ENHANCED CRYPTOGRAPHIC ALGORITHM BASED ON CHAOTIC MAPS AND WAVELET PACKETS

Corina MACOVEI[1], Adina-Elena LUPU (BLAJ)[2], Mircea RĂDUCANU[3]

This paper presents an enhanced version of an existing encryption algorithm by combining wavelets and chaos theory concepts. The novelty consists in replacing the simple permutation block in the existing algorithm with subbands permutation using logistic map and then integrating the tent map chaotic system to benefit from its properties. Subbands permutation is more secure than simple permutations. Chaotic maps add more security by their well-known properties: pseudo-randomness, ergodicity and sensitivity to initial conditions. The proposed encryption scheme is successfully applied on a wide range of images with different features. The theoretical analysis and Matlab simulations show that the enhanced algorithm produces secure encrypted signals. Also, a comparison between the original algorithm and its enhanced version is presented.

Keywords: chaos-based cryptographic algorithm, logistic map, tent map, subband wavelet decomposition

1. Introduction

Secure data transmission is perhaps one of the main challenges in the age of digitalization. The main technique used for this purpose is encryption, whether we are talking about text, images or video. Transmitting them on an insecure channel can be the target of cryptanalytic attacks, so data protection plays an important role. Although security is always a mandatory requirement, sometimes the encryption speed is more important, commonly used algorithms like DES (Data Encryption Standard) [1] and AES (Advanced Encryption Standard) [2] - time consuming and high complexity algorithms [3] - not being suitable. Thus, the use of chaotic maps is a good alternative due to their properties [4], such as sensitivity to initial conditions, ergodicity or random behavior that are relevant for encryption. The sensitivity to initial conditions - or to bifurcation parameters - means that if we encrypt a message with a chaotic map having some initial conditions/bifurcation parameters and another message with the same chaotic map

[1] PhD student, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania, e-mail: corina.macovei@stud.etti.upb.ro
[2] PhD student, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania, e-mail: adina_elena.lupu@stud.etti.upb.ro
[3] Assistent Professor, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania, e-mail: mircea@comm.pub.ro

and slightly different initial conditions or bifurcation parameters we obtain two different enciphered messages. Ergodicity ensures that the statistical properties of the process that describes the chaotic map can be computed from a single sample with many iterations. In addition, the speed and the low complexity make the chaotic maps-based encryption suitable for a large number of practical applications.

A speech encryption is presented in [5], where the speech signal is divided into blocks and then the wavelet transforms and the Hénon chaotic map are used to encrypt the signal. In [6] wavelet decomposition is mentioned as a method to remove noise in a forensic speech enhancement schema. Wavelet packets transforms and chaotic maps are used in [7] to perform simultaneously image compression and encryption. The proposed method is fast and efficient due to the two concurrent operations. Paper [8] presents wavelet packet transforms and chaotic maps as methods for securing sensitive biometric data. Another study, [9], presents a robust encryption scheme based on image decomposition into approximation and detail components using wavelets, followed by the diffusion of the approximation coefficients through a chaotic map. In [10], an adaptive encryption scheme for digital images based on wavelet optimization is presented. The wavelet transforms are used there to decompose the image, while a chaotic map is used to encrypt it. Paper [11] investigates the benefits of wavelets combined with chaotic maps in the new field of quantum computing.

Inspired by the algorithm designed and implemented in paper [12], this study proposes an improved version. The original algorithm is based on the Hénon chaotic map and consists in transformations, multiple substitutions and fixed transposition operations. The purpose, here, is to enhance the performance of the algorithm by replacing the pixels' permutation with subband decomposition and permutation of the resulted subbands with the logistic map. The reason we are performing this change is the fact that subband decomposition followed by permutation using a chaotic map is a more secure technique than a simple permutation of pixels, an additional security layer being added. The choice of the wavelet function used in this article is done by testing its behaviour in our context. By several trials, we concluded that Haar wavelet function is fitting our purpose due to its simplicity and good results. Furthermore, we replaced Hénon's map with the tent map chaotic system to benefit from the latter's uniform distribution.

2. Preliminaries

2.1 Wavelet transforms and wavelet packets

The Fourier transform is a representation of the signal in the frequency domain. Thus, the temporal or the spatial location, in the case of images, is lost. The Short-Time Fourier Transform (STFT) built as a windowed Fourier transform

overcomes this problem. However, the major deficiency of STFT is that for a chosen window function the time and frequency resolutions are constant for the entire time-frequency plane. The wavelet transforms correct this shortcoming of the STFT. The theory of continuous and discrete wavelet transforms [13], [14], wavelet packets [15-17], their connection with filter banks and sub-band analysis [18], [14], multi-resolution analysis have been presented in numerous papers that can be considered references for this field.

The continuous wavelet transform is defined:

$$Wf(a,b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{+\infty} f(t)\overline{\psi\left(\frac{t-b}{a}\right)}dt; \quad a \in \mathbb{R}^*, \quad b \in \mathbb{R} \tag{1}$$

where ψ(t) is a wavelet function.

The scaling function corresponding to two-dimensional images can be written as φ(x,y)=φ(x)φ(y). The wavelet function in one-dimensional case is transformed in three wavelet functions (horizontal, vertical and diagonal): $\psi^H(x,y)=\psi(x)\varphi(y)$, $\psi^V(x,y)=\varphi(x)\psi(y)$ and $\psi^D(x,y)=\psi(x)\psi(y)$.

The two-dimensional discrete wavelet transform (see Fig. 1) can be implemented using digital filters (h(n) and g(n) being the impulse response functions of a low-pass filter, respectively of a highpass filter) and downsamplers.

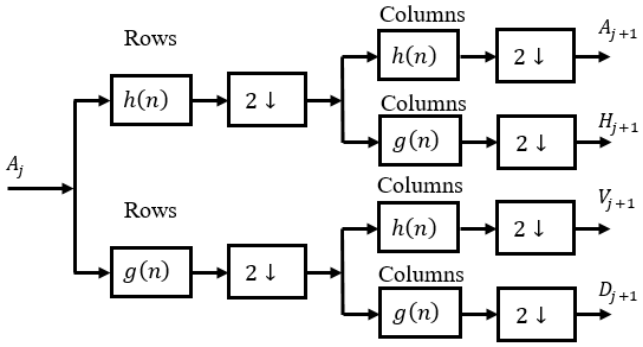

Fig. 1. The two-dimensional discrete wavelet transform

In Fig. 1, A_{j+1} is the approximation coefficient for the (j+1)th level, while H_{j+1}, V_{j+1} and D_{j+1} are three detail coefficients for the same level. The algorithm may continue recursively by decomposing the approximation coefficient A_{j+1}, thus obtaining the coefficients: A_{j+2}, H_{j+2}, V_{j+2} and D_{j+2}. Further, the low frequency component (A_{j+1}), as well as the high frequency components (H_{j+1}, V_{j+1}, D_{j+1}) are decomposed in subbands resulting wavelet packets, [17]-[18].

The Haar sequence was proposed in 1909 by A. Haar as an exemple of orthonormal system function for $L^2([0,1])$. Later on, it has been shown that these are actually wavelet functions. The Haar mother wavelet and scaling function are defined by:

$$\psi_H(t) = \begin{cases} 1;\ 0 \le t < 0.5 \\ -1;\ 0.5 \le t < 1 \\ 0;\ \text{otherwise} \end{cases}; \qquad \varphi_H(t) = \begin{cases} 1;\ 0 \le t < 1 \\ 0;\ \text{otherwise} \end{cases} \tag{2}$$

From (2) results the two-scale equations:

$$\varphi_H(t) = \varphi_H(2t) + \varphi_H(2t-1) \tag{3}$$

$$\psi_H(t) = \varphi_H(2t) - \varphi_H(2t-1) \tag{4}$$

In general, some Haar transform properties are exploited, namely:

- it has the simplest expression;
- it is the only symmetric wavelet in the Daubechies family;
- it allows the exact reconstruction of a signal (image) from the transform coefficients without introducing edge effects;
- it decomposes the vector of data representing the signal into two vectors of half its length;
- the impulse response h(n) and g(n) form a QMF (quadrature mirror filters) filter bank.

2.2 Chaotic maps

Two of the simplest chaotic maps are used in this paper: the logistic map and the tent map.

The definition of the logistic map is given by:

$$x_{k+1} = R\, x_k(1 - x_k) \tag{5}$$

where R is the control parameter with values in (0; 4] and x_k belongs to the domain (0; 1); k denotes discrete time.

The definition of the tent map [20] is given by equation:

$$y_{k+1} = \begin{cases} \frac{2}{p'+1} y_k + \frac{1-p'}{p'+1}, & -1 < y_k < p' \\ \frac{2}{p'-1} y_k - \frac{p'+1}{p'-1}, & p' \le y_k < 1 \end{cases} \tag{6}$$

where p' is the control parameter with values in (-1,1) / {0} and the generated y_k values belong to the (-1,1) interval; *k* denotes iteration.

The bifurcation parameters values are very important for chaotic maps, engendering the regime of the map: chaotic or periodic. In cryptographic applications only the values which lead to chaotic behavior are relevant. Metrics such as Lyapunov exponents and bifurcation diagrams are useful when selecting the bifurcation parameter value. Hence, to generate a chaotic behaviour for the logistic map, the bifurcation parameter R should be restricted to the interval [3.6, 4]. Also, when selecting R we must take into account the computation step to avoid periodicity of the map, as it was experimentally emphasized in [21]. In the case of the tent map, all the values p' belonging to (-1,1)/{0} lead to chaotic

behavior [20], this being one of the main reasons we choose this map in our implementation, alongside with its uniform distribution, independent of the bifurcation parameter value.

3. Chaos based cryptographic algorithm

3.1 Encryption algorithm based on the chaotic generalized Hénon map

In [12], it is proposed an encryption method based on simple operations, some permutations and XORs, that are embedded in a hyperchaotic map, the 3D generalized Hénon map. It is applied on different types of signals (text or image) leading to good results and high security.

The algorithm is performed in several steps, the first one being the division of the interval of chaotic map's possible values in ten subintervals corresponding to S-box (substitution box) subintervals. While iterating the chaotic map, the sine function is applied as function of two states of the map and the result is mapped to one of the subintervals. The next step is a bitxor operation between the value assigned to the S-box subinterval resulted from sine function and the plain message character or pixel converted to binary (1 byte). The result is then permuted according to a preset rule. The new encrypted message is converted from binary to decimal and scaled by a factor, ensuring that will preserve the chaotic behaviour. Finally, the cryptogram is included in the Hénon map iterations. The testing results prove this is an efficient and secure encryption scheme.

A disadvantage of this algorithm is the resulted non-uniform histogram of the encrypted image. A good encryption algorithm should lead to a uniform or gaussian histogram of the encrypted image, so no patterns could be detected. Another disadvantage is the long time needed to encrypt an image, about 941 seconds.

3.2 Proposed image encryption algorithm

Instead of implementing the generalized Hénon map, as in [12], this paper uses the tent map described in [20] to encrypt and embed the signal. The scheme of the encrypting algorithm is presented in Fig. 2.

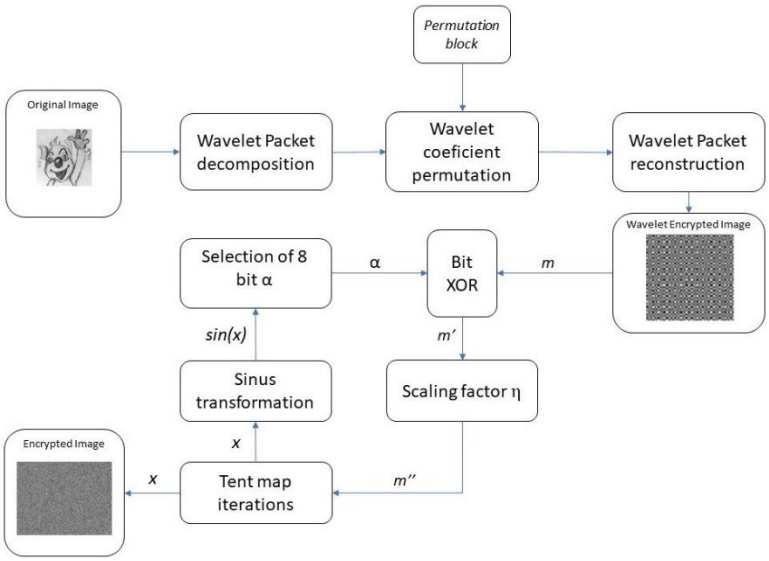

Fig. 2. Encrypting scheme

The encryption steps are the following:

- Image decomposition in subbands using the Haar wavelet packets on a fixed level.
- Subband permutation using the logistic map.
- Image reconstruction of the permuted wavelet packets.
- Divide the attractor of the tent map in 10 subintervals; the probability for a value generated by the tent map to fall in one of the 10 subintervals is uniform. This is one important advantage of the proposed algorithm over the one in [12].
- For each subinterval a value from $K_\alpha = \{\alpha_1, \alpha_2 \dots \alpha_{10}\}$ is associated, where α_i are fixed integers in (0, 255) interval; these α values are randomly chosen and stored in a vector.
- For each value *x*, generated by the tent map, apply a sinus transformation: *sine(x)*. This is necessary to ensure that the value is in the range (-1,1), after the message was embedded in the evolution of the map.
- Depending in which subinterval *sine(x)* falls, select the corresponding α value from K_α.
- The next step is a bit XOR between the 8 bit representation of α and 8 bits representation of the message (*m*).
- The resulted value *m′* is converted back to decimal and divided by $\eta = 10^5$, which results to *m″*.
- Finally, *m″* is added to the evolution of the chaotic map, resulting in the transmitted cryptogram.

We should mention that the original image in Fig. 2 is taken from the article used as reference [12] in our work. An important aspect is the fact that the bifurcation parameter of the chaotic map should be carefully selected, which is a part of the encryption/decryption key. Only the parameters with positive Lyapunov exponents may lead to a secure encryption [21].

4. Results and interpretation

A secure cryptographic algorithm should prove certain characteristics to be resistant to statistical and cryptanalytic attacks. These properties are evaluated through tools like histograms, entropy or correlation. The key space should be large enough to avoid the brute-force attack to succeed by exhaustive key search. The sensitivity to key changes should be a mandatory condition, since nowadays the attacker can try many possibilities within a reasonable time frame. If he computes the algorithm steps with some keys in the vicinity of the good key, then the output should be completely different compared to the output using the correct key. Also, the algorithm should be low time-consuming for both operations: encryption and decryption. Often a trade-off between the security of the system and its complexity should be considered.

In this paper we present the algorithm results illustrated on four gray PNG images having $256X256$ size. These images are displayed in Fig. 3, alongside with their corresponding histograms. The first image is also present in the previous article, the foundation of our work [12]. The second image is a landscape image taken by a phone camera, the image being characterized by high entropy. To better emphasize the difference between the original image and the encrypted one, the results are illustrated as well on two low entropy images having a few gray levels (the third and the fourth images in Fig. 3). The study was performed in parallel on the four images to highlight the idea that our algorithm can be applied on a large range of images with different properties.

The programming language used in our implementation is Matlab version R2017b and the algorithm was run on an ASUS ROG GR8 II system having the following properties:

- Windows-10 (64-bit).
- Processors: Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, 3.60GHz.
- Memory: 16-GB.

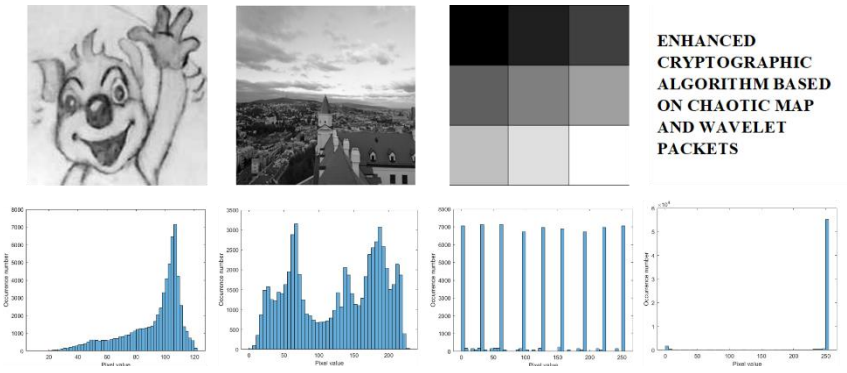

Fig. 3. Original images (up) and their corresponding histograms (down).

The first step of our algorithm is to apply on the original images the subband decomposition on 7 levels using the Haar wavelet function. Subband permutation using the logistic map is performed subsequently, followed by image reconstruction (see Fig. 4). One can notice that the images are unrecognizable, still some patterns are present. The histograms under each image in Fig. 4 show that the pixels are more diffused in the entire range (although these are not uniformly or Gaussian distributed), compared to the histograms of the original images.

For a better encryption we performed a XOR operation between elements of the wavelet encrypted image and an α value known. The result is divided to 10^5 and then added to the iterations' values of the tent map. Thus, a uniform distribution is obtained, see Fig. 6.

One disadvantage of our algorithm that should be taken into consideration is the fact that the encrypted image is eight times bigger than the original one because of multiple transformations applied. The size of the encrypted image is $512X1024$, while the size of the original one is $256X256$ as mentioned before. The decrypted image is the same as the original one, so it is perfectly reconstructed.

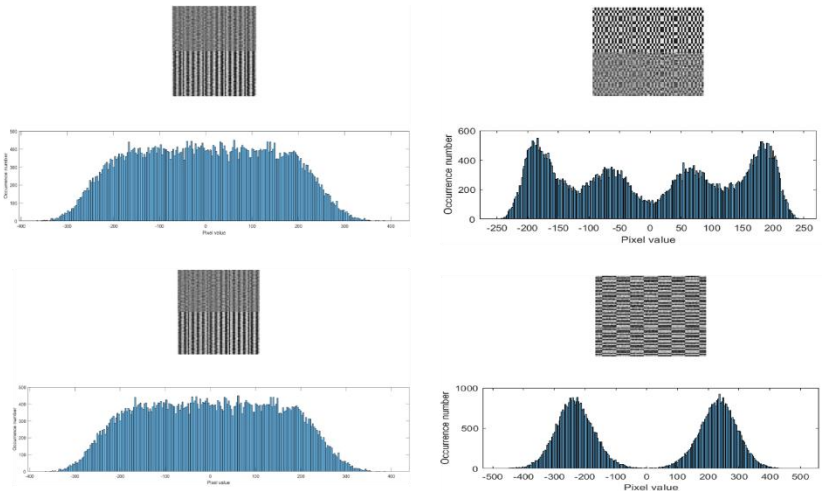

Fig. 4. Subband decomposition for cartoon (top-left), high entropy (top-right), low entropy (bottom-left) and bi-level (bottom-right) images and their corresponding histograms.

The entropy is a measure of randomness. An increased entropy means that the pixels are shuffled and the image redundancy is diffused. Considering this, it can be observed in Table I that the encrypted image entropy is close to the maximum value 8, meaning that the image is well-encrypted.

The correlation between adjacent pixels was analyzed by plotting scatter diagrams of the encrypted images compared to those of the original images as it can be seen in Fig. 5. Correlation measures the relationship between pixels. It is clear that a strong correlation exists between the pixels of the original images, while the encryption algorithm described in this paper leads to a weak correlation between the pixels.

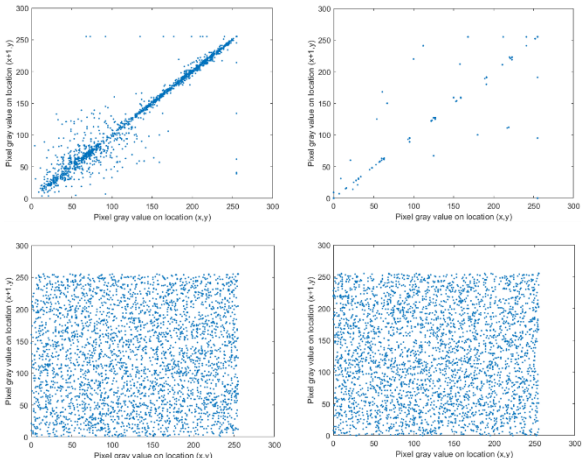

Fig. 5. Correlation for the original and the encrypted images– the high entropy image (left) and the low entropy image (right) – for the improved algorithm.

The encrypted image is sent to the receiver and he must know the encryption key to decrypt it. Subbands permutation key is represented by the initial condition and bifurcation parameter corresponding to the logistic map. For the second part of encryption, namely chaotic encryption, the key is the initial condition and bifurcation parameter of the tent map chaotic system.

5. A Comparison between Improved and Original Algorithms

As mentioned before, the new improved algorithm provides better results compared to the original algorithm. In Fig. 6 it is obvious that the histogram corresponding to the encrypted image with the new algorithm is uniform, while the other histogram corresponding to the original algorithm is not uniform. Well encrypted images should have uniform or Gaussian histograms.

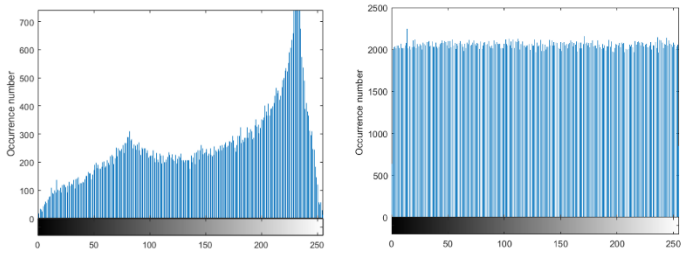

Fig. 6. Histograms for the encrypted image with the original algorithm vs. improved algorithm.

In Table 1, one can notice that the entropy for the encrypted image is close to the maximum value 8 when encryption is performed with the improved algorithm, while the entropy for encrypted image using the original algorithm (although is higher than the entropy for the plain image) is not close to the maximum value. The entropy enhancement with our algorithm is about 2.76% (compared to the original one), a higher entropy meaning a better encryption.

Table 1

Entropy values for encrypted images.

Image	Entropy original image	Entropy encrypted image with the original algorithm	Entropy encrypted image with the improved algorithm	Enhancement
Cartoon	5.9036	7.7863	7.9964	2.6983%
High Entropy	7.5909	7.7766	7.9966	2.8289%
Low Entropy	3.6309	7.7823	7.9966	2.7536%
Bi-level	1.9857	7.7798	7.9964	2.7841%

A low correlation between adjacent pixels corresponds to a good encryption. By comparing Fig. 5 and Fig. 7, it can be observed that the correlation between adjacent pixels is low for the image encrypted with the improved algorithm (Fig. 5) and a stronger correlation is present for the images encrypted with the original algorithm (Fig. 7).

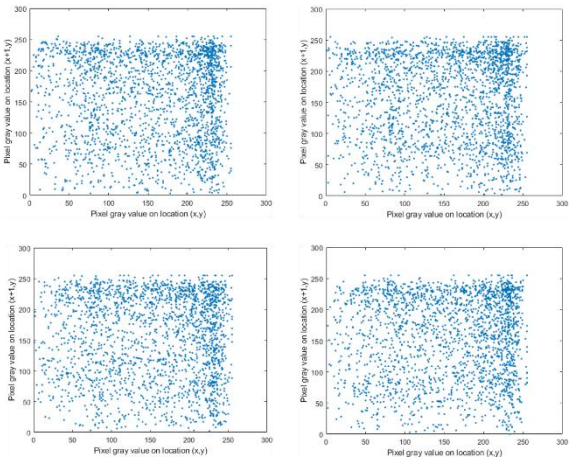

Fig. 7. Correlation for encrypted cartoon image(top left), high entropy level image (top right), low entropy level image (bottom left) and bi-level image(bottom right) with the original algorithm.

Also, the execution time was improved. This aspect is very important because the algorithms should run in a reasonable time to be used in real-time applications. The original algorithm runs in about 941 seconds for a PNG image of size $256X256$ and the time increase exponentially for large images. On the other hand, the improved algorithm presented in this paper runs in 48 seconds, being about 20 times faster.

6. Conclusions

The results show that the performance of the new encryption algorithm is independent of the image content and the proposed scheme is efficient and secure. It should be noted that the bi-level images are the ones that could benefit more from the proposed algorithm because those images contain pixels with just two values 0 or 255, these values being distributed in the entire possible range (0,255) in the encryption process.

The encryption is performed in two stages, thus ensuring resistance against cryptographic attacks. As future work, there are also other evaluations that should be taken into consideration when testing the algorithm results. Also, we intend to investigate other wavelet functions.

REFERENCES

[1]. *E. Biham* and *A. Shamir*, Differential cryptanalysis of the data encryption standard, Springer Science and Business Media, 2012.

[2]. *J. Daemen* and *V. Rijmen*, The design of Rijndael: AES-the advanced encryption standard, Springer Science and Business Media, 2013.

[3]. *J. S. Khan* and *J. Ahmad*, "Chaos based efficient selective image encryption", Multidimensional Systems and Signal Processing, 30(2), 943-961,2019, DOI: 10.1007/s11045-018-0589-x

[4]. *G. Alvarez* and *Li. Shujun*, "Some basic cryptographic requirements for chaos-based cryptosystems," International journal of bifurcation and chaos 16.08, 2006, 2129-2151.

[5]. *H.B.A. Wahab* and *I. M. Sundus*, "Speech Encryption Based on Wavelet Transformation and Chaotic Map," Engineering and Technology Journal 34.5 Part (B) Scientific, 2016, 721-729.

[6]. *Ghe. Pop*, and *D. Burileanu*, "Speech enhancement for forensic purposes," UPB Scientific Bulletin, Series C, **Vol.81**, Iss. 3, 2019, 41-52.

[7]. *Lv, X., Liao, X.* and *Yang, B.*, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," Multimed Tools Appl 77, 28633–28663 (2018). https://doi.org/10.1007/s11042-018-6013-6

[8]. G. *Bhatnagar* and *Q. M. JonathanWu*., "A Novel Chaotic Encryption Framework for Securing Palmprint Data," Procedia Computer Science 10 (2012): 442-449.

[9]. *Luo, Yuling, Minghui Du*, and *Junxiu Liu*., "A symmetrical image encryption scheme in wavelet and time domain," Communications in Nonlinear Science and Numerical Simulation 20.2 (2015): 447-460.

[10]. *Wang, Jian, Wenyuan Liu*, and *Shuai Zhang*. "Adaptive encryption of digital images based on lifting wavelet optimization," Multimedia Tools and Applications (2019): 1-24.

[11]. *Hu, Wen-Wen*, et al. "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," Quantum Information Processing 19.3 (2020): 1-29.

[12]. *O. Datcu, J.P. Barbot, A. Vlad*, "New enciphering algorithm based on chaotic Generalized Hénon Map," CHAOS THEORY Modeling, Simulation and Applications, 2011, 143-150.

[13]. *I. Daubechies*, Ten Lectures on Wavelets, **Vol. 61**, SIAM, Philadelphia, PA, 1992.

[14]. *M. Vetterli*, and *J. Kovačević*, Wavelets and Subband Coding, Prentice Hall PTR, 1995

[15]. *R. R. Coifman, Y. Meyer, S. Quake*, and *M. V. Wickerhauser*, "Signal processing and compression with wavelet packets," Technical report, Dept. of Math., Yale University, 1991.

[16]. *R. R. Coifman* and *M. V. Wickerhauser*, "Entropy-based algorithms for best basis selection," IEEE Trans. on Inform. Theory Special Issue on Wavelet Transforms and Multiresolution Signal Analysis, 38(2):713–718, March 1992.

[17]. *M. V. Wickerhause*, "Acoustic signal compression with wavelet packets," In C. K. Chui, editor, Wavelets: A Tutorial in Theory and Applications, 679–700, Academic Press, New York, 1992.

[18]. *M. Vetterli* and *C. Herley*, "Wavelet and filter banks: Theory and Design," IEEE Trans. Signal Proc., 40(9):2207–2232, September 1992.

[19]. *S. C. Phatak*, and *S. Suresh Rao*, "Logistic map: A possible random-number generator," Physical review E 51.4 (1995), 3670.

[20]. *D.M. Kato, M. Eisencraft*, "On the power spectral density of chaotic signals generated by skew tent maps," In 2007 ISSCS, (**Vol. 1**, pp. 1-4). IEEE, July 2007.

[21]. *O. Datcu, A.E. Lupu (Blaj), T. Blaj, R. Hobincu*, "NIST tests, Lyapunov exponents and bifurcation diagrams when evaluating chaos-based PRNGS," Special Issue of Proceedings of the Romanian Academy, Series A, The Publishing House Of The Romanian Academy, **Vol 21**, Issue 1, pp. 29-36, March 2020.