Physica A 456, 22-30 (2016)

Perceptual security of encrypted images based on wavelet scaling analysis

C. Vargas-Olmos[a], J. S. Murguía[b], M. T. Ramírez[c], M. Mejía Carlos[a], H. C. Rosu[d], H. González-Aguilar[b]

[a]*Instituto de Investigación en Comunicación Óptica-Facultad de Ciencias, Universidad Autónoma de San Luis Potosí, Álvaro Obregón 64, 78000 San Luis Potosí, S.L.P., Mexico*

[b]*Facultad de Ciencias, Universidad Autónoma de San Luis Potosí, Álvaro Obregón 64, 78000 San Luis Potosí, S.L.P., Mexico*

[c]*Coordinación Académica Región Altiplano Oeste, Universidad Autónoma de San Luis Potosí, Álvaro Obregón 64, 78000 San Luis Potosí, S.L.P., Mexico*

[d]*Instituto Potosino de Investigacion Cientifica y Tecnologica, Camino a la presa San José 2055, Col. Lomas 4a Sección, 78216, San Luis Potosí, S.L.P., Mexico*

Abstract

The scaling behavior of the pixel fluctuations of encrypted images is evaluated by using the detrended fluctuation analysis based on wavelets, a modern technique that has been successfully used recently for a wide range of natural phenomena and technological processes. As encryption algorithms, we use the Advanced Encryption System (AES) in RBT mode and two versions of a cryptosystem based on cellular automata, with the encryption process applied both fully and partially by selecting different bitplanes. In all cases, the results show that the encrypted images in which none understandable information can be visually appreciated and whose pixels look totally random present a persistent scaling behavior with the scaling exponent α close to 0.5, implying no correlation between pixels when the DFA

*Corresponding author. Tel.: +52 4448262491
Email address: ondeleto@uaslp.mx (J. S. Murguía)

with wavelets is applied. This suggests that the scaling exponents of the encrypted images can be used as a perceptual security criterion in the sense that when their values are close to 0.5 (the white noise value) the encrypted images are more secure also from the perceptual point of view.

Keywords: Encryption system, Wavelet transform, Detrended fluctuation analysis, Scaling laws.

1. Introduction

Data multimedia has become in recent years an important part of our daily lives. Either personal information such as a mobile phone call, an online payment, an electronic transaction or classified information as military strategies, require transmission, reception or storage of secure and confidential information in a short time. It is for this reason that encryption techniques together with their respective evaluation criteria are relevant topics. In particular, due to the large number of images used in diversified applications, the image encryption methods, as well as their efficiency analysis and security evaluation, play a crucial role.

Security is the basic requirement of multimedia content encryption, but different from text/binary encryption requires both cryptographic security and perceptual security. The cryptographic security refers to the ability of the encryption schemes to resist cryptanalysis techniques such as differential analysis, related-key attack, and statistical attack, among others, whereas perceptual security refers to a high visual degradation of the multimedia content which makes it unintelligible to human perception [1].

In this context, this paper presents the scaling exponent α of the pixel fluctuation function as an objective metric with good potentiality for measuring the perceptual security of an encrypted image. This is important because usually a subjective metric is based on visual inspection which is carried out by persons that act as referees, but whose judgment depend on personal decisions such as emotional state or physical condition. On the other hand, the main features of an objective metric are consistency, efficiency, and robustness. Besides, it is mathematically defined and it can be used automatically, being generically less time consuming.

Since the encrypted images must be completely unintelligible, namely not exhibiting any feature of the images from which they are generated that might be understandable to the

viewer, the image pixels should be made as random as possible. This randomness of the encrypted image pixels can be quantified in terms of the fractal dimension of the encrypted image [1] but also by means of its scaling exponent. It is well established that the latter is close to that of the $1/f$ noise when a two-dimensional DFA approach is used [2].

Considering the above and bearing in mind that the partial image encryption through selective bitplane encryption has been recognized as a desirable option to reduce the computational demand and to protect the most important visual parts of an image [3], we have used previously two methods to obtain the scaling exponent of images that has been encrypted in complete or partial manners. One of these methods is based on the two-dimensional DFA algorithm [4] and the other is based on the DFA procedure using wavelets [5]. Of the two methods, the latter one will be applied here because it is a well-suited procedure to analyze the singular behavior that may be hidden in time series data with much less computational cost and better accuracy. In addition, with the aim of minimizing the processing time of the main tasks of an encryption system we carry out a selective image encryption by applying the encryption stages to some bitplanes only. Subsequently, we calculate the peak signal to noise ratio (PSNR) of the encrypted images, perform the analysis of our results and end up with some conclusions.

2. Database of encrypted images, scaling methods, and PSNR

2.1. Database of encrypted images

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. The same image database was used in Ref. [2] and is shown in Figure 1. These images have been chosen because they are widely used as standard test images in the field of image processing, and they can freely be downloaded at http://sipi.usc.edu/database, except the final two pictures, the one representing the Mars Yardangs region that can be downloaded from https://solarsystem.nasa.gov and the last one which represents a fractional Brownian surface with Hurst exponent $H = 0.5$ generated by the MATLAB software FRACLAB 2.1 developed by INRIA.

The simplest way to encrypt a two- or three-dimensional multimedia data is to consider it as a one-dimensional data stream and perform the encryption with any available cipher,

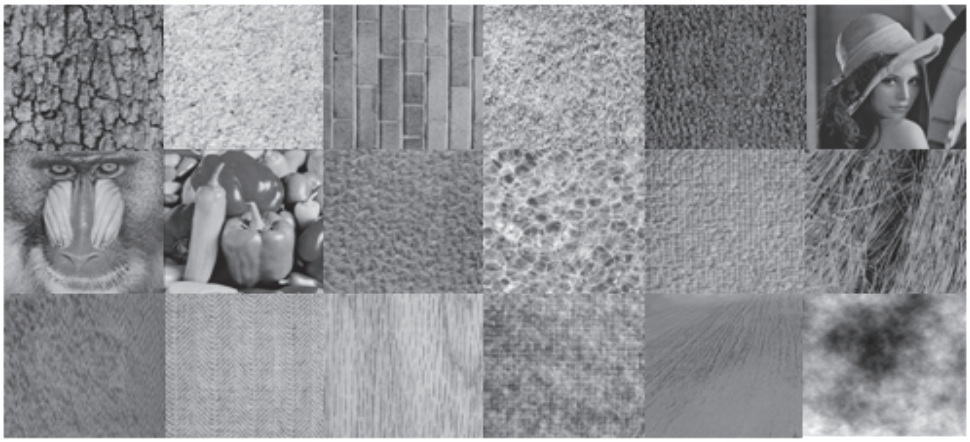

Figure 1: The image dataset considered in this work.

like Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), among others [6]. In this work, we encrypt all images using three encryption schemes that are known for their simplicity, flexibility, and security: the AES in RBT mode [7], the ESCA system, which is an encryption system based on the synchronization phenomenon of the cellular automata with rule 90 [8], and finally with an improved form of the ESCA encryption system described in Reference [9]. Moreover, a selective encryption of images has been also carried out by encrypting only certain parts of the data [3, 10] in order to reduce the time consuming cost.

2.2. Detrending fluctuation analysis using wavelets (W-DFA)

There are several methods to deal with the scaling properties of the fluctuations displayed by many natural and technological processes. One method is the detrending fluctuation analysis (DFA) proposed by Peng in 1994 [11]; several years later, in [12], Kantelhardt and collaborators unveiled the multifractal detrending fluctuation analysis (MF-DFA), which is a generalization of the same method. Subsequently, a DFA procedure using wavelets was introduced by Manimaran [13]. Here, we implement the latter proposal, because it appears to be a very acceptable algorithm with a less computational cost and better accuracy to obtain important scaling properties in different applications, see for example [5, 14, 15] and references therein. In particular, this method exploits the fact that the approximation version of the discrete wavelet decomposition allows to calculate the local trend of information, which traditionally is achieved by a polynomial fit. In general, for a time series $x(t_k) = x[k]$, with

$t_k = k\Delta t$ and $k = 1, 2, \ldots, N$, this procedure consists of the following steps:

1. Calculate the profile $Y[k]$ of the temporal series,

$$Y[k] = \sum_{i=1}^{k} (x[i] - \mu) \tag{1}$$

where μ is the average of the time series $x[k]$.

2. Calculate the wavelet decomposition of the profile using the fast wavelet transform for each level m. The way in which the concept of levels enters in the algorithm is given in the Appendix.

3. Then, for each level m, obtain the fluctuations of the profile of the temporal series by subtracting the local trend of information, i.e.:

$$\Delta Y[k; m] = Y[k] - \tilde{Y}[k; m], \tag{2}$$

where $\tilde{Y}[k; m]$ is the profile reconstructed after removing of the detail coefficients at each level m.

4. The fluctuations $\Delta Y[k; m]$ at each level m are divided into $M_s = \text{int}(N/s)$ non-overlapping windows whose size is s. Because the length of N may not be a multiple of s, the division is performed beginning both with the start and the end of the profile, i.e., it has $2M_s$ segments. Subsequently, one calculates the local variances associated with each window ν

$$F^2[\nu, s; m] = \text{var}(\Delta Y[(\nu - 1)s + j; m]), \tag{3}$$

for each ν ($\nu = 1, \ldots, 2M_s$) $j = 1, \ldots, s$.

5. Next, perform an averaging over all segments to obtain the fluctuation function

$$F_2[s; m] = \left\{ \frac{1}{2M_s} \sum_{\nu=1}^{2M_s} |F^2[\nu, s; m]|^{1/2} \right\}^{1/2}. \tag{4}$$

6. Repeat steps 4 and 5 for different segment lengths s.

If the fluctuation function $F_2[s; m]$ displays a power law scaling

$$F_2[s; m] \sim s^{\alpha}, \tag{5}$$

then the analyzed sequence has a fractal scaling behavior with scaling fluctuation exponent α. This exponent can be found as the slope of the line in a $\log F_2[s;m]$ versus $\log s$ plot, and it is a measure of the degree of correlation in the sequence as follows. If $\alpha = 0.5$ there is no correlation and the uncorrelated signal is also known as coming from a white noise process. On the other hand, if $0 < \alpha < 0.5$ the signal presents an anticorrelated behavior evidenced through an alternation of small and large values, and the time series is said to be anti-persistent; if $0.5 < \alpha < 1$, the correlations in the time series are persistent, where large values in the series of data are more likely to appear after large values, and vice versa. The values $\alpha = 1$ and $\alpha = 1.5$ correspond to $1/f$ noise and Brownian motion, respectively.

To apply the W-DFA to images, we consider the steps similar to the DFA procedure used in Ref. [16], to study the correlations in image textures. Such a technique contains the following steps:

- Let $\mathbf{I}$ denote an image, and let $\mathbf{I}_\theta$ be a subimage of $\mathbf{I}$ with orientation θ. In this work, we consider two directions: the North-South orientation ($\theta = 0°$), and the East-West orientation ($\theta = 90°$).

- The subimage $\mathbf{I}_\theta$ is defined as a rectangular array $\mathbf{A}_\theta(a, b)$ with N rows and M columns, i.e., $a = 1, \ldots, N$, and $b = 1, \ldots, M$.

- For each subimage, the analysis can be performed depending on the orientation, either rows or columns. For example, for columns the W-DFA is applied to $\mathbf{A}_\theta(a, b)$ on each array column $a = 1, \ldots, N$, obtaining a fluctuation function $F_\theta[b; s; m]$, as calculated in the previous procedure, for each $b = 1, \ldots, M$.

- The scaling exponent can be determined from the geometric mean of the fluctuation functions

$$F_{\text{ave}}[s;m] = \left(\prod_{b=1}^{M} F_\theta[b;s;m] \right)^{1/M} . \tag{6}$$

  The analysis is also carried out for different segment lengths s, and the scaling exponent α_θ is calculated as the slope of the graph of $\log F_{\text{ave}}[s;m]$ in terms of $\log s$.

2.3. The peak signal-to-noise ratio

To assess the quality of reconstructed images the peak signal-to-noise ratio (PSNR) is usually considered. This metric is used to measure images' quality losses caused by certain operations such as transmission errors and compression, among others. PSNR is measured in decibels (dB) and is defined by

$$\mathrm{PSNR} = 10 \log_{10} \frac{L^2}{\mathrm{MSE}} \ , \tag{7}$$

where $L = (2^B - 1)$ is the image pixel's gray level, with B as the number of bits, and MSE denoting the mean square error, defined as

$$\mathrm{MSE} = \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \|\mathbf{I}(m,n) - \hat{\mathbf{I}}(m,n)\| \ , \tag{8}$$

where $\mathbf{I}$ is an $N \times M$ image and $\hat{\mathbf{I}}$ is its approximation. Assuming pixel values in the range $[0, 255]$, the reconstructed images have been considered in (7) of good quality if the PSNR values are of 30 dB or more.

3. Results and Discussion

To carry out the scaling analysis of the considered encryption schemes, we load a plain image $\mathbf{I}$ of size $N \times M$ 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). The results of applying the W-DFA method with the db-4 wavelet function to the mandrill test image and its full-encrypted versions are shown in Figure 2, where the North-South orientation, 0°, and the East-West one, 90°, are considered. In this work, the db-4 wavelet of MATLAB is used, which having 8 filter coefficients retains the cubic polynomial trend of the data [17], and thus provides a more accurate determination of their scaling characteristics. This is in agreement with the conclusions of references [18, 19].

One can observe that the values of the scaling exponent α provided by the three encryption systems used present a similar behavior in both directions. The complete scaling exponents for the image datasets and their encrypted versions are given in Table 1. We notice that the

majority of the scaling exponents α of the encrypted images are close to the value of 0.5, which suggests that the encrypted images present a behavior close to the Gaussian noise.

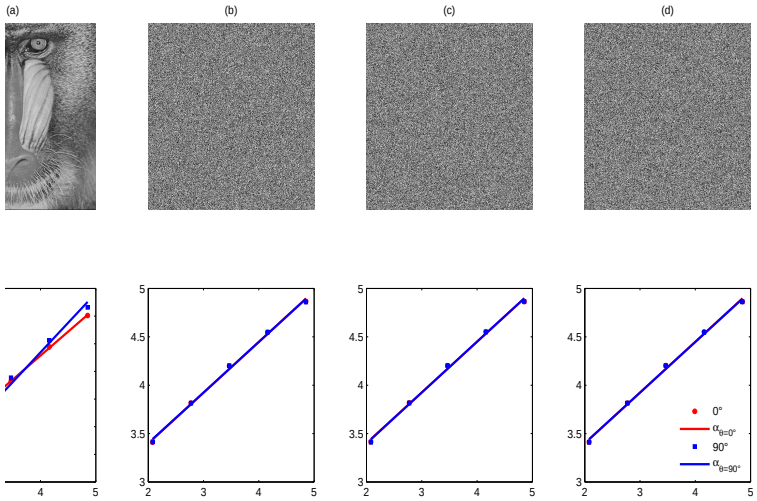

Figure 2: Top row: the mandrill image test (a) and the encrypted image performed with (b) the ESCAv1 system, (c) the ESCAv2 system, and (d) the AES system. Bottom row: their respective scaling fluctuation exponents provided by the fluctuation function of the W-DFA method.

Furthermore, we have reduced the time consuming negative feature of the encryption by a selective encryption process in which different groups of bitplanes for each of the images were chosen and encrypted. We have selected groups of four and three bitplanes, where the subset of bitplanes starts from the MSB until the subset of bitplanes containing LSB of the pixels is attained. To take into account all the possible combinations, a circular shift of one bit to the right is made until we get the corresponding number of selected bitplanes. For instance, in the case of four bits we obtained the eight following subsets: $b_8b_7b_6b_5$, $b_7b_6b_5b_4$, $\ldots$, $b_4b_3b_2b_1$, $b_3b_2b_1b_8$, $b_2b_1b_8b_7$, $b_1b_8b_7b_6$. This allows us to analyze the groups of bitplanes that preserve or not the most representative image information. The results of the W-DFA method for partial encryption of images for the resulting subsets of four and three bitplanes are presented in Figs. 3 and 4, respectively. The first and eighth subsets of bits considering three bitplanes are $b_8b_7b_6$ and $b_1b_8b_7$, respectively.

One can notice that for the encryption systems ESCAv1 and AES, the values of the scaling exponent are getting close to the values of the scaling exponents of the plain images as we get the fifth and sixth group of bits considering four and three bitplanes, respectively,

Table 1: The values of the α scaling exponents obtained from applying the W-DFA at the orientation of 0° to the eighteen test images and their encrypted versions.

Test	α exponents			
image	**Original**	**ESCAv1**	**ESCAv2**	**AES**
Bark	1.3328	0.5239	0.5218	0.5245
Beach sand	1.2326	0.5109	0.5111	0.5126
Brick	1.0595	0.5257	0.5227	0.5235
Grass	1.2586	0.5109	0.5123	0.5104
Leather	1.2498	0.5224	0.5243	0.5260
Lena	1.3219	0.5253	0.5255	0.5244
Mandrill	0.8647	0.5253	0.5240	0.5247
Peppers	1.5540	0.5225	0.5239	0.5247
Pigskin	1.2370	0.5246	0.5238	0.5249
Plastic bubbles	1.2790	0.5111	0.5104	0.5138
Raffia	1.2383	0.5240	0.5245	0.5262
Straw	1.4725	0.5273	0.5233	0.5209
Water	1.5743	0.5248	0.5250	0.5258
Weave	1.1953	0.5254	0.5248	0.5248
Wood	1.4895	0.5240	0.5234	0.5244
Wool	1.2503	0.5273	0.5252	0.5218
Yardangs	1.0099	0.5121	0.5110	0.5133
fBm	1.4099	0.5107	0.5123	0.5122

whereas for the encryption system ESCAv2 the scaling exponents remain without significant changes. These results illustrate that the latter encryption system can provide high confidentiality when a partial encryption is considered. In Figs. 5-7, we display the images after the selected bitplanes have been encrypted. We can observe that in some images there is sufficient structural information from which the original image can be traced out.

With the aim to assess the measure images' quality losses of the encrypted images, we compute the PSNR. Figures 8 and 9 display the values of the PSNR between the partially encrypted images and the original images. The results obtained with this metric present the

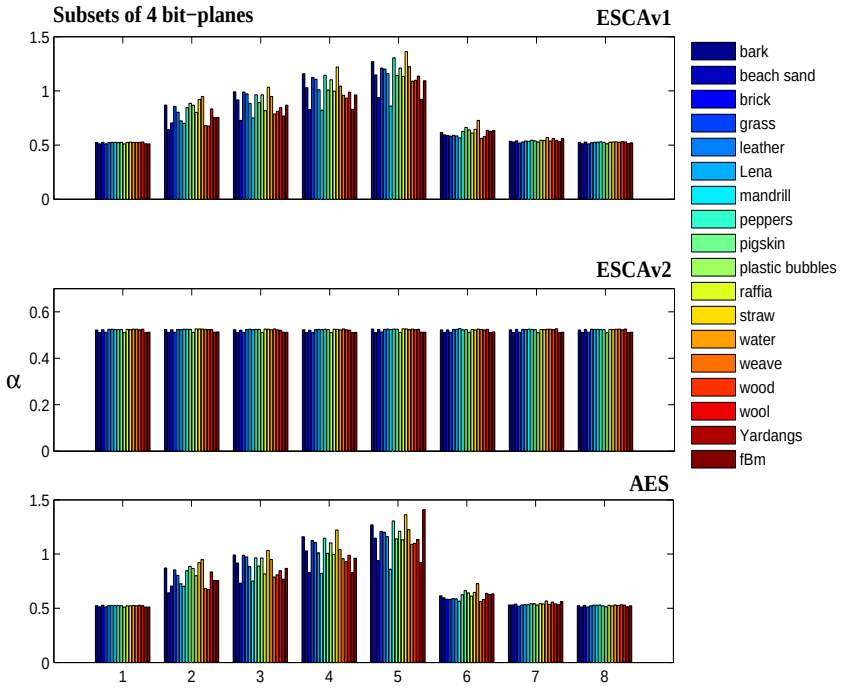

Figure 3: Scaling exponents of the encrypted images considering four bitplanes when the W-DFA algorithm is applied.

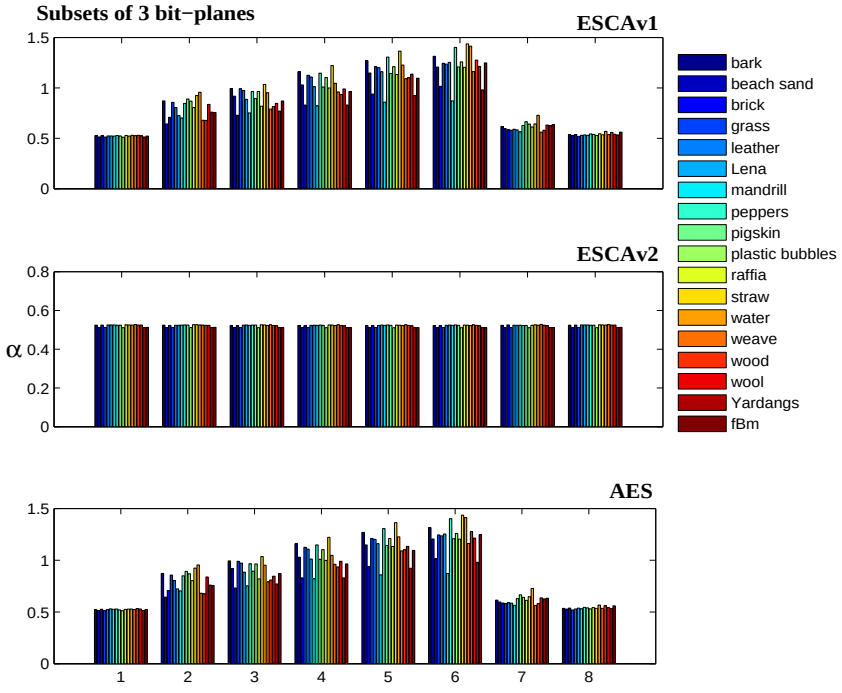

Figure 4: Scaling exponents of the encrypted images considering three bitplanes when the W-DFA algorithm is applied.

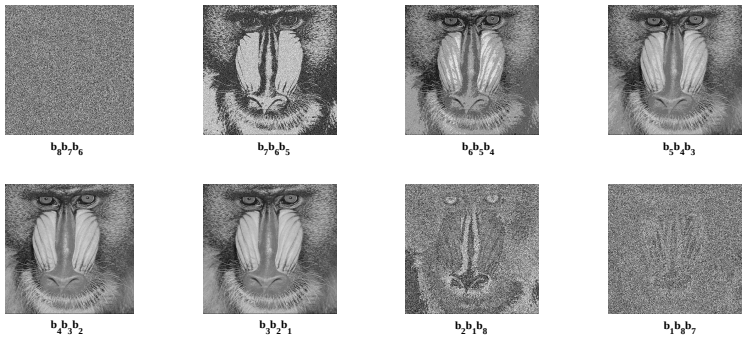

Figure 5: Partial encryption of the mandrill test image considering the selected three bitplanes when the cryptosystem ESCAv1 is applied.

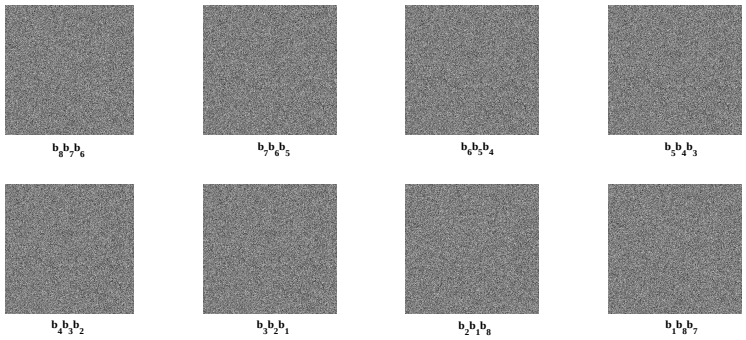

Figure 6: Partial encryption of the mandrill test image considering the selected three bitplanes when the cryptosystem ESCAv2 is applied.

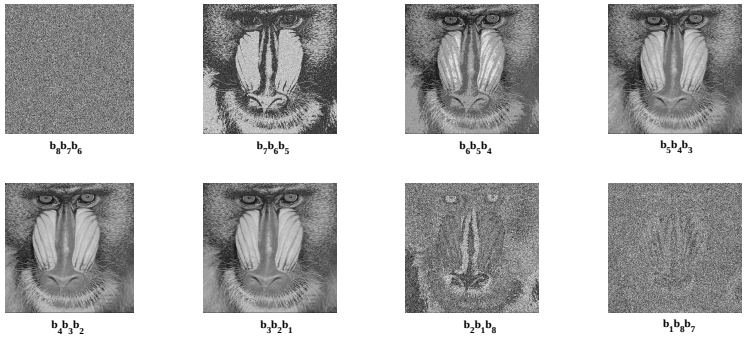

Figure 7: Partial encryption of the mandrill test image considering the selected three bitplanes when the cryptosystem AES is applied.

same tendency of the scaling coefficients. However, Sun and collaborators [20] found that the PSNR values do not work appropriately for the visual security assessment of some special

encryption algorithms. This means that sometimes this typical metric may not reflect a good visual security degree of the encrypted images

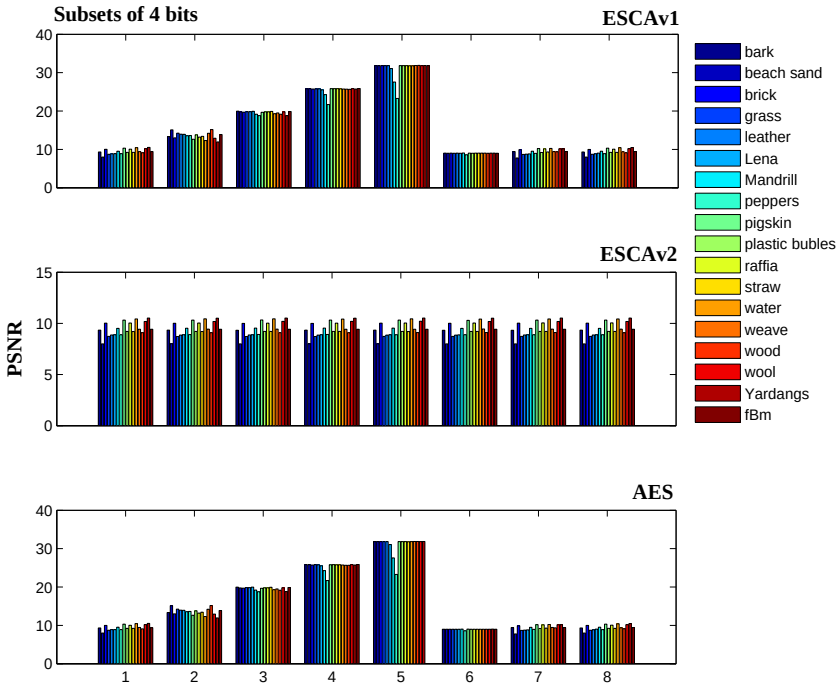

Figure 8: PSNR values of the encrypted images considering four bit-planes.

4. Conclusions

In this work, we have analysed the scaling behavior of different gray images that have been encrypted through three encryption schemes.

The scaling exponent has been calculated using the DFA method based on wavelets. The results show that if the most significant bits of an image are encrypted, the value of its scale exponent is very close to the value of the scale exponent corresponding to the encryption of the whole image, while if the encryption of the less significant bits is performed then the scale exponents are closer to the values corresponding to the initial image. Despite the fact that the PSNR is sometimes considered as an objective metric of encrypted images [1], this metric sometimes presents some drawbacks to have an objective visual security [20]. For this reason, we assert that the value of the scale exponent which is close to that for the Gaussian noise

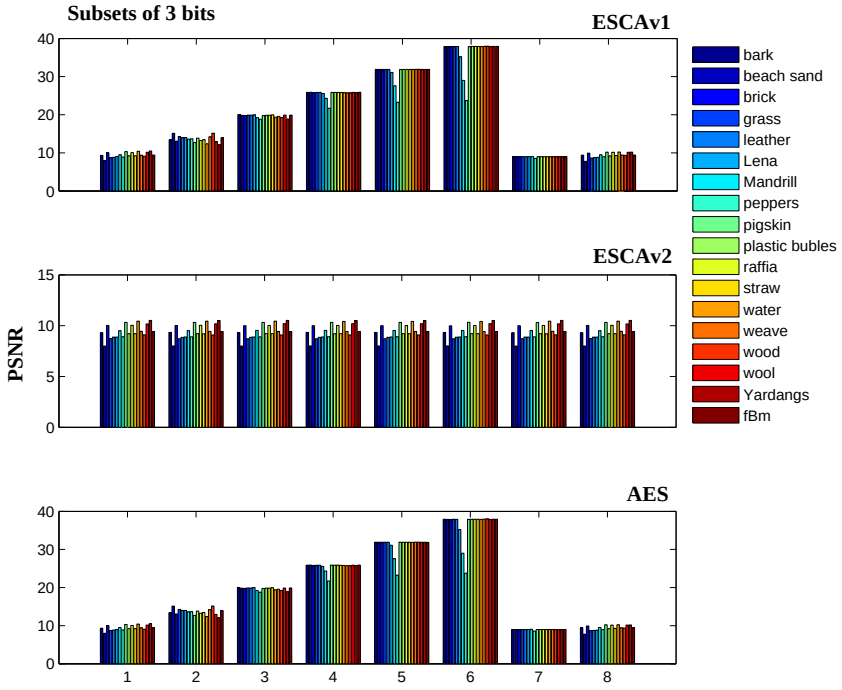

Figure 9: PSNR values of the encrypted images considering three bit-planes.

can be well chosen as an objective measure of the unintelligible features of the image that has been encrypted. This is because when such values occur the encrypted images do not reveal any piece of information that can allow to distinguish the original image. Moreover, although the PSNR of the encrypted images has the same tendency, the original and the encrypted images are needed altogether in order to make the appropriate calculations. This does not happen for the value of the scale exponent which can be calculated without having the original image.

However, one cannot fully guarantee so far that an encrypted image with such values of the scaling exponent is absolutely immune to any type of attack because while it is true that AES and ESCAv2 are highly reliable with respect to plaintext attacks when a full encryption scheme was applied to the image, this is not so for the ESCAv1.

Acknowledgments

This work received partial financial support from FAI-UASLP, and C. Vargas-Olmos has been supported by CONACyT through a doctoral fellowship at IICO-UASLP.

Appendix

The discrete wavelet transform (DWT) is considerably the most common choice for the persistently wavelet transform required when performing the analysis and synthesis of the original signal due to its enormous versatility for computational calculations through its multiresolution filter bank structure [21]. Within this framework, the representation of a function or process, $x(t)$, is given in terms of the translated and dilated versions of the wavelet function, $\psi(t)$, as well as its associated scaling function, $\varphi(t)$ [21]. Drawing on this principle and considering that the scaling and wavelet functions

$$\varphi_{m,n}(t) = 2^{m/2}\varphi(2^m t - n), \qquad \psi_{m,n}(t) = 2^{m/2}\psi(2^m t - n), \quad m, n = 0, \pm 1, \pm 2, \ldots \tag{9}$$

form an orthonormal basis, one can then write the expansion of $x(t)$ as

$$x(t) = \sum_n \left(a_{m_0,n}\varphi_{m_0,n}(t) + \sum_{m=m_0}^{M-1} d_{m,n}\psi_{m,n}(t) \right), \tag{10}$$

where the scaling or approximation coefficients $a_{m,n}$, and the wavelet coefficients $d_{m,n}$ are defined as

$$a_{m,n} = \int x(t)\varphi_{m,n}(t)dt, \qquad d_{m,n} = \int x(t)\psi_{m,n}(t)dt, \tag{11}$$

with m and n denoting the dilation and translation indices, respectively.

In this context, to calculate $a_{m,n}$ and $d_{m,n}$, Mallat [21] developed an efficient algorithm referred as fast wavelet transform (FWT), in which the multiresolution analysis (MRA) approach is involved. A multi-resolution decomposition of a signal is based on successive decomposition into a series of approximations and details, which become increasingly coarse. The FWT calculates the scaling and wavelet coefficients at scale m from the scaling coefficients at the next finer scale $m + 1$ using

$$a_{m,n} = \sum_k h[k - 2n]a_{m+1,k}, \tag{12}$$

$$d_{m,n} = \sum_k g[k - 2n]a_{m+1,k}, \tag{13}$$

where $h[n]$ and $g[n]$ are typically called low pass and high pass filters, respectively, in the associated analysis filter bank. In fact, the signals $a_{m,n}$ and $d_{m,n}$ correspond to the convolutions of $a_{m+1,n}$ with the filters $h[n]$ and $g[n]$ followed by a down-sampling of factor 2 [21], respectively.

Conversely, a reconstruction of the original scaling coefficients $a_{m+1,n}$ can be made from the following combination of the scaling and wavelet coefficients at a coarse scale

$$a_{m+1,n} = \sum_k \left(h[2k-n]a_{m,k} + g[2k-n]d_{m,k} \right) \ . \tag{14}$$

which corresponds to the synthesis filter bank, and represents the inverse of the FWT for computing (10). This part can be viewed as the discrete convolutions between the up-sampled signal $a_{m,l}$ and the filters $h[n]$ and $g[n]$. In other words, by following an up-sampling of factor 2, the convolutions between the up-sampled signal and the filters $h[n]$ and $g[n]$ are calculated.

To initialize the FWT, we consider a discrete time signal $X = \{x[1], x[2], \ldots, x[N]\}$ of length $N = 2^L$. The first application of (12) and (13), beginning with $a_{m+1,n} = x[n]$, defines the first level of the FWT of X. The process goes on, always adopting the $(m+1)$th scaling coefficients to calculate the "m" scaling and wavelet coefficients. Iterating (12) and (13) M times, the transformed signal consists of M sets of wavelet coefficients at scales $m = 1, \ldots, M$, and a signal set of scaling coefficients at scale M. There are exactly $2^{(L-m)}$ wavelet coefficients $d_{m,n}$ at each scale m, and $2^{(L-M)}$ scaling coefficients $a_{M,n}$. The maximum number of iterations is $M_{\max} = L$.

[1] Lian S. Multimedia content encryption. Techniques and applications. Boca Raton: CRC Press Taylor and Francis group; 2009.

[2] Vargas Olmos C, Murguía JS, Ramírez-Torres MT, Mejía Carlos M, Rosu HC, González Aguilar H. Two-dimensional DFA scaling analysis applied to encrypted images. Int. J. Mod. Phys. C 2015; 26:1550093.

[3] Podesser M, Schmidt H-P, Uhl A. Selective bitplane encryption for secure transmission of image data in mobile environments. In: Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002); 2002.

[4] Gu GF, Zhou WX. Detrended fluctuation analysis for fractals and multifractals in higher dimensions. Phys. Rev. E 2006; 74:061104.

[5] Murguía JS, Perez-Terrazas JE, Rosu HC. Multifractal properties of elementary cellular automata in a discrete wavelet approach of MF-DFA, Europhys. Lett. 2009; 87:28003.

[6] Grgic M, Delac K, Ghanbari M. Eds. Recent advanced in multimedia signal processing and communications. Berlin Heidelberg: Springer; 2009. p 422. Kulkarni NS, Raman B, Gupta I. Multimedia encryption: A brief overview, pp 417-449.

[7] Lian S, Sun J, Zhang D, Wang Z. Advances in multimedia information processing-PCM 2004. pp. 65-72. Berlin Heidelberg: Springer; 2005.

[8] Murguía JS, Flores-Eraña G, Mejía Carlos M, Rosu HC. Matrix approach of an encryption system based on cellular automata and its numerical implementation, Int. J. Mod. Phys. C 2012; 23:1250078.

[9] Ramírez-Torres MT, Murguía JS, and Mejía Carlos M. Image encryption with an improved cryptosystem based on a matrix approach. Int. J. Mod. Phys. C 2014; 25:1450054.

[10] Van Droogenbroeck M, Benedett R. Techniques for a selective encryption of uncompressed and compressed images. In: Proc. advanced concepts for intelligent vision systems (ACIVS). Ghent, Belgium, pp 90-97; 2002.

[11] Peng CK, Buldyrev SV, Havlin S, Simons M, Stanley HE, Goldberger AL. Mosaic organization of DNA nucleotides. Phys. Rev. E 1994; 49:1685-1689.

[12] Kantelhardt JW, Zschiegner SA, Koscielny-Bunde E, Havlin S, Bunde A, Stanley HE. Multifractal detrended fluctuation analysis of nonstationary time series. Physica A 2002; 316:87-114.

[13] Manimaran P, Panigrahi PK, Parikh JC. Wavelet analysis and scaling properties of time series, Phys. Rev. E 2005; 72:046120.

[14] Murguía JS, Rosu HC. Multifractal analyses of row sum signals of elementary cellular automata. Physica A 2012; 391:3638-3649.

[15] Murguía JS, Rosu HC, Jimenez A, Gutiérrez-Medina B, García-Meza JV. The Hurst exponents of Nitzschia sp. diatom trajectories observed by light microscopy. Physica A 2015; 417:176-184.

[16] Alvarez-Ramirez J, Rodriguez E, Cervantes I, Echeverria JC. Scaling properties of image textures: A detrending fluctuation analysis approach. Physica A 2006; 361:677-698.

[17] Manimaran P, Panigrahi PK, Parikh JC. Multiresolution analysis of fluctuations in non-stationary time series through discrete wavelets, Phys. A 2009; 388:2306–2314.

[18] P. Oświęcimka, J. Kwapień, S. Drożdż, Wavelet versus detrended fluctuation analysis of multifractal structures, Phys. Rev. E 2006; 74 Article no. 016103.

[19] P. Oświęcimka, J. Kwapień, S. Drożdż, A. Z. Górski, Effect of detrending on multifractal characteristics, Acta Phys. Polon. 2013; 123:597-603.

[20] Sun J, Xu Z, Liu J, Yao Y, An objective visual security assessment for cipher-images based on local entropy, Multimedia Tools and Applications 2011; 53:75-95.

[21] Stéphane Mallat, *A Wavelet Tour of Signal Processing*, 2nd. Edition, Academic Press, 1999.