolution with rule							
	C	C	C	C	C̄	C	C	C
	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
4	1	0	0	0	1	0	0	1
5	0	0	0	1	1	0	1	1
6	0	0	1	1	1	1	1	0
7	0	1	1	1	0	1	0	0
8	1	1	1	0	0	0	0	0

Figure 5. CCA evolution with CSR rules.
Source: The Authors.

In addition, reversible rules with capability to change the order of bits of an initial state arise, labeled as Bit Position Change Rules (BPCR). Fig. 6 shows the behavior of a CCA with initial state ‘00101010’ that evolves four times with composite reversible rule ‘BCABCABB’. Note that this BPCR is also an SRR. Nevertheless, there exist NSRR type BPCRs, as in the case of rules ‘BC̄ABC̄ABB’ and ‘BCĀBCĀBB’.

Finally, Identity-Complement Rules (ICR) arise, they are composed exclusively of the elementary rules ‘B’ and ‘B̄’, and they are also SRR.

In Fig. 7, reversible composite rule classification performed in this work is shown.



Discrete time (t)	CCA evolution with rule							
	B	C	A	B	C	A	B	B
	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
0	0	0	1	0	1	0	1	0
1	0	1	0	0	0	1	1	0
2	0	0	1	0	1	0	1	0
3	0	1	0	0	0	1	1	0
4	0	0	1	0	1	0	1	0

Figure 6. CCA evolution with BPCR rule.
Source: The Authors.

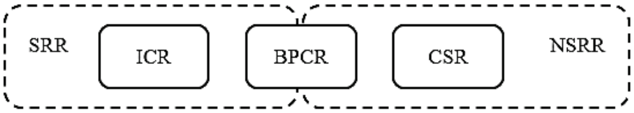


Figure 7. Reversib*l*e composite rule classification.
Source: The Authors.

The number of composite reversible rules N_{CRR} for a given r value is calculated using eq. (6)-(9), where N_{BPCR}, N_{CSR} and N_{ICR} represent the number of BPCR, CSR and ICR type rules, respectively.

$$N_{BPCR}(r) = 2^r \times (N_{BPCR}(r-1) + N_{BPCR}(r-2) + 1),\quad N_{BPCR}(1) = 0,\quad N_{BPCR}(2) = 2 \tag{6}$$

$$N_{CSR}(r) = 2^{r+1} \tag{7}$$

$$N_{ICR}(r) = 2^r \tag{8}$$

$$N_{CRR}(r) = N_{BPCR}(\mathrm{r}) + N_{CSR}(r) + N_{ICR}(r) \tag{9}$$

Note that N_{CRR} grows considerably as the r value increases.

3.3. Composite reversible rules for LCA encryption

From possible composite reversible rules with r value equal to 8, sixteen pairs were selected with the purpose of establish a different 4-bit sequence identifier for each one, they are listed in Table 2. The first eight pairs are CSR, and the eight remaining pairs are BPCR. The rules on the first column (rule set 1) are used in encryption, and the remaining (rule set 2) in decryption, that is, in original information recovery.

As a strategy for the selection of eight first pairs of rules (numbered from 0 to 7 in Table 2), entropy values of the 256 possible 8-bit strings, finding 70 different combinations with entropy value 1, that is, strings which have four zeros and four ones in any order. From this string set, a group of eight was selected with a Hamming distance equal to four or six [35]. With these strings, eight CSR were constructed, first four are composed of 'A' and '$\bar{A}$'; and remaining four are composed of 'C' and '$\bar{C}$', being the number 1 replaced by 'A' or 'C' and the number 0 replaced by '$\bar{A}$' or '$\bar{C}$'.

Table 2.
Rule sets for encryption and decryption.

Index	Identifier	Rule set 1	Rule set 2
0	0000	$AAA\bar{A}\bar{A}A\bar{A}\bar{A}$	$CC\bar{C}\bar{C}C\bar{C}\bar{C}C$
1	0001	$A\bar{A}\bar{A}A\bar{A}\bar{A}AA$	$\bar{C}\bar{C}C\bar{C}\bar{C}CCC$
2	0010	$\bar{A}A\bar{A}\bar{A}AAA\bar{A}$	$C\bar{C}\bar{C}CCC\bar{C}\bar{C}$
3	0011	$\bar{A}\bar{A}AAA\bar{A}\bar{A}A$	$\bar{C}CCC\bar{C}\bar{C}C\bar{C}$
4	0100	$CC\bar{C}CC\bar{C}\bar{C}\bar{C}$	$\bar{A}AA\bar{A}AA\bar{A}\bar{A}$
5	0101	$\bar{C}\bar{C}CC\bar{C}CC\bar{C}$	$\bar{A}\bar{A}\bar{A}AA\bar{A}AA$
6	0110	$C\bar{C}\bar{C}\bar{C}CC\bar{C}C$	$AA\bar{A}\bar{A}\bar{A}AA\bar{A}$
7	0111	$\bar{C}CC\bar{C}\bar{C}\bar{C}CC$	$A\bar{A}AA\bar{A}\bar{A}\bar{A}A$
8	1000	$BB\bar{B}BC\bar{A}\bar{C}\bar{A}$	$BB\bar{B}B\bar{C}A\bar{C}\bar{A}$
9	1001	$\bar{B}\bar{C}AB\bar{C}AB\bar{B}$	$\bar{B}C\bar{A}BC\bar{A}B\bar{B}$
10	1010	$C\bar{A}\bar{B}\bar{B}BC\bar{A}B$	$\bar{C}A\bar{B}\bar{B}B\bar{C}AB$
11	1011	$\bar{B}BC\bar{A}\bar{B}\bar{B}CA$	$\bar{B}B\bar{C}A\bar{B}\bar{B}CA$
12	1100	$\bar{B}\bar{C}ACA\bar{B}\bar{B}B$	$\bar{B}C\bar{A}CA\bar{B}\bar{B}B$
13	1101	$\bar{B}B\bar{B}\bar{C}ACA\bar{B}$	$\bar{B}B\bar{B}C\bar{A}CA\bar{B}$
14	1110	$CAB\bar{C}\bar{A}B\bar{B}\bar{B}$	$CAB\bar{C}\bar{A}B\bar{B}\bar{B}$
15	1111	$B\bar{B}\bar{C}A\bar{B}\bar{C}AB$	$B\bar{B}C\bar{A}\bar{B}C\bar{A}B$

Source: The Authors.

Similarly, as a strategy for the selection of rest pairs of rules (numbered from 8 to 15 in Table 2), the set of 15 possible 8-bit strings with exactly two pairs of consecutive ones are considered because their entropy is also 1, and a group of eight with a Hamming distance equal to two, four or six was selected from this set. With these strings, eight BPCR were constructed, being each pair of ones replaced by the elementary rule pair 'CA', '$\bar{C}$A', '$\bar{C}\bar{A}$' or 'C$\bar{A}$', and each zero is replaced by 'B' or '$\bar{B}$'.

3.4. Regions of interest detection and extraction

In the encryption process, the sender stores the original video with hidden RoIs, the isolated cipher RoIs and their location in the video frames. Thus, a receiver can recover the encrypted video completely through the stored data and the correct keys.

The encryption method is tested with a straightforward mechanism for RoI detection, that consider perceptible motion patterns in video as RoIs. An initial frame is considered as background, and the next frames are compared with initial frame to determine the pixels with changed value. If a group of pixels with changed value is connected and has a size greater or equal than 256 pixels, it will be enclosed by a rectangle and considered as a RoI. If two RoIs are 16 pixels away or less, they are grouped into an only RoI. Finally, each RoI dimensions are rounded to the closest multiple of 8 in order to allow a correct encryption process. This process was implemented through a routine in Matlab, using Image Processing Toolbox and Image Acquisition Toolbox libraries.

3.5. Key generation

Starting with an LCA from a predetermined image (such as example in Fig. 3) an initial sequence of 1027 consecutive bits is extracted to form a 1027 columns matrix along with the LCA bits from a RoI, repeating, if required, bits from initial sequence to fill all columns. Subsequently, XOR operation is performed with each column entries, obtaining a 1027-bit sequence that will be the key to encrypt every RoI in a frame.

The first 1023 bits in the key are named $\boldsymbol{ps}_0$, and the remaining four bits in its decimal representation define the value N_0 that indicates the iteration number to evolve $\boldsymbol{ps}_0$ with elementary rule 30.

3.6. Cryptographic method steps

The encryption proposal consists of eight steps that are applied on each video frame.

Step 1: RoIs detection, extraction and replacement by black rectangles in the original frame for storage.

Step 2: Transpose RoIs which height is greater than their width.

Step 3: A RoI in the frame is selected for key generation as explained in Section 3.5. RoIs in different frames are encrypted with different keys.

Step 4: Let $\boldsymbol{s}_{ECA}$ be an ECA initial state, and N the number of evolutions with elementary rule 30, the 1023-bit sequence $\boldsymbol{ps}$ is calculated by expression in eq. (10), assigning to $\boldsymbol{s}_{ECA}$ and N the previously defined values of $\boldsymbol{ps}_0$ and N_0, respectively.

$$\boldsymbol{ps} = rule30(\boldsymbol{s}_{ECA}, N) \qquad (10)$$

Step 5: Bit in position 1024 from the key is appended to $\boldsymbol{ps}$ and read from right to left in 4-bit segments. Decimal representation of each segment is obtained adding one, avoiding the appearing of zeros, forming a list of 256 integer numbers in the interval from 1 to 16 called multiplier sequence $\boldsymbol{ms}$.

Step 6: Composite rule identifiers sequence **R**, expressed by eq. (11) is obtained from algorithm 1, assuming that $\boldsymbol{ps}$ and $\boldsymbol{ms}$ have periodic boundary conditions, where N_S, previously specified in eq. (3), is the maximum number of CCAs in the LCA that is obtained with the RoI of the largest width or height in the frame, and R_i is a 4-bit string associated to a composite rule in Table 2.

$$\mathbf{R} = \{R_1, R_2, \ldots R_i, \ldots\ R_{N_S}\} \qquad (11)$$

In this step, rule 30 (eq. 10) is used to evolve $\boldsymbol{ps}$, that along with multiplication and modulo of integer numbers in $\boldsymbol{ms}$ contribute to guarantee key sensitivity. The values in $\boldsymbol{ms}$ are used in the algorithm 1 to define numbers for the $\boldsymbol{ps}$ evolution with elementary rule 30 and determine the js values that acts as a displacement number for $\boldsymbol{ps}$. Note that the bits that constitute **R** are 4-bit sequences coming from a specific $\boldsymbol{ps}$ state.

Step 7: Evolution of LCAs obtained from each RoI. Each row that constitutes the layers in the LCA is considered the initial state of an CCA which corresponding evolution rule is identified by R_i. For encryption, the bits that form each LCA are reordered in three different ways:

a) By rows for each layer.
b) By layers for each column.
c) By layers for each row.

One evolution is performed after each rearrangement, thus, every LCA evolves three times. For decryption, each LCA evolve before each rearrangement, which order is inverted.

Algorithm 1 Composite rule identifiers extraction

```
Input: ps sequence, ms sequence, Ns value, N0 value;
Output: Composite rule identifiers sequence R;
ps=rule30(ps, ms(N0 + 1));
j = 1;
for i = 1 to Ns do
        R_i = ps(j to j + 3);
        js = i * pow(ms(i), 2) mod 257;
        j = j + js + 4;
        if j mod 256 == 0
                ps = rule30(ps, ms(i));
        end if
end for
return R
```

Source: The Authors.

Step 8: Obtain encrypted RoIs from evolved LCAs. Transpose the previously transposed RoIs in Step 2 to recover their initial dimensions.

The sender stores the cipher RoIs, and the receiver decrypt them to completely recover each frame of video. Decryption uses the second rule set in Table 2 to perform the same process except for steps 1 and 3, because the decryption key for original video recovery is the same encryption key.

4. Performance evaluation, analysis and discussion of results

To corroborate the effectiveness of the proposed encryption and decryption process, a series of test and performance measures based on the image encryption literature [1-17] were performed. Each test allows to deduce that the proposed method excels as a security alternative and it is applicable in real environments.

4.1. Experimental tests

In order to show that proposed method is functional, robust and effective, a surveillance video segment coming from a security camera in the Universidad Distrital Francisco José de Caldas from Bogotá was encrypted. Fig. 8 shows a video frame, RoIs extraction and hiding, encryption and recovery of original image results.

Executions of this algorithm were performed on a computer with 8GB RAM and processor Intel Core i3 in the Matlab 2018a platform. Encryption and decryption times in for different sizes of image are shown in Table 3.

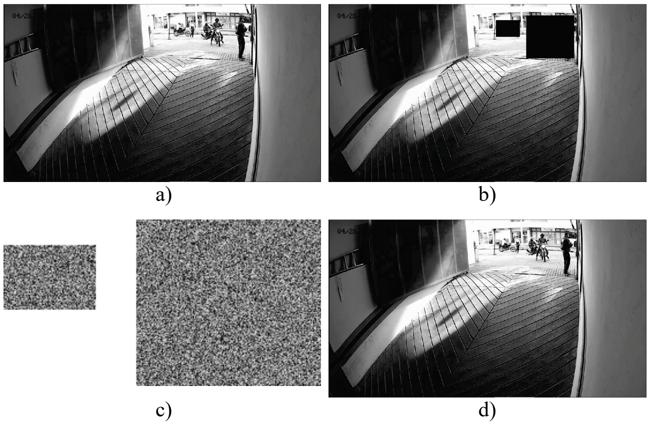

a)
b)
c)
d)

Figure 8. Application of the proposed method in a surveillance video. (a) Original frame, (b) Frame with hidden RoIs, (c) Cipher RoIs, (d) Recovered frame through decryption process.
Source: The Authors.

Table 3.
Encryption and decryption time in milliseconds for proposed method.

Size of image	Encryption time (ms)	Decryption time (ms)
256 x 256	184	166
512 x 512	720	704

Source: The Authors.

Proposed algorithm depends on image dimensions, that is, the number of CCAs that evolve in Step 7 and their length. Therefore, its computational complexity is $O(3 \times M \times N)$.

4.2. *Key space analysis*

A cipher key in the proposed method is formed by 1027 bits. Thus, the key space size to encrypt a video frame or image is equal to 2^{1027}, that is greater that other proposals with same purpose as [1,3,6,8-15], which guarantees resistance to brute force attacks. In addition, it grows proportionally with the number of frames in a video.

The following subsections refer to four images that have been encrypted with the proposed method. Original and cipher images are shown in Fig. 9.

4.3. *Histogram analysis*

In Fig. 10, histograms of original and cipher images from Fig. 9 are presented, proving that frequency distribution of pixel values in cipher images is uniform as expected.

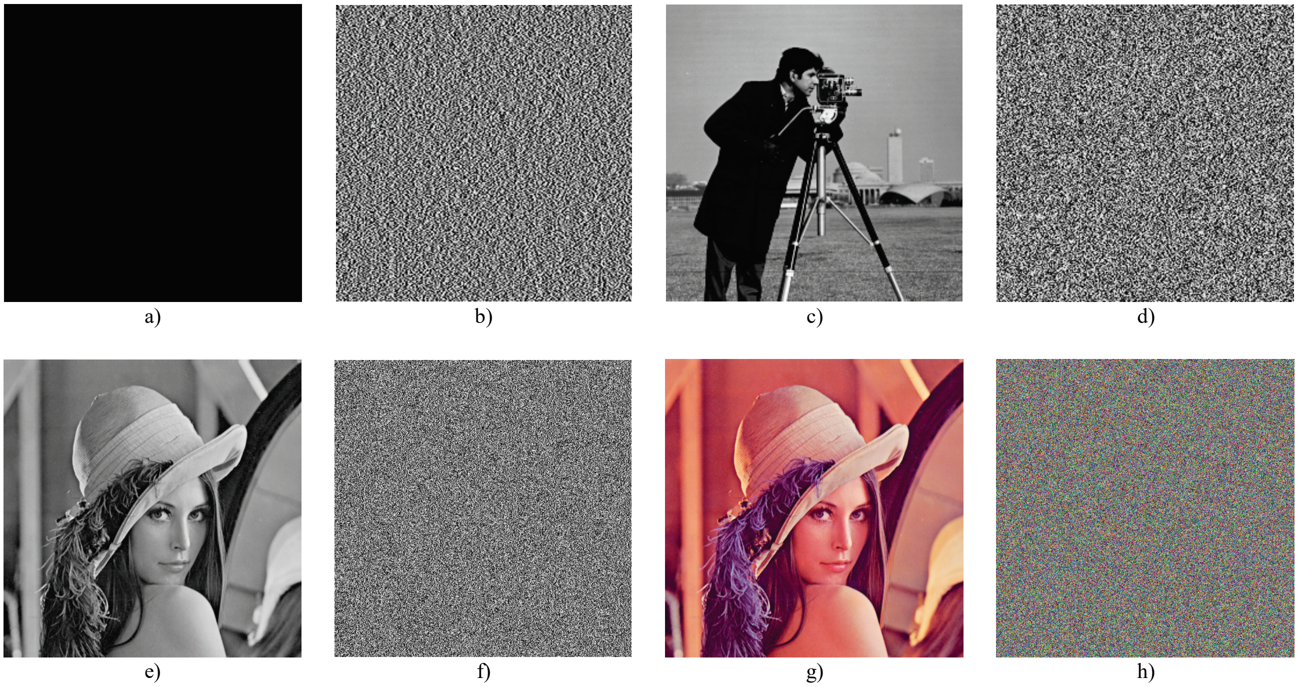


Figure 9. Original and encrypted images. (a) Black image with size 256 x 256, (b) Encrypted black image, (c) Cameraman with size 256 x 256, (d) Encrypted camera*m*an, (e) Grayscale Lena with size 512 x 512, (f) Encrypted grayscale Lena, (g) Color Lena with size 512 x 512, (h) Encrypted color Lena.
Source: The Authors.

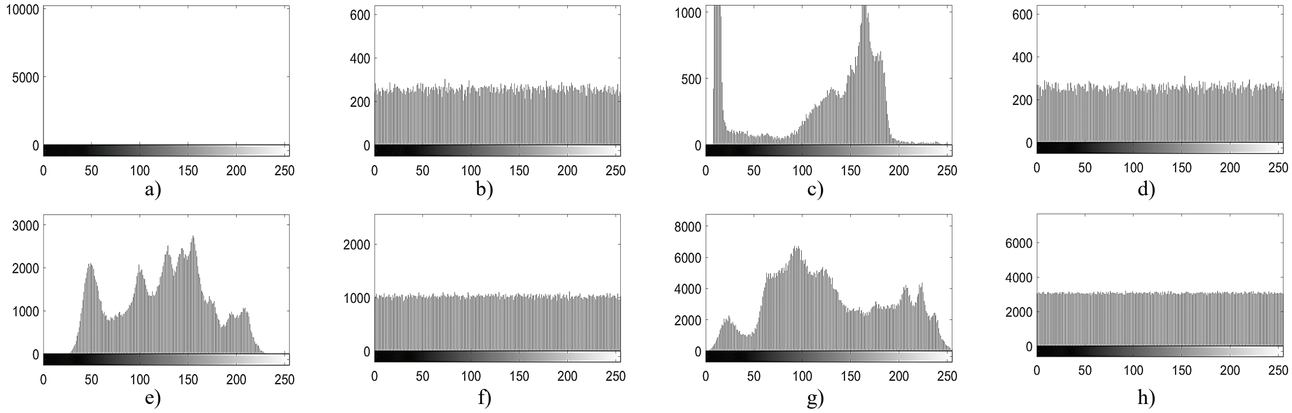


Figure 10. Histogram of images from Fig. 9. (a) Black image, (b) Encrypted black image, (c) Cameraman, (d) Encrypted *c*ameraman, (e) Grayscale Lena, (f) Encrypted grayscale Lena, (g) Color Lena, (h) Encrypted color Lena.
Source: The Authors.

Table 4.
Entropy values for original and cipher i*m*ages.

Entropy	Black image	Cameraman	Grayscale Lena	Color Lena
Plain image	0,0000	7,0097	7,4451	7,7502
Cipher image	7,9972	7,9972	7,9993	7,9998

Source: The Authors.

4.4. Entropy analysis

For a grayscale image I, the entropy $H(I)$ measures the pixel distribution values, which optimal values for a cipher image tends to 8 [13, 30]. It is defined by eq. (12).

$$H(I) = -\sum_{i=1}^{L} p(x_i)log_2(p(x_i)) \tag{12}$$

Where x_i is the i_{th} gray value of I, $p(x_i)$ is the occurrence probability of x_i, and L is the number of pixels that constitute the image. For color images, this conception is applied on each RGB channel. Entropy values of original and cipher images in Fig. 9 are listed in Table 4, proving that encrypted images by proposed method present high randomness.

Obtained entropy values for cipher images are comparable to the values obtained in [1, 3, 5-13, 16, 17]. In addition, entropy value of cameraman cipher image in [13] is 7.988, less than the obtained with this method.

4.5. Differential attack analysis

Let E_1 and E_2 denote two images which result of encrypt two almost identical images with one-pixel difference, the Number of Pixel Changed Rate (NPCR) is the number of pixels at the same location in E_1 and E_2 with different values, and it is defined by eq. (13)-(14).

$$D(i,j) = \begin{cases} 0, & E_1(i,j) = E_2(i,j) \\ 1, & otherwise. \end{cases} \tag{13}$$

$$NPCR = \frac{1}{M \times N}\sum_{i,j} D(i,j) \tag{14}$$

The Unified Averaged Change Intensity (UACI) is the average absolute value of the difference between each pair of pixels at the same location in E_1 and E_2, and it is defined by eq. (15).

$$UACI = \frac{1}{M \times N}\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255} \tag{15}$$

For two random images, NPCR and UACI optimal values are nearly 99.6094% and nearly 33.4635%, respectively [36].

Let I_1 denote an image from Fig. 9, I_2 equal to I_1 except for a modified pixel value. E_1 and E_2 are the images obtained by encrypt I_1 and I_2, respectively. Minimum, maximum and average obtained values of NPCR and UACI in 10 executions are presented in Table 5, which are close to the optimal values, proving that the proposed method resists differential attacks.

Table 5.
NPCR and UACI values.

Image	NPCR			UACI		
	Minimum	Maximum	Average	Minimum	Maximum	Average
Cameraman	0,99573	0,99637	0,99607	0,33246	0,33648	0,33496
Color Lena	0,99589	0,99618	0,99607	0,33370	0,33563	0,33469

Source: The Authors.

4.6. Correlation of adjacent pixels

The correlation coefficient for an image is a decimal value between -1 and 1 defined by eq. (16)-(19) and it is calculated from a random adjacent pixel sample in different directions. In plain images, the correlation coefficient is close to 1, and the expected value in cipher images is close to 0 [13].

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{16}$$

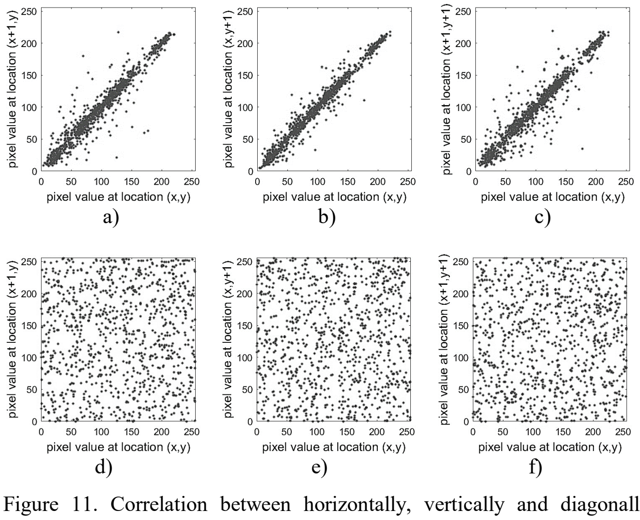
$$D(x) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(x))^2 \tag{17}$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n} (x_i - E(x))(y_i - E(y)) \tag{18}$$

Table 6.
Correlation coefficients for each RGB channel in two images.

Coefficient	Original color image Lena			Cipher color image Lena		
	Red	Green	Blue	Red	Green	Blue
Horizontal	0,9757	0,9898	0,9686	0,0304	0,0379	0,0063
Vertical	0,9614	0,9830	0,9540	0,0236	0,0074	0,0618
Diagonal	0,9239	0,9617	0,9175	0,0184	0,0277	0,0333

Source: The Authors.



a) b) c)

d) e) f)

Figure 11. Correlation between horizontally, vertically and diagonally adjacent pixels in the green channel of the original color image Lena (a)-(c), and the cipher color image Lena (d)-(f).
Source: The Authors.

$$CC(x,y) = \frac{cov(x,y)}{\sqrt{D(x)\,D(y)}} \tag{19}$$

In order to measure the existent correlation between adjacent pixels in images from Fig. 9(g) and Fig. 9(h), a set of 1000 random pairs of pixels in horizontal, vertical and diagonal position were considered for each RGB channel.

Obtained values are grouped in Table 6, showing an almost null correlation value in every channel of the cipher image.

Fig. 11 shows the horizontal, vertical and diagonal values of adjacent pixels in the green channel for the original and the cipher image.

4.7. Key sensitivity

A feature of secure cryptosystems is key sensitivity, that means, a slight change in the cipher key must produce a completely different cipher result [30].

In order to prove key sensitivity from the sender side, the image from Fig. 9(c) was encrypted using two keys K_1 and K_2 with one-bit difference, obtaining the results shown in Fig. 12. The UACI and NPCR values related to the images in Fig. 12 (b) and (c) are 99.61% and 33.42% respectively, that implies that these cipher images are completely different.

In order to prove key sensitivity from the receiver side, K_1 are K_2 are used to decrypt the image from Fig. 12(b), obtaining the results shown in Fig. 13.

Note that original image is completely recovered by using K_1, but it is not possible to retrieve encrypted information by using K_2.

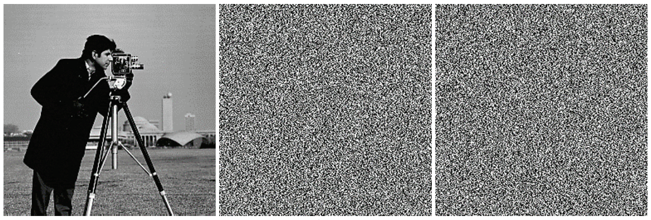


Figure 12. Encryption of image with two similar keys. (a) Original image, (b) Encrypted image using K$_1$, (c) Encrypted image using K$_2$.
Source: The Authors.

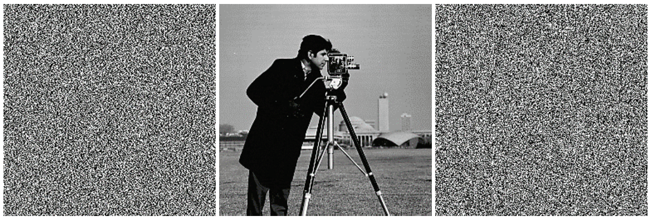


Figure 13. Decryption of a cipher image with two similar keys. (a) Cipher image, (b) Decrypted image using K$_1$, (c) Decrypted image using K$_2$.
Source: The Authors.

It is remarked that every sensitivity test shows similar results, independently of the position occupied by the difference bit between K_1 and K_2. Therefore, this method presents key sensitivity.

The results presented in this section expose that the proposed method resists brute force attacks, correlation attacks, differential attacks, chosen-plaintext attacks according to performance results in encryption of Fig. 9(a), and known-plaintext attacks as an effect of the strategy in Section 3.3, which frustrates the possibility of obtain the rules in **R** without having the cipher key.

Although there are few encryption works focused on surveillance videos using the guideline proposed in this work, it was possible to calculate a collection of performance measures reported independently in several references, highlighting that the obtained measures are comparable with those in [1,3,5-13,15-17]. That implies high security of the proposed method and makes this work a significant contribution in the fields of image and video encryption.

5. Conclusions and future work

The implemented CCA-based encryption method presents quantitative and qualitative optimal performance values, demonstrating that is an effective security alternative. Nevertheless, the efficiency of this method is dependent on the size of the RoIs.

The proposed method is extensible and modifiable since not only a high number of composite reversible rules can be applied to the cryptosystem, but also it is possible to increase or reduce key size because it is not dependent on the size of the RoIs.

Rectangular shape of RoIs could be adjusted to irregular contours with the aim of increase encryption efficiency. In addition, it is possible to modify the RoIs detection and extraction mechanism to avoid equivocal motion perceptions such as shadows reflected by lighting.

Combining the behavior of elementary rule 30 with the multiplication and modulo operations to random numbers in the developed algorithm increases randomness and sensitivity of results in the proposed method, that implies the impossibility of successful fraudulent attacks.

References

[1] Pan, H., Lei, Y. and Jian, C., Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP Journal on Image and Video Processing, 2018(1), pp. 1-10, 2018. DOI: 10.1186/s13640-018-0386-3

[2] Dongare, A.S., Alvi, A.S. and Tarbani, N.M., An efficient technique for image encryption and decryption for secured multimedia application. International Research Journal of Engineering and Technology (IRJET), 4(4), pp. 3186-3190, 2017.

[3] Zhang, X. and Wang, X., Digital image encryption algorithm based on elliptic curve public cryptosystem. IEEE Access, 6, pp. 70025-70034, 2018. DOI: 10.1109/ACCESS.2018.2879844

[4] Chai, X., Fu, X., Gan, Z., Lu, Y. and Chen, Y., A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 166, pp. 44-62, 2019. DOI: 10.1016/j.sigpro.2018.09.029

[5] Naseri, M., Abdolmaleky, M., Laref, A., Parandin, F., Celik, T., Farouk, A., Mahamadi, M. and Jalanian, H., A new cryptography

algorithm for quantum images. Optik 155, pp. 44-62, 2019. DOI: 10.1016/j.ijleo.2016.09.123

[6] Yang, Y-G., Tian, J., Lei, H., Zhou, Y. and Shi, W., Novel quantum image encryption using one-dimensional quantum cellular automata. Information Sciences, 345, pp. 257-270, 2016. DOI: 10.1016/j.ins.2016.01.078

[7] Chen, B., Yu, M., Tian, Y., Li, L., Wang, D. and Sun, X., Multiple-parameter fractional quaternion Fourier transform and its application in colour image encryption. IET Image Process, 12(12), pp. 2238-2249, 2018. DOI: 10.1049/iet-ipr.2018.5440

[8] Sneha, P.S., Sankar, S. and Kumar, A.S., A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. Journal of Ambient Intelligence and Humanized Computing (2019), pp 1-20, 2019. DOI: 10.1007/s12652-019-01385-0

[9] Attaullah, A.J. and Shah, T., Cryptosystem techniques based on the improved Chebyshev map: an application in image encryption. Multimedia Tools and Applications (2019), pp. 1-20, 2019. DOI: 10.1007/s11042-019-07981-8

[10] Wang, X., Zhu, X. and Zhang, Y., An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access 6, pp. 23733-23746, 2018. DOI: 10.1109/ACCESS.2018.2805847

[11] Bakhshandeh, A. and Eslami, Z., An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering, 51(6), pp. 665-673, 2013. DOI: 10.1016/j.optlaseng.2013.01.001

[12] Wang, X. and Luan, D., A novel image encryption algorithm using chaos and reversible cellular automata. Communications in Nonlinear Science and Numerical Simulation, 18(11), pp. 3075-3085, 2013. DOI: 10.1016/j.cnsns.2013.04.008

[13] Zhang, X., Seo, S. and Wang, C., A lightweight encryption method for privacy protection in surveillance videos. IEEE Access, 6, pp. 18074-18087. DOI: 10.1109/ACCESS.2018.2820724

[14] Zhang, X., Zhang, H. and Xu, C., Reverse iterative image encryption scheme using 8-layer cellular automata. KSII Transactions on Internet and Information Systems, 10(7), pp. 3397-3413, 2016. DOI: 10.3837/tiis.2016.07.029

[15] Wang, Y., Zhao, Yi., Zhou, Q. and Lin, Z., Image encryption using partitioned cellular automata. Neurocomputing, 275, pp. 1318-1332, 2018. DOI: 10.1016/j.neucom.2017.09.068

[16] Li, K., Sun, M., Li, L. and Chen J., Image encryption algorithms based on non-uniform second-order reversible cellular automata with balanced rules. In: Huang, D.S., Bevilacqua, V., Premaratne, P. and Gupta, P., eds. Intelligent computing theories and application, ICIC 2017, part of Lecture Notes in Computer Science. Springer, Cham, Liverpool, UK, 2017. pp. 445-455. DOI: 10.1007/978-3-319-63309-1_41

[17] Zhang, X., Wang, C., Zhong, S. and Yao, Q., Image encryption scheme based on balanced two-dimensional cellular automata. Mathematical Problems in Engineering (2013), pp. 1-10, 2013. DOI: 10.1155/2013/562768

[18] George, S.N., Augustine, N. and Pattathil, D.P., Audio security through compressive sampling and cellular automata. Multimedia Tools and Applications, 74(23), pp. 10393-10417, 2015. DOI: 10.1007/s11042-014-2172-2

[19] Orúe, A., Contribución al estudio del criptoanálisis y diseño de los criptosistemas caóticos, Tesis Dr., Escuela Técnica Superior de Ingenieros de Telecomunicación (ETSIT), Universidad Politécnica de Madrid (UPM), España, 2013, 260 P.

[20] Kari, J., Theory of cellular automata: a survey. Theoretical Computer Science, 334(1-3), pp. 3-33, 2005. DOI: 10.1016/j.tcs.2004.11.021

[21] Bilotta, E. and Pantano, P., Cellular Automata and Complex Systems: Methods for Modeling Biological Phenomena. IGI Global, 2010.

[22] Deutsch, A. and Dormann, S., Cellular Automaton Modeling of Biological Pattern Formation: Characterization, Applications and Analysis. Birkhäuser Boston, 2005.

[23] Auer S., Bliem A., Engel D., Uhl A. and Unterweger A., Bitstream-based JPEG encryption in real-time. International Journal of Digital Crime and Forensics, 5(3), pp. 1-14, 2013. DOI: 10.4018/jdcf.2013070101

[24] Mateu, O., Análisis y detección de objetos de primer plano en secuencias de video, Proyecto final de carrera, Universitat Politècnica de Catalunya, Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona, 2009, 67 P.

[25] Negri, P. and Garayalde, D., Pedestrian tracking using probability fields and a movement feature space. DYNA 84(200), pp. 217-227, 2017. DOI: 10.15446/dyna.v84n200.57028

[26] Sun, X., Wu, P. and Hoi, S., Face detection using deep learning: an improved faster RCNN approach. Neurocomputing, 299, pp. 42-50, 2018. DOI: 10.1016/j.neucom.2018.03.030

[27] Zhou, X., Yao, C., Wen, H., Wang, Y., Zhou, S., He, W. and Liang, J., EAST: an efficient and accurate scene text detector. Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, 2017, pp. 2642-2651. DOI: 10.1109/CVPR.2017.283.

[28] Wolfram, S., A new kind of science. Wolfram Media, Champaign, IL, 2002 [accessed August 1st, 2019]. Available at: https://www.wolframscience.com/nks.

[29] Stallings, W., Cryptography and network security: principles and practice. 7th ed., Pearson Education, 2017.

[30] Shannon, C., Communication theory of secrecy systems. Bell System Technical Journal, 28(4), pp. 656-715, 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x

[31] Devaney, R.L., An Introduction to Chaotic Dynamical Systems. 2nd ed., Addison-Wesley, 1989.

[32] Cattaneo, G., Formenti, E., Margara, L. and Mauri, G., On the dynamical behavior of chaotic cellular automata. Theoretical Computer Science, 217(1), pp. 31-51, 1999. DOI: 10.1016/S0304-3975(98)00149-2

[33] Coleman, I., Finite-width elementary cellular automata. Senior Project Archive, Whitman College, WA, 2011.

[34] Gage, D., Laub, E. and McGarry, B., Cellular automata: is rule 30 random?. Proceedings of the Midwest NKS Conference, Indiana University, 2005.

[35] Hamming, R.W., Error detecting and error correcting codes. The Bell System Technical Journal, 29(2), 1950. DOI: 10.1002/j.1538-7305.1950.tb00463.x

[36] Wu, Y., Noonan, J.P. and Agaian, S., NPCR and UACI randomness tests for image encryption. Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), pp. 31-38, 2011.

L.M. Cortés-Martinez, received the BSc. Eng. in Systems Engineering from the Universidad Distrital Francisco José de Caldas, Colombia, in 2019. His research interests include cryptography, cellular automata, fuzzy logic and algorithmic composition of music. He is member of the Grupo de Complejidad de la Universidad Distrital (ComplexUD), Colombia.
ORCID: 0000-0003-0606-3742

L.D. Alvarado-Nieto, received the BSc. Eng in Systems Engineering from the Universidad Distrital Francisco José de Caldas, Colombia, in 1991, the MSc. in Systems Engineering in the Universidad Nacional de Colombia in 2003, and the PhD degree in Computer Science and Artificial Intelligence in the Universidad de Oviedo, Spain, in 2002. Currently, she is professor at the Engineering School of the Universidad Distrital Francisco José de Caldas, and Director of the Grupo de Complejidad de la Universidad Distrital (ComplexUD), Colombia.
ORCID: 0000-0002-1305-3123

E.I. Amaya-Barrera, received the BSc. in Mathematics in the Universidad Distrital Francisco José de Caldas in 1995, and the MSc. in Mathematics Sciences in the Universidad Nacional de Colombia in 1999. Currently, she is professor in the Engineering School of Universidad Distrital Francisco José de Caldas, Colombia. She is member of the Grupo de Complejidad de la Universidad Distrital (ComplexUD), .
ORCID: 0000-0002-8845-5901