WAVELET MULTIFRACTAL DETRENDED FLUCTUATION ANALYSIS OF ENCRYPTION AND DECRYPTION MATRICES

J. S. MURGUÍA[†1], M. MEJÍA CARLOS[‡], C. VARGAS-OLMOS[‡], M. T. RAMÍREZ-TORRES[‡], H.C. ROSU[⋄]

[†] Facultad de Ciencias, Universidad Autónoma de San Luis Potosí (UASLP)
Álvaro Obregón No. 64 Centro, C. P. 78000 San Luis Potosí, S.L.P., Mexico
[‡] Instituto de Investigación en Comunicación Óptica (UASLP)
Álvaro Obregón No. 64 Centro, C. P. 78000 San Luis Potosí, S.L.P., Mexico
[⋄] IPICyT, Instituto Potosino de Investigacion Cientifica y Tecnologica,
Apartado Postal 3-74 Tangamanga, 78231 San Luis Potosí, México

Int. J. Mod. Phys. C 24(9), 1350069 (2013)

Abstract

In this paper, we study in detail the multifractal features of the main matrices of an encryption system based on a rule-90 cellular automaton. For this purpose we consider the scaling method known as the wavelet transform multifractal detrended fluctuation analysis (WT-MFDFA). In addition, we analyze the multifractal structure of the matrices of different dimensions, and find that there are minimal differences in all the examined multifractal quantities such as the multifractal support, the most frequent singularity exponent, and the generalized Hurst exponent.

DOI: 10.1142/S0129183113500691
Keywords: Cryptography; wavelet transform; multifractal spectrum
PACS numbers: 05.40.-a, 05.45.Df, 05.45.Tp

1 Introduction

Elaborating algorithms or methods to analyze the singular behavior that may be hidden in functions, signals, distributions, or time series, has been a lasting goal along many decades. At the present time, there are a large number of methods or techniques to analyze or detect singular behavior.[1, 2] To recall a few, we have the structure function method,[3] the wavelet transform module maxima (WTMM) method,[3, 4, 5, 6, 7, 8] the detrended fluctuation analysis (DFA),[9] and its variants.[1, 10, 11]

In 2005, Manimaran *et. al*[12] proposed to combine the discrete wavelet transform with DFA procedures. Based on this, Murguía *et. al*[13] implemented and used this approach to investigate the multifractal behavior of the time series of the row-sum signals of certain cellular automata rules. This technique, denominated as multifractal detrended fluctuation analysis based on the wavelet transform (WT-MFDFA), was also used in Ref. [14] to obtain the multifractal characteristics of complementary cellular automata (CA) rules for different initial conditions achieving a better performance compared with other multifractal methods. In a previous work, we have also used the WT-MFDFA method to reveal multifractal features of a sequence matrix that generated recursively the pseudo-random sequences of an encryption system based on the CA rule 90.[15] In fact, the main functions of such an encryption system are based on both the forward and backward evolution of the CA rule 90. In Ref. [16], the matrix approach was extended to almost all the components of the encryption system. This situation motivates us to apply the efficient WT-MFDFA method to reveal multifractal properties of the sum of ones in the sequences of the rows of the encryption main matrices that can be used for their characterization. There is a work that related some multifractal

[1]Corresponding author. E-mail: ondeleto@uaslp.mx

parameters to encrypted information,[23] but there the analysis is performed on encrypted signals and not directly to the encryption elements of the encryption system as we do here.

The organization of this paper is as follows. In Section 2, we briefly give a description of the encryption system considered in terms of the matrix approach. Section 3 contains the results obtained by applying the WT-MFDFA technique to the encryption matrices. In addition, we also vary the dimensions of the encryption matrices to see how the WT-MFDFA results depend on this important parameter.

2 Encryption System Model

In this work we consider the encryption scheme used in Ref. [17], where the synchronization phenomenon of cellular automata (CA) has been applied to devise the two families of permutations and an asymptotically perfect pseudo-random number generator. The encryption system is based on the usage of CA that evolves according to the local rule $x_i^{t+1} = \left(x_{i-1}^t + x_{i+1}^t\right) \bmod 2$, which corresponds to the rule 90. The phenomenon of synchronization in coupled pairs of CA is described in detail in Ref. [18], where it was found that a pair of coupled CA can synchronize if every pair of consecutive coordinates is separated by a block of $\left(2^k - 1\right)$ uncoupled sites.

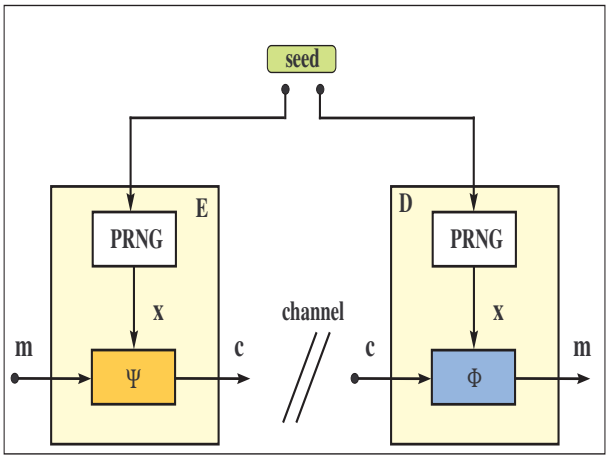

Fig. 1: The encryption model considered in this work with its main components: the indexed families of permutations, Ψ and Φ, and the pseudorandom generator of keys.

Figure 1 shows the complete encryption system. Basically, the class of the considered block cryptosystem transforms a plain text sequence $\mathbf{m}$ to a sequence $\mathbf{c}$, called the cipher-text. The transformation $\mathbf{m} \mapsto \mathbf{c}$ is selected from an indexed family of permutations $\Psi = \{\psi_{\mathbf{x}} : M \to C | \mathbf{x} \in X\}$ by choosing an index $\mathbf{x}$ from the set of indices X. The sets M, C and X are all sets of binary words of length N, i.e., Z_2^N, where $Z_2 = \{0, 1\}$. The words in M and C are called the clear-blocks and cipher-blocks, respectively, whereas the words in the set of indices X are the encyphering keys. To disclose from the sequence of cipher-blocks, the cryptosystem also provides the family of inverse permutations $\Phi = \{\phi_{\mathbf{x}} : C \to M | \mathbf{x} \in X\}$ such that for every $\mathbf{x} \in X$ one has $\mathbf{m} = \phi_{\mathbf{x}}(\varphi_{\mathbf{x}}(m))$. Since the complete encryption scheme is private, the encryption and decryption processes use the same deterministic generator that is initialized with a common seed.

2.1 Matrix approach of the ESCA system

Murguía and collaborators[16] used a matrix approach to implement effectively the main components of the ESCA system. In fact, with some basic matrix operations or transformations on the main sequence matrix, denoted by $\mathbf{Q}_N$, they were able to implement the great majority of the stages involved in the encryption system, i.e., the family of permutations, and the pseudo-random number generator.

2.1.1 Encryption matrices: the Ψ permutation

For the encryption process, $\mathbf{c} = \Psi_{\mathbf{x}}(\mathbf{m})$, we require two matrices, $\mathbf{P}_N$ and $\mathbf{Q}_N$, such that

$$\mathbf{c} = \Psi_{\mathbf{x}}(\mathbf{m}) = [(\mathbf{P}_N \times \mathbf{x}) + (\mathbf{Q}_N \times \mathbf{m})] \bmod 2. \tag{1}$$

In this process, both matrices have dimensions $N \times N = (2^n - 1) \times (2^n - 1)$, for $n = 1, 2, 3, \ldots$. The $\mathbf{P}_N$ matrix is initially generated from the vector $\mathbf{p} = [p_1, p_2, \ldots, p_N]$, which constitutes the first row, and the components with position index $j = (2^n + 1) - 2^{i+1}$, $i = 0, 1, 2, \ldots, (n-1)$, have a value of 1, and 0 otherwise. The $(N-1)$ rows are generated by applying a right shift of one position of the previous row with a zero as its first value.

On the other hand, the main $\mathbf{Q}_N$ matrix can be generated initially from the vector $\boldsymbol{a} = [a_1, 0, \ldots, 0]$, where the component a_1 has a value of 1, and N is the number of bits, i. e., $\boldsymbol{a}$ is a vector with N components. This vector constitutes the first row of the matrix $\mathbf{Q}_N$ and the $(N-1)$ rows are generated by applying the CA rule 90 of the previous row with fixed boundary conditions of zero to the left and right sides. For instance, for $N = 15$ we have that $\mathbf{P}_{15}$, and $\mathbf{Q}_{15}$ have the form

$$\mathbf{P}_{15} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}, \quad \mathbf{Q}_{15} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}. \tag{2}$$

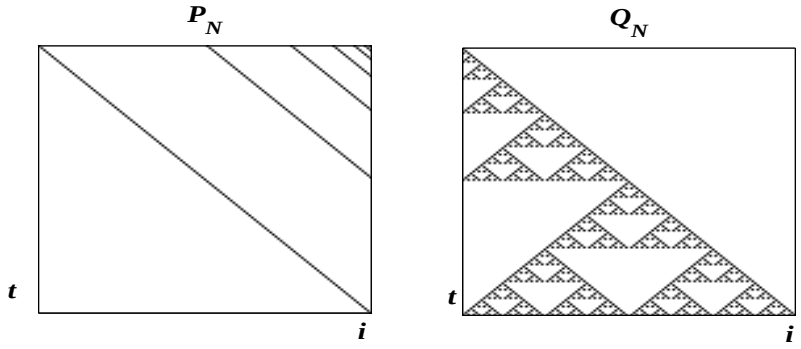

Fig. 2: Space-time pattern of the two matrices, P_N and Q_N, involved in the encryption process when $N = 127$ bits.

In Fig. 2 one can see the space-time pattern of the two encryption matrices for $N = 127$, $\mathbf{P}_{127}$ and $\mathbf{Q}_{127}$, where a pattern can be noticed with an appearance of a Sierpinski triangle in the $\mathbf{Q}$ matrix.

2.1.2 Decryption matrices: the Φ permutation

The matrix implementation of the inverse permutation $\mathbf{m} = \Phi_{\mathbf{x}}(\mathbf{c})$ has a similar structure of (1), that is,

$$\mathbf{m} = \Phi_{\mathbf{x}}(\mathbf{c}) = [(\mathbf{R}_N \times \mathbf{x}) + (\mathbf{T}_N \times \mathbf{c})] \bmod 2, \tag{3}$$

where the matrices have dimensions $N \times N = (2^n - 1) \times (2^n - 1)$, for $n = 1, 2, 3, \ldots$. From equation (1), $\mathbf{R}_N = [-\mathbf{Q}_N^{-1}\mathbf{P}_N] \mod 2$, whereas the $\mathbf{T}_N$ matrix is just the inverse of $\mathbf{Q}_N$, i.e., $\mathbf{T}_N = \mathbf{Q}_N^{-1} \mod 2$. As an example, and considering again $N = 15$, we have that the matrices $\mathbf{R}_{15}$ and $\mathbf{T}_{15}$ are

$$R_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}, \quad T_{15} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&1
\end{pmatrix}. \tag{4}$$

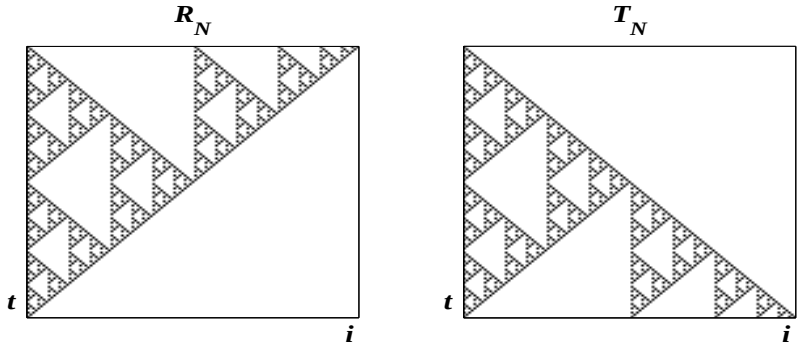

Fig. 3: Space-time pattern of the two matrices, R_N and T_N, involved in the decryption process when $N = 127$ bits.

In Fig. 3, the two resulting matrices, $\mathbf{R}_N$ and $\mathbf{T}_N$, for $n = 7$, i.e., $N = 127$ bits, are displayed. Since both matrices are the result of some matrix operations on the matrix $\mathbf{Q}_N$, it is clear that both of them must present a "similar" pattern.

2.1.3 The pseudo-random generator

In a previous work,[15] we introduced a sequence matrix $\mathbf{H}_N$ of dimensions $(2N+1) \times (2N+1)$ to compute feasibly the pseudo-random sequences of N bits. Since the matrix implementation of this matrix is described in Ref. [15] we omit its description and we only describe the format of the matrix $\mathbf{H}_N$ in terms of $\mathbf{Q}_N$, which is the following one

$$\mathbf{H}_N = \left(\begin{array}{c:c} \mathbf{Q}_N^{-1} & \hat{\mathbf{Q}} \\ \hdashline \mathbf{I} & \mathbf{0} \end{array}\right), \tag{5}$$

where $\mathbf{I}$ is the identity matrix with dimensions $(N+1) \times (N+1)$, and $\mathbf{0}$ is a zero matrix with dimensions $N \times (N+1)$. The matrix $\hat{\mathbf{Q}}$ has dimensions $N \times (N+1)$, where the first $(N-1)$ rows and N columns are comprised of the matrix $\mathbf{Q}_N^{-1}$, but without the first row. The components of the N-row and the $(N+1)$-column of $\hat{\mathbf{Q}}$ have a value of 0 except in the intersection of both, which has a value of 1. For instance, for $N = 15$ and considering the $\mathbf{Q}_{15}$ matrix of (2), we have the following matrix

$$
\mathbf{H}_{15} = \left(\begin{array}{cccccccccccccccc|cccccccccccccccc|c}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0&0\\
1&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0\\
1&0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right),
\tag{6}
$$

where we can directly see the role of the matrix $\mathbf{Q}_{15}$ in the implementation of the matrix $\mathbf{H}_{15}$.

3 Multifractal Properties of the Encryption and Decryption Matrices

In Ref. [13], we have employed the wavelet transform multifractal detrended fluctuation analysis (WT-MFDFA) to determine a possible multifractal behavior of some time series of cellular automata, in particular for rules 90, 105 and 150. It was found that these CA rules have an intrinsic multifractal behavior. In addition, in a previous work published in this journal,[15] we analyzed and found multifractal features of the matrix H_N, where this matrix was computed in a slightly different matrix approach. The WT-MFDFA method is based on the calculation of the so-called q-th order fluctuation function defined as

$$
F_q(s;m) = \left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} |F^2(\nu,s;m)|^{q/2} \right\}^{1/q}, \tag{7}
$$

where $q \in \mathbb{Z}$ with $q \neq 0$. The diverging behaviour for $q \to 0$ can be avoided by using a logarithmic averaging for the 0-th order fluctuation function $F_0(s;m) = \exp\left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} \ln|F^2(\nu,s;m)| \right\}$, see Ref. [10]. To assess the fractal scaling behavior of a time series, the fluctuation function $F_q(s;m)$ should reveal a power law scaling

$$
F_q(s;m) \sim s^{h(q)}. \tag{8}
$$

The exponent $h(q)$ is the generalized Hurst exponent since it depends on q, while the original Hurst exponent is $h(2)$. If $h(q)$ is constant for all q then the time series is monofractal, otherwise it has a multifractal behavior. In the latter case, one can calculate various other multifractal scaling exponents, such as the singularity (Hölder) spectrum $f(\alpha)$ of a signal or distribution $g(t)$ as the Legendre transform of the scaling exponent $\tau(q)$[19], i.e.,

$$
\alpha = \frac{d\tau(q)}{dq}, \qquad \text{and} \qquad f(\alpha) = q\alpha - \tau(q), \tag{9}
$$

where α characterizes the strength of singularities, and the Hölder spectrum of dimensions $f(\alpha)$ is a non-negative convex function that is supported on the closed interval $[\alpha_{\min}, \alpha_{\max}]$. The spectrum $f(\alpha)$

can be interpreted as the Hausdorff fractal dimension of the subset of data characterized by the Hölder exponent α.[7, 20] The most "frequent" singularity, which corresponds to the maximum of $f(\alpha)$, occurs for the value of $\alpha(q=0)$, whereas the boundary values of the support, $\alpha_{\min}$ for $q>0$ and $\alpha_{\max}$ for $q<0$, correspond to the strongest and weakest singularity, respectively. On the other hand, a linear behavior of $\tau(q)$ indicates monofractality whereas a non-linear behavior indicates a multifractal signal. Additionally, there is a relation between the scaling exponent $\tau(q)$ and the generalized Hurst exponents $h(q)$, which is given by $\tau(q)=qh(q)-1$.[10]

As an example, we carry out the analysis of the binomial multifractal model.[10, 21] For the multifractal time series generated through the binomial multifractal model, a series of $N=2^{n_{\max}}$ numbers x_k, with $k=1,\ldots,N$, is defined by

$$x_k = a^{n(k-1)}(1-a)^{n_{\max}-n(k-1)}. \tag{10}$$

where $0.5<a<1$ is a parameter and $n(k)$ is the number of digits equal to 1 in the binary representation of the index k. The scaling exponents $h(q)$ and $\tau(q)$ can be calculated analytically in this model, and they have the closed form

$$h(q) = \frac{1}{q} - \frac{\ln[a^q+(1-a)^q]}{q\ln 2}, \qquad \tau(q) = -\frac{\ln[a^q+(1-a)^q]}{q\ln 2}. \tag{11}$$

To illustrate the efficiency of the WT-MFDFA method, we present the comparison of the multifractal quantities h and τ for $a=3/4$ between the values for the theoretical values and the numerical results obtained through the WT-MFDFA analysis. The results for this case are displayed in Fig. 4, whereas Table 3 contains the theoretical values ($h_T(q)$) and the numerical results obtained through the wavelet approach ($h_W(q)$). Notice that the numerical values have a small downward shift. Adding the vertical offset $\Delta = h_T(1)-h_W(1)$ to $h_W(q)$, we can notice that the theoretical and numerical values are very close.

In a similar way as in our previous work[13], and since the main sequence matrix $\mathbf{Q}_N$ is based on the evolution of rule 90, we analyze with the WT-MFDFA method the sum of ones in the sequences of the rows of this matrix, using the db-4 wavelet function belonging to the Daubechies orthogonal family [22]. We select this wavelet function because of its desirable properties, such as orthogonality, approximation quality, and numerical stability;[22] in addition, the algorithm with the Daubechies family wavelet functions is memory efficient and is reversible, whereas other wavelet bases have a slightly higher computational overhead and are conceptually more complex.

The results for the row sum of the encryption matrix $\mathbf{Q}_N$ are illustrated in Fig. 5. We consider $N=2^{12}-1=4095$ data points of the time series, and the fact that the generalized Hurst exponent is not a constant horizontal line is indicative of a multifractal behavior in this time series, see Fig. 5 (b). Since the scaling exponent τ is not of a single slope, Fig. 5 (c), it can be considered as another clear feature of multifractality. The strength of the multifractility is roughly measured with the width $\Delta\alpha=\alpha_{\max}-\alpha_{\min}$ of the "parabolic" singularity spectrum $f(\alpha)$ on the α axis, see Fig. 5 (d). For this matrix, the width $\Delta\alpha_{\mathbf{Q}_{4095}}=1.0160-0.0080=1.0080$, and the "most" frequent singularity occurs at $\alpha_{\mathrm{mf}_{\mathbf{Q}_{4095}}}=0.5540$.

On the other hand, the multifractal results for the decryption matrices, $\mathbf{T}_N$ and $\mathbf{R}_N$, are displayed in Fig. 6. We notice that both time series have a smaller $\Delta\alpha$ that the previous one. However, both of them present a similar multifractal behavior. For instance, the width $\Delta\alpha_{\mathbf{R}_{4095}}=0.9740-0.2180=0.7560$ and $\Delta\alpha_{\mathbf{T}_{4095}}=0.9600-0.2180=0.7420$ do not present a big difference. In fact, the "most" frequent singularity occurs at the same alpha value $\alpha_{\mathrm{mf}_{\mathrm{R}_{4095}}}=\alpha_{\mathrm{mf}_{\mathrm{T}_{4095}}}=0.4280$. These results were expected since these decryption matrices depend on the matrix $\mathbf{Q}_N$.

In order to assess the impact of finite signal lengths on the multifractal quantities, we apply the WT-MFDFA technique to the time series obtained from the encryption matrices involved in the ESCA system for different lengths: $N=2^n-1$, $n=9,10,11,12,13$. Table 3 summarizes the results obtained, where we notice that the results of matrix $\mathbf{Q}_N$ are more stable than the results obtained from the decryption matrices, $\mathbf{T}_N$ and $\mathbf{R}_N$. In fact, the results obtained for $\mathbf{Q}_N$ are in very good agreement with the results obtained in a previous work,[13] where the WT-MFDFA method was applied to different CA rules, including the CA rule 90.

It is worth pointing out that we studied the intrinsic multifractal properties of the main sequence matrices of an encryption system having in mind their possible usage in cryptanalysis. In Ref. [23] the authors have considered the generalized Hurst exponent $h(q)$ as a representative multifractal parameter. In that paper, they analyzed a chaotic carrier with an embedded signal and found that this quantifier helped to detect the presence of a message, meaning that it can be used as an efficient measure of encryption schemes. But, the

analysis is performed on encrypted signals and not directly to the encryption elements of the encryption system as we do here. A similar approach has been considered in another work, where we hope to establish a relationship between an encrypted signal and multifractal quantities.

4 Conclusions

We have used the wavelet-based variant of the multifactal detrended fluctuation analysis to reveal the multifractal features of some matrices that carry out the main functions in an encryption system. To accomplish this goal, we discussed some multifractal quantities such as the generalized Hurst exponent $h(q)$, the singularity spectrum $f(\alpha)$, and the scaling exponent $\tau(q)$ of these matrices. In general, the multifractal quantities provide useful statistical information and characterization of the matrices used in some classes of encryption systems.

Acknowledgments

C.V.O. and M.T.R.T. are doctoral fellows of CONACyT (Mexico) in the Graduate Program on "Ciencias Aplicadas" at IICO-UASLP.

References

[1] J.W. Kantelhardt, *Encyclopedia of Complexity and Systems Science* (Springer, Berlin, 2009).

[2] E.A.F. Ihlen, *Behavior Research Methods* (2013).

[3] J.F. Muzy, E.Bacry, and A. Arneodo, *Phys. Rev. E* **47**, 875 (1993).

[4] S. Mallat, W.L. Hwang, IEEE Trans. Inform. Theory **38**, (2) 617-643 (1992).

[5] J.F. Muzy, E.Bacry, and A. Arneodo, *Phys. Rev. Lett.* **67**, 3515 (1991).

[6] E.Bacry, J.F. Muzy, and A. Arneodo, *J. Stat. Phys.* **70**, 635 (1993).

[7] J.F. Muzy, E.Bacry, and A. Arneodo, *Int. J. of Bifurcation and Chaos* **4**, 245 (1994).

[8] A. Arneodo, E.Bacry, and J.F. Muzy, *Physica A* **213**, 232 (1995).

[9] C.-K. Peng, S.V. Buldyrev, S. Havlin, M. Simons, H.E. Stanley, and A.L. Goldberger, *Phys. Rev. E* **49**, 1685 (1994).

[10] J.W. Kantelhardt, S.A. Zschinegner, E. Koscielny-Bunde, S. Havlin, A. Bunde, and H.E. Stanley, *Physica A* **316**, 87 (2002).

[11] P. Oswiecimka, J.Kwapien, and S. Drozdz, *Phys. Rev. E* **74**, 016103 (2006).

[12] P. Manimaran, P.K. Panigrahi, J.C. Parikh, *Phys. Rev. E* **72**, 046120 (2005).

[13] J. S. Murguía, J. E. Perez-Terrazas, and H. C. Rosu, *Europhysics Letters* **87**, 28003 (2009).

[14] J.S. Murguía, H.C. Rosu, *Physica A* **391**, 3638 (2012).

[15] J. S. Murguía, M. Mejía Carlos, H. C. Rosu, and G. Flores-Eraña, *Int. J. Mod. Phys. C* **21**, 741 (2010).

[16] J. S. Murguía, G. Flores-Eraña, M. Mejía Carlos and H. C. Rosu, *Int. J. Mod. Phys. C* **23**, 1250078 (2012).

[17] J. Urías, E. Ugalde and G. Salazar, *Chaos* **8**, 819 (1998).

[18] J. Urías, G. Salazar, and E. Ugalde, *Chaos* **8**, 814 (1998).

[19] T.C. Halsey, M.H. Jensen, L.P. Kadanoff, I. Procaccia, B.I. Shraiman, *Phys. Rev. A* **33**, 1141 (1986).

[20] J.S. Murguía, J. Urías, *Chaos* **11**, 858 (2001).

[21] J. Feder, Appendix B in *Fractals* (Plenum Press, New York) 1998.

[22] S. Mallat, *A Wavelet Tour of Signal Processing*, (Academic Press, 2nd. Ed., 1999).

[23] L. Zunino, M. C. Soriano, A. Figliola, D. G. Pérez, M. Garavaglia, C. R. Mirasso, and O. A. Rosso, *Optics Communications* **282**, 4587 (2009).

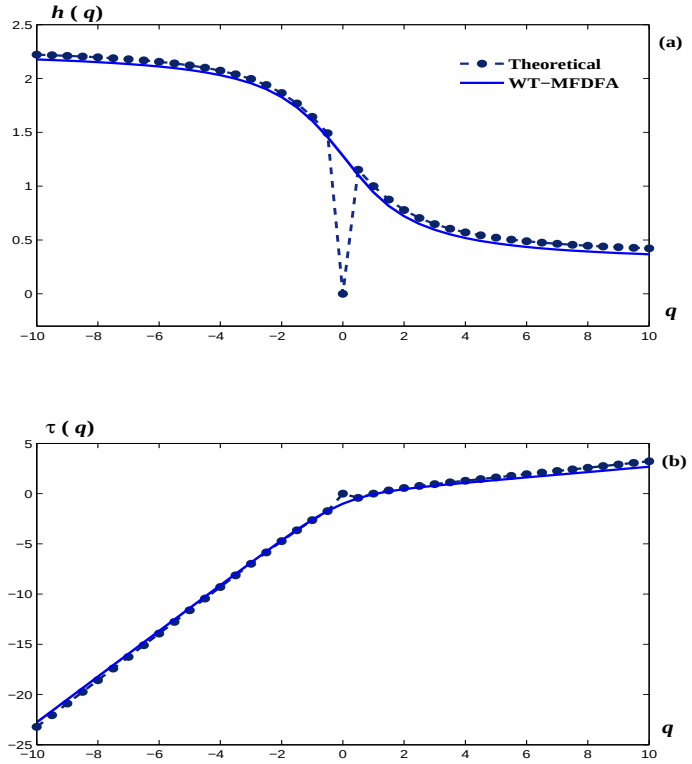

Fig. 4: (a) The generalized Hurst exponent $h(q)$, and (b) the scaling exponent $\tau(q)$ for the binomial multifractal model with $a = 3/4$. The theoretical values of $h(q)$ and $\tau(q)$ with the WT-MFDFA calculations are shown for comparison.

The values obtained for the multifractal the generalized Hurst exponent h for the binomial multifractal model with $a = 3/4$, which were computed analytically and with the wavelet approach.

q	$h_T(q)$	$h_W(q)$	$h_W(q) + \Delta$
-10	1.9000	1.8550	1.9000
-9	1.8889	1.8443	1.8893
-8	1.8750	1.8310	1.8760
-7	1.8572	1.8139	1.8589
-6	1.8337	1.7913	1.8363
-5	1.8012	1.7602	1.8052
-4	1.7544	1.7156	1.7606
-3	1.6842	1.6487	1.6936
-2	1.5760	1.5450	1.5900
-1	1.4150	1.3878	1.4328
0	0.0000	1.1779	1.2229
1	1.0000	0.9577	1.0026
2	0.8390	0.7899	0.8349
3	0.7309	0.6829	0.7279
4	0.6606	0.6138	0.6588
5	0.6139	0.5669	0.6119
6	0.5814	0.5339	0.5789
7	0.5578	0.5099	0.5549
8	0.5400	0.4917	0.5367
9	0.5261	0.4776	0.5225
10	0.5150	0.4662	0.5112

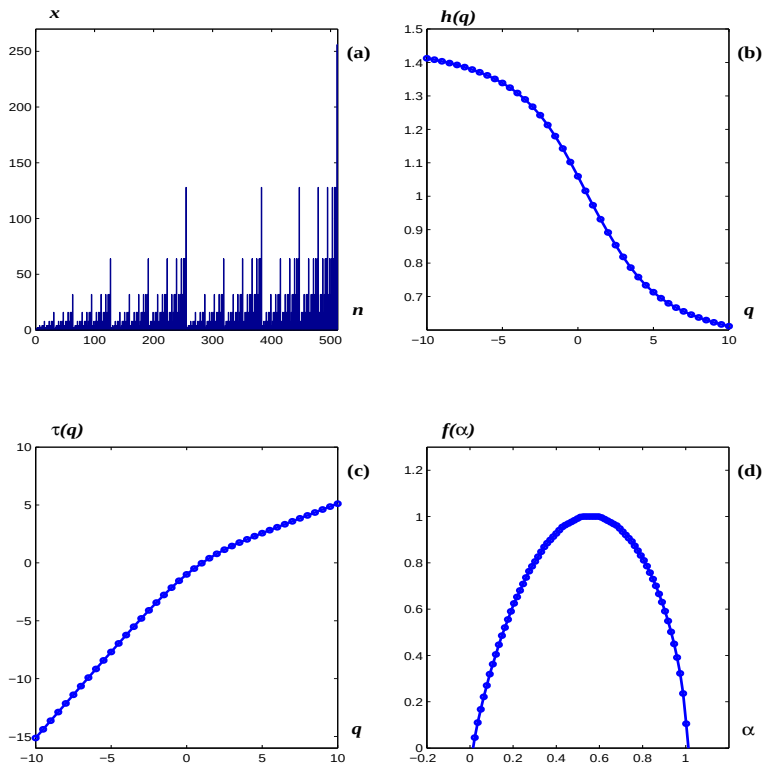

Fig. 5: (a) Time series of the row signal of Q_{4095}. Only the first 2^9 points are shown of the whole set of $(2^{12}-1)$ data points. (b)The generalized Hurst exponent $h(q)$, (c) the τ exponent, where $\tau(q) = qh(q) - 1$, and (d) the singularity spectrum $f(\alpha) = q\frac{d\tau(q)}{dq} - \tau(q)$.

The values of the width $\Delta\alpha = [\alpha_{\min}, \alpha_{\max}]$ and the most "frequent" singularity, $\alpha_{\rm mf}$, for different dimensions of the three matrices $\mathbf{Q}_N$, $\mathbf{R}_N$ and $\mathbf{T}_N$ obtained by means of the WT-MFDFA method.

Matrix		n = 9	10	11	12	13
$\mathbf{Q}_N$	$\alpha_{\min}$	0.1200	0.0500	0.0220	0.0080	0.0080
	$\alpha_{\max}$	1.1000	1.0580	1.0300	1.0160	1.0160
	$\Delta\alpha$	0.9800	1.0080	1.0080	1.0080	1.0080
	$\alpha_{\rm mf}$	0.6520	0.5960	0.5820	0.5540	0.5540
$\mathbf{R}_N$	$\alpha_{\min}$	0.0360	0.1060	0.1620	0.2180	0.2460
	$\alpha_{\max}$	0.8060	0.8760	0.9320	0.9740	0.9880
	$\Delta\alpha$	0.7700	0.7700	0.7700	0.7560	0.7420
	$\alpha_{\rm mf}$	0.2880	0.3440	0.4000	0.4280	0.4560
$\mathbf{T}_N$	$\alpha_{\min}$	0.0220	0.1060	0.1620	0.2180	0.2460
	$\alpha_{\max}$	0.8060	0.8760	0.9320	0.9600	0.9880
	$\Delta\alpha$	0.7840	0.7700	0.7840	0.7420	0.7420
	$\alpha_{\rm mf}$	0.3020	0.3440	0.4000	0.4280	0.4560

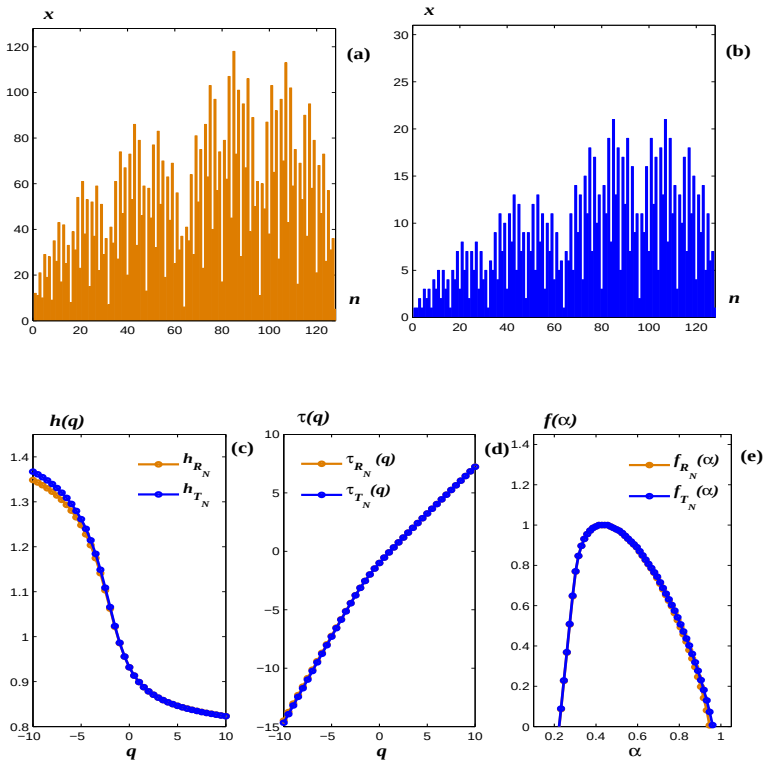

Fig. 6: Time series of the row signal of the matrices (a) R_{4095}, and (b) T_{4095}. Only the first 2^8 points are shown of the whole set of $(2^{12}-1)$ data points. (c)The generalized Hurst exponent $h(q)$ for the row signals R_{4095}, and T_{4095}, (d) the τ exponent for each signal, and (e) the corresponding singularity spectrum $f(\alpha)$.