TWO-DIMENSIONAL DFA SCALING ANALYSIS APPLIED TO ENCRYPTED IMAGES

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

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

Int. J. Mod. Phys. C 26(8), 1550093 (2015)

Abstract

The technique of detrended fluctuation analysis (DFA) has been widely used to unveil scaling properties of many different signals. In this paper, we determine scaling properties in the encrypted images by means of a two-dimensional DFA approach. To carry out the image encryption, we use an enhanced cryptosystem based on a rule-90 cellular automaton and we compare the results obtained with its unmodified version and the encryption system AES. The numerical results show that the encrypted images present a persistent behavior which is close to that of the $1/f$-noise. These results point to the possibility that the DFA scaling exponent can be used to measure the quality of the encrypted image content.

DOI: 10.1142/S012918311550093X
Keywords: Encryption system; two-dimensional DFA; scaling laws.
PACS numbers: 05.40.-a, 05.45.Df, 05.45.Tp

1 Introduction

At the present time, there are a great number of different methods to analyze or detect singular or fractal behavior that may be embedded in different kind of information.[1, 2] To list a few of them, we count with the wavelet transform and its versions,[3, 4, 5] the detrended fluctuation analysis (DFA),[6] the multifractal detrended fluctuation analysis (MF-DFA) and its different modifications,[1, 7, 8] or combination of the discrete wavelet transform with the DFA.[9] With the aim to extract meaningful features from high-dimensional signals, such as images, some of the previous methods have been applied. For instance, the roughness features present in the texture of images are an important characteristic that was analyzed by DFA scaling techniques.[10] In particular, the DFA technique allows to extract the Hurst indices of the one-dimensional sequences at different orientations in the plane of the image and based on their values the average scaling exponent can be estimated. However, this is just a multiple form of the one-dimensional DFA method. In 2006, Gu and Zhou,[11] generalized the DFA and MF-DFA methods to higher dimensions, in particular to the two-dimensional case for distinguishing fractal and multifractal properties of synthetic surfaces. There is no doubt that these methods to detect long-range correlation and multifractal properties are very useful tools in the field of image analysis, since they have been applied to investigate characteristics in some lymphoma images,[12] to extract texture features,[13] to identify singular regions of crop leaf affected by diseases,[14] and so on. It is worth to note that the performance of the methods based on fractal or multifractal techniques are superior to other methods, due to the isotropic characteristics that present a huge amount of natural and synthetic images.

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

On the other hand, the digital image encryption is an important issue since there are many applications that require to protect different kind of information such as medical imaging systems, military image communications, surveillance, among others.[15] Despite that there are numerous image encryption methods, it is crucial if we may be able to determine some kind of quality of the encrypted image content. In this sense, we consider to apply to encrypted images an algorithm based on the two-dimensional DFA, since after encryption, the image pixels tend to have isotropic characteristics or a "random" behavior. In fact, Ref. [16] considered the generalized Hurst exponent as an efficient measure of encryption schemes, and the authors were able to detect the presence of a message in a chaotic carrier with an embedded signal. In addition, to achieve multimedia security some authors strongly suggest to use the selective encryption, see for example References [17]-[18]. Here, following ideas expressed in Ref. [17], but employing different tools, we find out that the encryption of four bitplanes is sufficient for providing high confidentiality.

The paper is organized as follows. Section 2 is devoted to a concise presentation of the enhanced encryption system based on a matrix approach that we introduced in previous works. In Section 3, the procedure of the two-dimensional detrended fluctuation analysis is presented, whereas Section 4 contains the results obtained by applying the two-dimensional DFA technique to the encrypted images. In addition, we analyze images when only a partial encryption is considered. Finally, the conclusions are drawn in Section 5.

2 Encryption System Model

We consider a cryptosystem that comprises the sets M, C and X of binary words of length N, i.e., Z_2^N, where $Z_2 = \{0, 1\}$, and two indexed families of permutations, $\Psi = \{\psi_{\mathbf{x}} : \mathbf{x} \in X\}$ and $\Phi = \{\phi_{\mathbf{x}} : \mathbf{x} \in X\}$. The words in M and C are called the plain-texts and cipher-texts, respectively, whereas the words in the set of indices X are the encyphering keys. In addition, the functions $\psi_{\mathbf{x}} : M \to C$, and $\phi_{\mathbf{x}} : C \to M$, are called the encryption and decryption functions, respectively. Basically, the cryptosystem transforms a plain-text sequence $\mathbf{m}$ to a cipher-text sequence $\mathbf{c}$, i.e., for every $\mathbf{x} \in X$ one has $\mathbf{c} = \psi_{\mathbf{x}}(\mathbf{m})$, whereas to disclose from the sequence of cipher-blocks, one uses the decryption functions $\phi_{\mathbf{x}}$, i.e., $\mathbf{m} = \phi_{\mathbf{x}}(\psi_{\mathbf{x}}(m))$. Since the complete encryption scheme is private, the encryption and decryption processes use the same enciphering key $\mathbf{x}$. Such a cryptosystem is based on the encryption scheme used in Ref. [19] where the synchronization phenomenon of cellular automata (CA), which evolves according to the local rule 90, has been applied to devise the two families of permutations and the asymptotically perfect pseudo-random number generator. The phenomenon of synchronization in the case of coupled pairs of CA is described in detail in Ref. [20], where it was found that a pair of coupled CA can synchronize if every pair of consecutive coordinates is separated by a block of $(2^n - 1)$ uncoupled sites, where n is a positive integer greater than 1. This encryption system based on the synchronization phenomenon of CA is called the ESCA system.

In our previous work,[21] we achieved a simple and flexible implementation by employing a matrix approach to implement almost all the components of the ESCA system. Moreover, in Ref. [22] the latter approach has been modified with the aim of making more flexible its matrix implementation and to improve its security.

For the convenience of the reader we recall some relevant material from Ref. [22], thus making our exposition self-contained.

In order to have an unintelligible form of the plain-text $\mathbf{m} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots\}$, where each plain-text block $\mathbf{m}_k$ has N bits, we apply the following operation

$$\begin{pmatrix} \hat{\mathbf{m}}_k \\ \mathbf{y}_{k+1} \end{pmatrix} = \mathbf{U} \begin{pmatrix} \mathbf{m}_k \\ \mathbf{y}_k \end{pmatrix} \bmod 2, \quad \text{with } \mathbf{U} = \left(\begin{array}{c} \mathbf{J}_N \\ \hline \mathbf{J}_N \\ \mathbf{b} \end{array}\right), \text{ and } k = 1, 2, \ldots, \tag{1}$$

where $\mathbf{J}_N$ represents an $N \times (2N + 1)$ matrix that is initially generated from two vectors of $(2N + 1)$ elements, $\mathbf{f} = [f_1, 0, \ldots, f_{N+2}, \ldots, 0]$ and $\mathbf{g} = [0, g_2, 0, \ldots, g_{N+1}, 0, g_{N+3}, \ldots, 0]$, where the components $f_1,\ f_{N+2},\ g_2,\ g_{N+1}$ and g_{N+3} have a value of 1. These vectors comprise the two first rows of the matrix $\mathbf{J}_N$, and the other $(N - 2)$ rows are generated by applying an addition modulo 2 operation of the two previous rows, with fixed boundary conditions of zero to the left-hand side followed by the elements of the previous row shifted to the right by one position. The row vector $\mathbf{b}$ has $(2N + 1)$ elements with a value of 1 in its first entry and 0 otherwise, i. e., $\mathbf{b} = [1,\ 0,\ \ldots, 0]$. In essence, to compute the sequence $\hat{\mathbf{m}}_\mathbf{1}$ of N bits we require the product of the square matrix $\mathbf{U}$ with a column vector that concatenates the plain-text sequence $\mathbf{m}_1 = \{m_1, m_2, m_3, \ldots, m_N\}$, and a random binary sequence $\mathbf{y}_1 = \{y_1, y_2, y_3, \ldots, y_{N+1}\}$, of $(N + 1)$ bits. Next, to compute $\hat{\mathbf{m}}_\mathbf{2}$ by means of (1), we require again two sequences, a plain-text sequence to be modified

$\mathbf{m}_2$, and a binary random sequence $\mathbf{y}_2$. At this time, the latter sequence comprises the $\hat{\mathbf{m}}_\mathbf{1}$ sequence, which becomes the initial bits of the new $\mathbf{y}_2$, and the first bit of the previous $\mathbf{y}_1$, which becomes the last bit of this sequence. For the following sequences, the same procedure is iterated repeatedly. Note that the top matrix $\mathbf{J}_N$ makes inexplicit the plain-text, whereas the low matrix $[\mathbf{J}_N; \mathbf{b}]$ helps to compute a new binary pseudo random sequence $\mathbf{y}_k$, for $k \geq 2$.

Now, in order to continue with the encryption process, we need two matrices, $\hat{\mathbf{P}}_N$ and $\hat{\mathbf{Q}}_N$, such that

$$\mathbf{c}_k = \Psi_\mathbf{x}(\hat{\mathbf{m}}_k) = \left[\left(\hat{\mathbf{P}} \times \mathbf{x}\right) + \left(\hat{\mathbf{Q}} \times \hat{\mathbf{m}}_k\right)\right] \bmod 2, \quad k \geq 1, \tag{2}$$

where the vectors $\mathbf{c}_k$ and $\hat{\mathbf{m}}_k$ have dimensions $L \times 1$, with $L = 2^l$, for $l = 1,\ 2, \ldots$, and $\mathbf{x}$ has dimensions $N \times 1$, with $N = 2^n - 1$, for $n = 1,\ 2, \ldots$, such that $n > l$. $\hat{\mathbf{P}}$ is an upper triangular matrix with dimensions $L \times N$, and it is initially generated from the vector $\mathbf{p} = [p_1, p_2, \ldots, p_N]$. This vector constitutes the first row, and the components with position index $j = (2^n + 1) - 2^{i+1}$, for $i = 0, 1, 2, \ldots, (n-1)$, have a value of 1, and 0 otherwise. The $(L-1)$ 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, $\hat{\mathbf{Q}}$ is a lower triangular matrix of order L, that can be generated initially from the vector $\boldsymbol{a} = [a_1, 0, \ldots, 0]$, where the component a_1 has a value of 1. The latter vector constitutes the first row of the matrix $\hat{\mathbf{Q}}$, and the $(L-1)$ 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. Since the decryption process is similar to the encryption procedure, the reader is referred to Ref. [22] for more details.

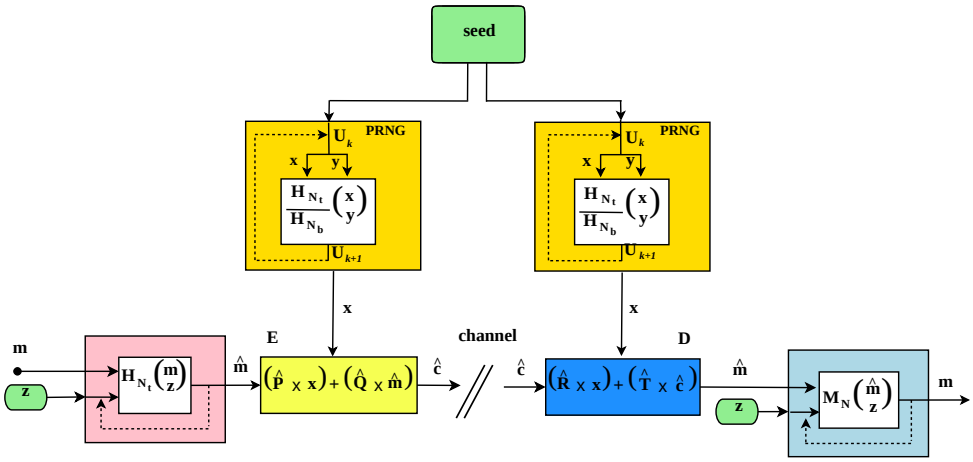

Fig. 1: The encryption model considered in this work with its main components: the indexed families of permutations, Ψ and Φ, and the pseudorandom generator of keys.

To carry out the encryption process, at first we load a plain-image $\mathbf{I}$ of size $U \times V$ having all of its pixels arranged into a vector by scanning the image $\mathbf{I}$ row by row. After that, each pixel value is converted to their corresponding 8-bit value, $[b_8 \ \cdots \ b_1]$, where b_1 is the least significant bit (LSB), whereas b_8 is the most significant bit (MSB).

3 Material and Methods

3.1 Material

A total of eighteen gray-level images were used in this study. Thirteen of them have dimensions of 512×512 pixels, and five have dimensions of 1024×1024 pixels. These images are shown in Figure 2 and have been chosen because they are widely used as standard test images in the field of image processing. This image database is freely available at http://sipi.usc.edu/database, except the final two pictures. The first of the latter pair, a picture of the Mars Yardangs region picture, can be downloaded from https://solarsystem.nasa.gov, while the last one is a fractional Brownian surface with Hurst exponent $H = 0.5$, which was generated by the MATLAB software FRACLAB 2.1 developed by INRIA.

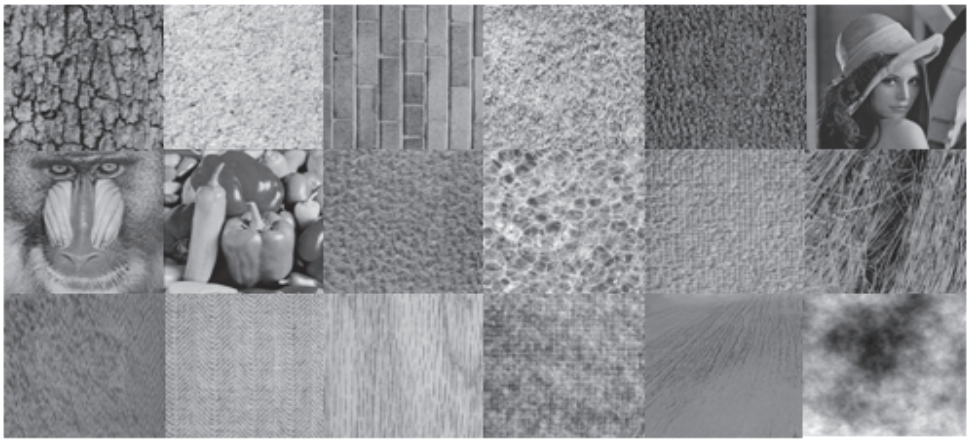

Fig. 2: The image dataset considered in this work.

3.2 Two-dimensional detrending fluctuation analysis

In general, an image $\mathbf{I}$ of size $U \times V$ will be considered as a surface and denoted by a matrix $X(i, j)$, where the number of rows and columns is represented by $i = 1, 2, \ldots, U$ and $j = 1, 2, \ldots, V$, respectively. In order to separate the trend from fluctuations in the images, we follow the two-dimensional DFA algorithm proposed by Gu and Zhou,[11] which consists of the following steps.

1. Divide the surface $X(i, j)$ into $U_s \times V_s$ disjoint square windows of the same size $s \times s$, where $U_s = \lfloor U/s \rfloor$ and $V_s = \lfloor V/s \rfloor$. Each window can be denoted by $X_{u,v}$ such that $X_{u,v}(i, j) = X(i + l_1, j + l_2)$ for $1 \leq i, j \leq s$, where $l_1 = (u - 1)s$ and $l_2 = (v - 1)s$.

2. Compute the cumulative sum for each window $X_{u,v}$, positioned by u and v, as

$$P_{u,v}(i, j) = \sum_{k_1=1}^{i} \sum_{k_2=1}^{j} (X_{u,v}(k_1, k_2) - \langle X_{u,v}(k_1, k_2) \rangle), \tag{3}$$

   where $\langle X_{u,v}(k_1, k_2) \rangle$ is the average of the sub-image $X_{u,v}$, for $1 \leq i, j \leq s$.

3. Determine the trend of the obtained sub-image by fitting the set of data to the plane $\tilde{P}_{u,v}(i, j) = ai + bj + c$, where a, b, and c are parameters which are estimated using the least square method. Subsequently, one calculates the local variances associated to each sub-image $X_{u,v}$ as

$$F^2(u, v, s) = \frac{1}{s^2} \sum_{i=1}^{s} \sum_{i=1}^{s} [P_{u,v}(i, j) - \tilde{P}_{u,v}(i, j)]^2. \tag{4}$$

4. Next, averaging over all sub-images the overall detrended fluctuation is obtained as

$$F_2(s) = \left(\frac{1}{U_s V_s} \sum_{u=1}^{U_s} \sum_{v=1}^{V_s} F^2(u, v, s) \right)^{1/2}. \tag{5}$$

This procedure is repeated for a broad range of segment lengths s, considering the range $6 \leq s \leq \min(U, V)/4$. In order to assess a fractal scaling property of the pixelated surface, the fluctuation function $F_2(s)$ should display a power law scaling

$$F_2(s) \sim s^{\alpha}, \tag{6}$$

where α is called the scaling fluctuation exponent. This scaling exponent can be found as the slope of a double logarithmic plot of F_2 as a function of s, and it is a measure of the degree of correlation among the pixels of the surface. In the one-dimensional case we have the following relationships: (a) If $\alpha = 0.5$

there is no correlation and the pixels are uncorrelated (white noise process). (b) For $0 < \alpha < 0.5$, the pixels present an anticorrelated behavior, which means that a large value is more likely to be followed by a small value, and vice versa; in this case the signal is said to be anti-persistent. (c) If $0.5 < \alpha < 1$, the correlation of the pixels is persistent, where large values of the data are more probably to appear after large values, or vice versa, small values are more probable after small values. (d) The values $\alpha = 1$ and $\alpha = 1.5$ correspond to $1/f$-noise and Brownian motion, respectively. Furthermore, this scaling exponent can be considered as a generalization of the Hurst exponent H satisfying $0 < H < 1$ as follows. For stationary signals, α is identical to the Hurst exponent H, whereas for non-stationary time signals $\alpha = H + 1$.[7, 23, 24, 25] On the other hand, in Ref. [26] is pointed out that the relationship between the Hurst exponent H and α for the two-dimensional case is as follows: (a) If the two-dimensional signal is stationary α is identical to the Hurst exponent H, whereas if it is non-stationary $\alpha = H + 2$.

4 Results and Discussion

In this Section, we present the results obtained using the two-dimensional DFA analysis described in the previous subsection. In the analysis, all of the eighteen standard gray-level images of different shapes and three different encryption procedures were considered. The encryption schemes are the ESCA system,[21] the improved form of the ESCA encryption system described in Section 2, and the Advanced Encryption Standard (AES) in CBC mode,[15] which here we call as ESCAv1, ESCAv2, and AES, respectively. The results of the performance of the two-dimensional DFA for the gray-scale mandrill plain-image and its encrypted versions are shown in Fig. 3. It is observed that the fluctuation function $F_2(s)$ presents a similar value and behavior for the three encryption procedures altogether. The fluctuation scaling exponents α for the image datasets considered in this paper are given in Table 1. Since the majority of the α exponents of the encrypted versions are close to unity, we can infer that in general the encrypted images present a persistent behavior which is close to the $1/f$-noise. As the fractal dimension is considered as an objective metric to measure the quality of the encrypted image content,[15] it is possible to consider the latter result as an alternative objective metric.

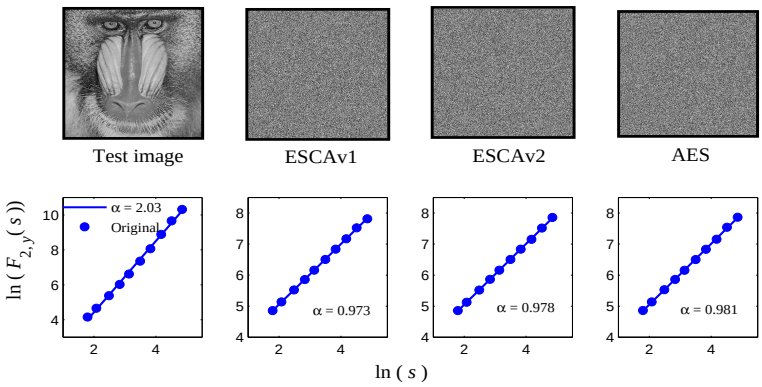

Fig. 3: In the top row, there are the test images and the different encrypted versions, whereas in the bottom row there are their respective scaling-fluctuation exponents provided by the fluctuation function F_2.

In addition, following the ideas of Ref. [17] to delve into the sensitivity to the encrypted pixels, we carry out a partial encryption of the images by encrypting four bits for each pixel, and apply the two-dimensional DFA to the resultant encrypted image. We took the four most significant bits, and we shift one bit of the group of four bits until we get the four least significant bits. The results of this scaling method for the encrypted mandrill plain-images are presented in Figures 4-6, and the rest of the fluctuation scaling exponents α for the considered image datasets are given in Tables 2-4. For the encryption systems ESCAv1 and AES, the scaling exponents of the encrypted image are getting close to the values of the scaling exponents of the plain-images as we get the four most significant bits, whereas for the encryption system ESCAv2 the scaling exponents are remain without a significant change. In fact, some information is visible when we encrypt the last three blocks of the least significant bits, that is, from the block of four bits $b_6, \ldots, b_3$ to the block $b_4, \ldots, b_1$. These results illustrate that the encryption system ESCAv2 can provide high confidentiality in

the case of partial encryption. In addition, since we just have a half-encryption of the data, we also improve the execution time.

Table 1: The values of the α scaling exponents obtained from applying the 2D DFA algorithm to the 18 test images and their encrypted versions.

Test	α exponents			
image	**Original**	**ESCAv1**	**ESCAv2**	**AES**
Bark	1.8173	0.9629	0.9721	0.9745
Beach sand	1.6555	0.9946	0.9759	0.9751
Brick	1.8347	0.9954	0.9742	0.9871
Grass	1.6243	0.9894	0.9810	0.9834
Leather	1.3778	0.9623	0.9918	0.9745
Lena	2.2544	0.9826	0.9806	0.9857
Mandrill	2.0335	0.9734	0.9783	0.9808
Peppers	2.2876	0.9770	0.9633	0.9782
Pigskin	1.5552	0.9701	0.9768	0.9610
Plastic bubbles	1.9467	1.0000	0.9858	0.9884
Raffia	1.4798	0.9841	0.9486	0.9798
Straw	1.7166	0.9555	0.9713	0.9870
Water	1.5591	0.9772	0.9795	0.9918
Weave	1.3403	1.0005	0.9588	0.9723
Wood	1.6261	0.9982	0.9788	0.9804
Wool	1.8473	0.9953	0.9760	0.9714
Yardangs	1.6223	0.9583	0.9930	0.9810
fBmS	2.5114	0.9884	0.9812	0.9900

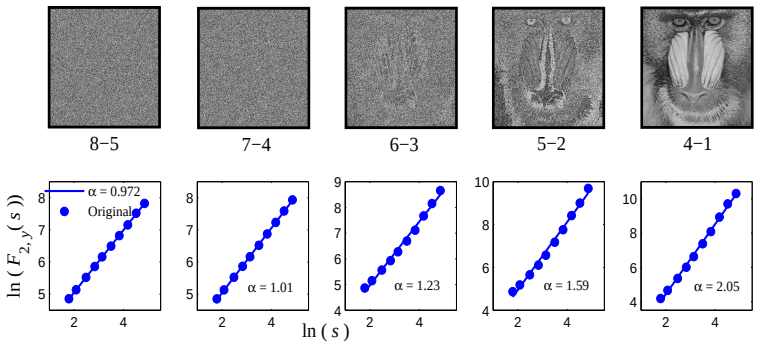

Fig. 4: In the top row, there are the encrypted images of the mandrill image performed with the ESCAv1 system, where only the indicated bits are encrypted and the other part is not changed. In the bottom row, there are their respective scaling-fluctuation exponents provided by the fluctuation function F_2.

5 Conclusions

In this work, we have used a two-dimensional DFA algorithm to determine the singular behavior of encrypted gray-level images. Although many methods for high-dimensional signals have been proposed, our results show that the two-dimensional DFA method seems to be a natural and efficient tool for describing this kind of images by means of scaling exponents. In addition, it is suggested that the fluctuation scaling exponent can be used as an appropriate and objective measure of the quality of encryption schemes. In our opinion, a good image encryption algorithm, such as the ESCAv2, should maintain the "same" scaling exponent despite a partial encryption is carried out.

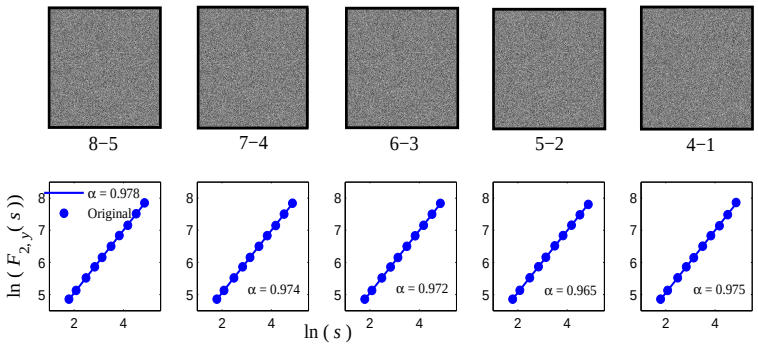

Fig. 5: Same caption comments as in the previous figure, but the encryption procedure is carried out by the ESCAv2 system.

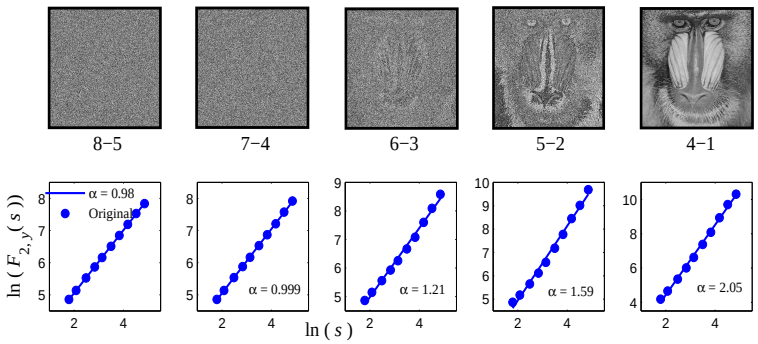

Fig. 6: Same caption comments as in the previous figure, but the encryption procedure is carried out by the AES system.

Table 2: The values of the α scaling exponents obtained after applying the 2D DFA algorithm to the 18 encrypted images by means of the ESCAv1 encryption system.

Test Image	α exponents				
	$b_8 \cdots b_5$	$b_7 \cdots b_4$	$b_6 \cdots b_3$	$b_5 \cdots b_2$	$b_4 \cdots b_1$
Bark	0.9622	0.9672	1.0337	1.3347	1.8150
Beach sand	0.9973	1.0023	1.1066	1.3791	1.6508
Brick	1.0001	1.0234	1.2576	1.6142	1.8288
Grass	0.9906	0.9952	1.0169	1.2062	1.6228
Leather	0.9646	0.9674	0.9937	1.1585	1.3769
Lena	0.9867	1.1250	1.3978	1.7999	2.2334
Mandrill	0.9718	1.0076	1.2347	1.5863	2.0460
Peppers	0.9702	1.1354	1.3487	1.7782	2.2537
Pigskin	0.9700	0.9692	1.0134	1.3231	1.5495
Plastic bubbles	0.9999	1.0033	1.1693	1.5566	1.9423
Raffia	0.9842	0.9872	1.0497	1.2177	1.4755
Straw	0.9543	0.9609	1.0253	1.3036	1.7143
Water	0.9745	0.9754	1.0885	1.3379	1.5496
Weave	1.0010	0.9992	1.0127	1.0634	1.3365
Wood	0.9976	1.0514	1.2495	1.2938	1.6204
Wool	0.9958	1.0000	1.0636	1.4865	1.8386
Yardangs	0.9599	1.0680	1.2584	1.4779	1.6275
fBmS	0.9973	1.1301	1.5487	1.8704	2.4288
mean	0.9821	1.0205	1.1594	1.4327	1.7728

Table 3: The values of the α scaling exponents obtained by applying the 2D DFA algorithm to the 18 encrypted images by means of the ESCAv2 encryption system.

Test image	α exponents				
	$b_8 \cdots b_5$	$b_7 \cdots b_4$	$b_6 \cdots b_3$	$b_5 \cdots b_2$	$b_4 \cdots b_1$
Bark	0.9700	0.9690	0.9734	0.9660	0.9825
Beach sand	0.9738	0.9711	0.9732	0.9800	0.9831
Brick	0.9748	0.9794	0.9824	0.9783	0.9721
Grass	0.9812	0.9823	0.9841	0.9939	0.9968
Leather	0.9936	0.9924	0.9789	0.9716	0.9458
Lena	0.9800	0.9742	0.9750	0.9769	0.9780
Mandrill	0.9779	0.9736	0.9724	0.9653	0.9745
Peppers	0.9630	0.9643	0.9611	0.9588	0.9773
Pigskin	0.9768	0.9758	0.9766	0.9750	0.9738
Plastic bubbles	0.9867	0.9878	0.9928	0.9908	0.9763
Raffia	0.9484	0.9510	0.9504	0.9727	0.9582
Straw	0.9722	0.9738	0.9744	0.9768	0.9606
Water	0.9796	0.9825	0.9869	0.9956	0.9881
Weave	0.9606	0.9636	0.9594	0.9711	0.9701
Wood	0.9781	0.9760	0.9751	0.9841	0.9777
Wool	0.9768	0.9760	0.9709	0.9610	0.9744
Yardangs	0.9926	0.9926	0.9943	0.9779	0.9983
fBmS	0.9828	0.9845	0.9843	0.9914	0.9834
mean	0.9761	0.9761	0.9759	0.9771	0.9762

Acknowledgments

C.V.O. and M.T.R.T. are doctoral fellows of CONACyT (México) in the Graduate Program "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] S. Mallat, W.L. Hwang, IEEE Trans. Inform. Theory **38**, 617 (1992).

Table 4: The values of the α scaling exponents obtained by applying the 2D DFA algorithm to the 17 encrypted images by means of the AES encryption system.

Test image	α exponents				
	$b_8 \cdots b_5$	$b_7 \cdots b_4$	$b_6 \cdots b_3$	$b_5 \cdots b_2$	$b_4 \cdots b_1$
Bark	0.9828	0.9775	1.0422	1.3340	1.8149
Beach sand	0.9851	1.0006	1.1011	1.3767	1.6509
Brick	0.9924	1.0339	1.2610	1.6134	1.8286
Grass	0.9962	0.9774	1.0186	1.2051	1.6228
Leather	0.9889	0.9932	1.0101	1.1601	1.3764
Lena	0.9783	1.1135	1.4007	1.8006	2.2331
Mandrill	0.9797	0.9992	1.2076	1.5908	2.0458
Peppers	0.9790	1.1253	1.3367	1.7752	2.2546
Pigskin	0.9849	1.0030	1.0315	1.3288	1.5499
Plastic bubbles	0.9693	0.9918	1.1504	1.5570	1.9425
Raffia	0.9570	0.9985	1.0683	1.2287	1.4751
Straw	0.9697	0.9754	1.0478	1.3058	1.7140
Water	0.9805	0.9858	1.0968	1.3365	1.5489
Weave	0.9747	0.9756	1.0000	1.0293	1.3357
Wood	0.9814	1.0517	1.2443	1.2779	1.6197
Wool	0.9753	0.9917	1.0615	1.4848	1.8389
Yardangs	1.0088	1.0814	1.2683	1.4786	1.6274
fBmS	0.9944	1.1268	1.5504	1.8701	2.5114
mean	0.9821	1.0224	1.1610	1.4308	1.7773

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

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

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

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

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

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

[10] J. Alvarez-Ramirez, E. Rodriguez, I. Cervantes and J.C. Echeverria, *Physica A* **361**, 677 (2006).

[11] G.-F. Gu and W.-X. Zhou, *Phys. Rev. E* **74**, 061104 (2006).

[12] R.-G. Yeh, C.-W. Lin, M. F. Abbod, and J.-S. Shieh, *Computational and Mathematical Methods in Medicine*, **2012**, 947191 (2012).

[13] F. Wang , Z.-S. Li , and G.-P. Liao, *Int. J. Pattern Recognit. Artif. Intell.* **28**, 1455005 (2014).

[14] F. Wang , J.-W. Li , W. Shi, and G.-P. Liao, *J. Appl. Phys.* **114**, 214905 (2013).

[15] S. Lian, J. Sun, D. Zhang, and Z. Wang, *Advances in Multimedia Information Processing-PCM 2004*, Springer Berlin Heidelberg, pp. 65-72, (2005).

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

[17] M. Podesser, H. P. Schmidt, and A. Uhl, *Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002)*, 2002.

[18] T. Lookabaugh and D. C. Sicker, *IEEE Commun. Mag.*, **42**, 124 (2004).

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

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

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

[22] M. T. Ramírez- Torres, J. S. Murguía, and M. Mejía Carlos, *Int. J. Mod. Phys. C* **25**, 1450054 (2014).

[23] J.S. Murguía, H.C. Rosu, A. Jimenez, B. Gutiérrez-Medina, and J.V. García-Meza, *Physica A* **417**, 176 (2015).

[24] D. Deligniéres, S. Ramdani, L. Lemoine, K. Torre, M. Fortes, and G. Ninot, *J. Math. Psychology* **50**, 525 (2006).

[25] A. Eke, P. Herman, J.B. Bassingthwaighte, G.M. Raymond, D.B. Percival, M. Cannon, I. Balla and C. Ikrényi, *Pflugers Archives* **439**, 403 (2000).

[26] Y. Zhou, Y. Leung, and Z.-G. Yu, *Phys. Rev. E* **87**, 012921 (2013).