entropy

MDPI

Article

A New Algorithm for Digital Image Encryption Based on Chaos Theory

Yaghoub Pourasad [1,*], Ramin Ranjbarzadeh [2] and Abbas Mardani [3]

[1] Department of Electrical Engineering, Urmia University of Technology, Urmia 57561-51818, Iran
[2] Department of Telecommunications Engineering, Faculty of Engineering, University of Guilan, Rasht 45371-38791, Iran; ranjbar.ramin24@gmail.com
[3] College of Business, University of South Florida, Tampa, FL 33813, USA; abbasmardani@usf.edu
* Correspondence: y.pourasad@uut.ac.ir

Abstract: In recent decades, image encryption, as one of the significant information security fields, has attracted many researchers and scientists. However, several studies have been performed with different methods, and novel and useful algorithms have been suggested to improve secure image encryption schemes. Nowadays, chaotic methods have been found in diverse fields, such as the design of cryptosystems and image encryption. Chaotic methods-based digital image encryptions are a novel image encryption method. This technique uses random chaos sequences for encrypting images, and it is a highly-secured and fast method for image encryption. Limited accuracy is one of the disadvantages of this technique. This paper researches the chaos sequence and wavelet transform value to find gaps. Thus, a novel technique was proposed for digital image encryption and improved previous algorithms. The technique is run in MATLAB, and a comparison is made in terms of various performance metrics such as the Number of Pixels Change Rate (NPCR), Peak Signal to Noise Ratio (PSNR), Correlation coefficient, and Unified Average Changing Intensity (UACI). The simulation and theoretical analysis indicate the proposed scheme's effectiveness and show that this technique is a suitable choice for actual image encryption.

Keywords: digital image encryption; image processing; chaos random sequence; discrete wavelet transform

Citation: Pourasad, Y.; Ranjbarzadeh, R.; Mardani, A. A New Algorithm for Digital Image Encryption Based on Chaos Theory. *Entropy* **2021**, *23*, 341. https://doi.org/10.3390/e23030341

Academic Editors: Abbas Mardani, Edmundas Kazimieras Zavadskas, Dragan Pamučar and Fausto Cavallaro

Received: 6 February 2021
Accepted: 8 March 2021
Published: 13 March 2021

1. Introduction

In recent years, image encryption has been an attractive area for research. It is extensively recognized as a useful technique for secure transmission. Every image encryption algorithm is aimed to generate a noisy image's top-quality to keep information secret [1,2]. Additionally, image encryption has a preferable part for guaranteeing classified transmission and image capacity over the web. Digital communication has become broader by the fast development of Internet technology [3,4]. People can send a digital image on the Internet anytime and anywhere [5,6]. This has resulted in the development of digital image encryption. Different methods representing digital image encryption in studies are connected to the ever-increasing necessity of security. Image encryption based on the chaos method is a novel encryption method for images where a random chaos sequence is applied for encrypting the image as an effective way for solving the intractable problems of highly secure and fast image encryption. Over the last few years, various versions of the chaos technique have been presented. Presently, four approaches have been adopted for image encryption, applying various principles individually and achieving the same objectives. The four principles include sharing and secret segmentation, sequential permutation, chaotic dynamical systems, and modern cryptography, each with unique features [7–13]. Chaos-based effective selective image encryption [14] was introduced by Khan et al. First, the plaintext image is initially divided by the proposed technique into some

blocks. The correlation coefficients are determined. The block with the highest association coefficients is pixel-wise eXclusive OR-2ed (XORed) with the random numbers created from a skew tent map in terms of a pre-determined threshold value. Ultimately, the entire image is permuted through two random sequences created from Two Dimensional Ellipse Reflecting Chaotic System (TD-ERCS) chaotic maps. A novel fast image encryption algorithm oriented by chaos [15] was introduced by Wang et al., oriented by the permutation-diffusion architecture. In their method, the image is first separated into pixel blocks.

The spatiotemporal chaos is then utilized for shuffling the blocks and simultaneously changing the pixel values. Patidar et al. represented another vigorous pseudorandom permutation-substitution outline based on chaos for image encryption [16]. It was a loss-less symmetric block cipher and designed especially for color images. It may also be utilized for grayscale images. Wang et al. proposed a block image encryption outline in dynamic random growth and chaotic hybrid maps [17]. Since the cat map is simply fractured by selected plaintext attack, and it is periodic, in another securer way, they used the cat map for eliminating the cyclical phenomenon and resisting selected plaintext attack. Volos et al. presented an image encryption procedure in terms of chaotic synchronization phenomena [18]. They provided a new image encryption scheme through a chaotic TRBG (True Random Bits Generator). Image encryption based on synchronizing fractional chaotic systems [19] was utilized by Xu et al. A DNA sequence and a hybrid genetic algorithm were used for image encryption by Enayatifar et al. [20]. They presented a new image encryption algorithm using a hybrid model of a genetic algorithm (GA), deoxyribonucleic acid (DNA) masking, and a logistic map. Xu et al. introduced a novel bit-level image encryption algorithm oriented by chaotic maps [21]. Chaos-based Genetic Algorithms are extensively utilized for image encryption by many researchers [22–26]. Multiple-image encryption through the robust chaotic map in wavelet transform domains [27] was represented by Li et al. In this work, first, discrete wavelet transform (DWT) was used to decompose the original images being used and reassemble the lower frequency components as the direct images (estimated images). The direct image was then totally scrambled through Arnold's cat map. Third, further decomposing the scrambled image and the resulting block images are employed separately to integrate with the amplitude parameter of the RCM (robust chaotic map) for generating keystream in each diffusion procedure. Satish et al. presented an outline to encrypt an image through the Logistic Map [28]. It would scramble the image pixels. Thus, the resulting cipher image will be XOR encrypted while dividing the output into various frequency coefficients through Integer Wavelet Decomposition. The Logistic Map is used to shuffle the resulting low-frequency coefficient wavelet, and all the frequency coefficient wavelets will be integrated via Inverse Integer Wavelet Transformation. The main objective of this manuscript provides a new technique based on chaos theory for digital image encryption. Nevertheless, the chaos-based image encryption technique has some problems, including limited accuracy. For this reason, in this research, the encryption of images is divided into spatial and transform domain encryption. Over the last few years, some image encryption schemes were presented by the frequency domain and spatial domain. Spatial domain methods directly act on the pixels of the plain image. Because this method contains high-speed encryption, it is used widely [29-30]. The transform domain encryption is used, considering some typical properties of digital images as a strong correlation between high redundancy and nearby pixels.

A method of encryption-decryption employing Rivest–Shamir–Adleman (RSA) algorithm components and topological image protection was suggested by Kovalchuk et al. The main advantages of the suggested approaches are accomplished by using images with functional fluctuation intensity [31]. The effect of the noise-adding functions added to the source picture, and also the different values of simple numbers of the RSA scheme on the effects of the process were analyzed in another work. These results were set to not give rise to the presence of contours in the encrypted image [32]. Additionally, other approaches, such as linear and quadratic fractal algorithms [33,34], projective transformations [35], and binary linear-quadratic transformations [36], are also used for image

encryption and decryption. A model of image encryption based on a complex chaos-based pseudorandom number generator and modified advanced encryption standard was proposed by Hafsa et al. On the Altera Cyclone III board, the overall system was created. The findings revealed that the cryptographic algorithm was quicker and could withstand attacks of some kind [37]. A novel grayscale image cryptosystem based on chaotic hybrid maps was introduced by Kari et al. The proposed scheme has better properties, including broader chaotic ranges and more dynamic chaotic behavior, based on the results [38].

This paper is oriented by the chaos sequence and wavelet transform value and the integration of the image encryption algorithm. Such algorithms are simulated through analyzing the algorithm to discover the gaps. Thus, the algorithm was enhanced. This method uses two one-dimensional chaotic systems that can use even a fundamental nonlinear equation to display chaotic behavior. Our main aim, as well as the proportion of taking this kind of map, is to discover a new discrete-time sequence, the same as the chaotic output of the logistic map with elementary equations with unique parameters.

This paper is presented in the following sections. In the "Introduction" section, the motivation and the statement of the problem are described. Moreover, the literature review of the related papers is interpreted in this section. Furthermore, in the "Methods and Materials," the basic mathematical concepts and expression of the proposed method are presented. Moreover, in the "Proposed Algorithm" section, the result of the proposed model implementation is described using graphical figures and tables. In addition, the comparison is presented in the "Proposed Algorithm" section. In the "Discussion" section, the findings are interpreted, and previous studies, hypotheses, limitations and suggested future works are described. Finally, the "Conclusion" section summarizes the results by numerical outcomes and perspective concepts.

2. Materials and Methods

2.1. Chaos and Transformation Theories

Nowadays, chaos and transformation theories have emerged as novel currencies in social sciences. Image transformation is a technique simplifying image processing and improving the performance of image processing. Image enhancement denotes highlighting and sharpening definite features. It includes the contours, edges, and contrast of an image to display, observe, or further analyze and process the image [39–42]. Chaos theory presents the 1st Transdisciplinary understanding of bifurcation and transformational change. As a mathematics field, it has focused on the dynamical systems' behavior with extreme sensitivity to primary conditions. Numerous attempts exist to apply chaotic signals for communications. However, there is a lack of a useful way for recovering chaotic signals from noises larger than the signals.

2.2. Chaotic Sequence Based on Logistic Map

A one discrete-time-dimensional nonlinear system displaying quadratic nonlinearity is called a logistic map. The logistics map is shown with the following function. f: [0, 1] $\rightarrow\Re$ as

$$f(x) = \mu_x(1 - x) \tag{1}$$

which is stated in state equation form as

$$x_{n+1} = f(x_n) = \mu_{xn}(1 - x), n = 1,2,\ldots \tag{2}$$

where $x_n \in (0,1)$ and $\mu \in (0,4)$ are known as the control parameter or bifurcation parameter.

Here, x_n represents the system's state at time $n.x_{n+1}$ indicates the following state, and n shows the discrete-time. By repeated iteration of *f*, a sequence of points $\{x_n\}\infty$ is increased, known as an orbit. The performance of the logistic map is sensitive to the value of μ. For $\mu \in (3.574)$, the logistic map is chaotic [43]. Now, the diffusion algorithm key is

chosen, for which the actual y, the primary iteration of the logistics, is with parameter μ. For different primary conditions, two logistic maps are utilized for executing the repetition operation. Moreover, the values of the state of two logistic maps are measured dynamically. With this operation, chaotic sequences are produced. The operation is as follows: place a grayscale image G with the size of $m \times n$, the two-dimensional data matrix of R, turn R into the one-dimensional matrix with the length of $m \times n$. Put R1 = {r_1, $r_2 \ldots r_{m \times n}$}, and put P_1 = {p_1, $p_2 \ldots p_{m \times n}$} as the encrypted 1D matrix. The procedure of the encrypted algorithm will be as follows:

Step NO.1: In the first step, two chaotic sequences, x = {x_1, $x_2 \ldots x_{m \times n}$} are produced by two one-dimensional logistic maps. Place the two logistic maps system parameter as a primary value as $x_1(0)$ and $x_2(0)$, respectively.

Step NO.2: In the second step, for every iteration, compare $x_1(i)$, and $x_2(i)$, i = 1, 2, m × n and choose one that is numerically larger.

Step NO.3: In the next step, perform the Exclusive NOR (XNOR) operation for sequences produced by Step NO.2 with the original image's pixels.

Step NO.4: In the last step, change the encrypted one-dimensional matrix, namely P, into a two-dimensional matrix. Set the size of this modified matrix to m × n. In this process, a two-dimensional data matrix R2 is generated. Thus, a diffused image is obtained.

2.3. Kinetics of Coupled Map Lattice

One of the most popular classes of models in the theory of space-time chaos is formed by the coupled map lattice (CML). Coupled map lattices are extensively applied to survey the dynamics of spatially prolonged logistic map systems. The CMLs are used in cryptography, physics, economics, steganography, and biology. They have a significant role in image encryption algorithms [44–46]. Then, we used a two-dimensional hyper-chaotic map CML to try pixel location. It can effectively and efficiently extend the keyspace. It increases the capability of anti-decryption. CML statement is as:

$$x_{n+1} = 1 - a(x_n^2 + y_n^2) \tag{3}$$

$$y_{n+1} = -2a(1 - 2b)x_n y_n \tag{4}$$

The digital images possess the digital matrix features for scrambling the location of pixels; thus, considering a random image, the impact of confidentiality is accomplished. The procedure of the encrypted algorithm will be as follows:

Step NO.1: In the first step, the chaotic sequences x_1, x_2 = {x_1, $x_2 \ldots x_m$} are produced with the length of m, and y_1, y_2 = {y_1, $y_2 \ldots y_n$} with the length of n similar to CML chaos mapping.

Step NO.2: In the second step, x, y chaotic sequences are arranged in rising sequences, producing position sequences w_2, w_3.

Step NO.3: In the last step, the pixel confusion is performed, using w_2, w_3 as the row, and column sequences of the data matrix R.

$$R(i, 1) = R(w_2(i, w_3(j))). \tag{5}$$

2.4. Wavelet Transform

A valuable instrument for analyzing the signal's frequency components is called the Fourier transform. Taking the Fourier to convert over the whole-time axis, it is impossible to determine the exact instant of increasing a specific frequency. The Fourier transform and the wavelet transform are the same with a completely various merit function. The wavelet transforms mainly aimed at only allowing changes by transforming the time extension rather than the shape. The main difference between these two is that the signal is decomposed by the Fourier transform into cosines and sine's; however, the wavelet transform utilizes the functions localized in both the Fourier and real space. Commonly, the wavelet transform is stated as follows:

$$f(a,b) = \int_{\infty}^{-\infty} f(x)\Psi^{*}(a,b).x.d(x) \quad (6)$$

in which * represents the complex conjugate symbol and function φ is a function which can be arbitrarily selected if it follows definite rules. The wavelet transform can have a signal into time, space, and frequency as independent space. It also focuses on the specific signal of any local details. Thus, further information can be extracted effectively from the signals much by wavelet transform.

Numerous types of wavelet transforms exist for particular purposes. We used continuous and discrete wavelet transforms to extract further information from the signals. Similar to the Fourier transform, inner products are used by the continuous wavelet transform for measuring the similarity between a signal and an analyzing function. Theoretical analysis is one of the areas for using a continuous wavelet transform. Within the particular realization on computers as a functional area of research, a continuous wavelet must be discretized [47–50]. Running the wavelet transformation through a discrete set of wavelet scales and translations following some determined rules is known as the discrete wavelet transform. The signal is decomposed by transforming into the mutually orthogonal group of wavelets as the necessary variation from the continuous wavelet transforms.

Moreover, the implementations for the discrete-time series are occasionally determined as the discrete-time continuous wavelet transforms. It is the most significant point to select the wavelet utilized for time-frequency decomposition. Through this selection, we can affect the frequency and time resolution of the results. This way cannot replace Wavelet Transformation (WT)'s basic features (low frequencies possess a wrong time resolution and true frequencies; higher frequencies possess a wrong frequency resolution and a good time). However, it is somehow possible to increment the total time resolution's total frequency. It is straightly proportional to the utilized wavelet's width in the Fourier and real space. Using the Morlet wavelet, we can presume high-frequency resolution as a very well-localized wavelet in frequencies. In reverse, utilizing a Derivative of Gaussian wavelet will lead to the right time localization but lower frequencies.

3. Proposed Algorithm

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

Figure 1 represents the proposed algorithm. The steps for implementing the suggested algorithm are:

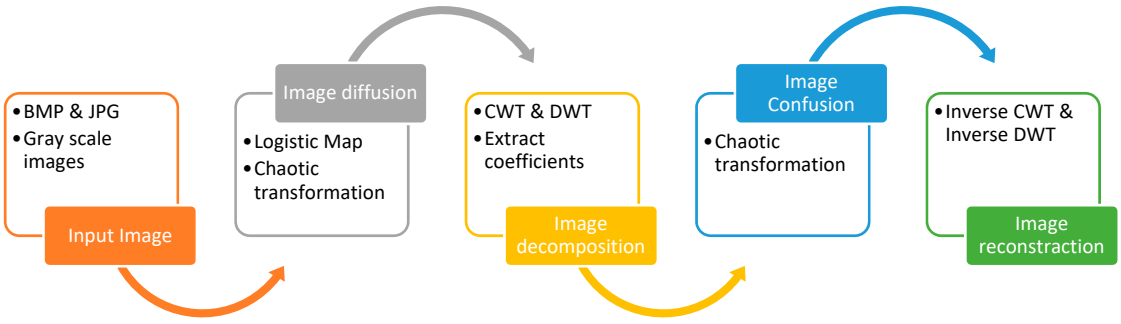


Figure 1. The proposed algorithm for image encryption: CWT: Continuous Wavelet Transform; DWT: Discrete Wavelet Table 1. In the first step, a grayscale image G is arranged. The image's size is set to m × n. Moreover, data matrix R is placed. By evaluating two logistic maps, a chaotic sequence is generated. Making XNOR with the primary image, the diffusion is terminated.

Step NO.2: In this step, for the diffused image in step NO.1, the wavelet decomposition is performed and then the wavelet coefficient is extracted, registered as ca1.

Step NO.3: Utilizing a two-dimensional hyper-chaotic map CML, the chaotic sequence is produced, and with ca1 established in step NO.2, the position confusion is performed.

Step NO.4: In the last step, the confused image can be rebuilt by wavelet. After all, the encrypted image is obtained. The inverse operations of the encryption are known as the decryption algorithm. System parameters and the primary value of the chaotic sequences in the image encryption and image decryption are consistent.

3.1. Encryption Assessments Metrics

We measured our cryptography scheme's performance by selecting some basic parameters to assess the algorithm. Visual inspection is one of the main parameters for assessing the encrypted images [51–53]. The characteristic diffusion survey is another parameter [54,55] determined for judging the randomization algorithm. Through inspection, the deviation of a product from a definite set of features is determined. Human operators usually accomplish the inspection; nevertheless, machine vision is utilized for automating this procedure [56–58]. By the excellent diffusion of an algorithm, the association between the original image and the encrypted image becomes too complicated and cannot be predicted simply. Here, we studied the Peak Signal to Noise Ratio (PSNR) computation metrics, the association between the encrypted image and the key-image. Ultimately, we assessed the specification diffusion by calculating two parameters of the Unified Average Changing Intensity (UACI) and the Number of Pixels Change Rate (NPCR).

3.2. Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) is an engineering formulation determined through mean square error (MSE). It is generally utilized for image quality evaluation as follows [59]:

$$PSNR = 10 \log\left(\frac{255^2}{MSE(f, f')}\right) \tag{7}$$

where f(x; y) and f′(x; y) denote the pixel values of m × n original and reconstructed images.

3.3. Number of Pixels Change Rate (NPCR)

Diffusion is represented by the number of the most essential parameters for judging the encryption algorithm randomization. NPCRs are used to examine the image encryption algorithm's security. Considering C_1 and C_2 as the two images with N × M size, we defined an array, D, with the sizes similar to images C_1 and C_2 as:

$$D(i,j) = \begin{cases} 0 if C_1(i,j) = C_2(i,j) \\ 1 if C_1(i,j) \neq C_2(i,j) \end{cases} \tag{8}$$

The NPCR determines the percentage of pixels within two different images, and it can be calculated as follows [31]:

$$NPCR = \frac{\sum_{ij-1}^{N \times M} D(i,j)}{N \times M} \times 100\% \tag{9}$$

3.4. Unified Average Changing Intensity (UACI)

UACI determines the average intensity of the difference within the two encrypted images (C_1 and C_2), using the below expression [60]. It is applied to evaluate the encryption method's strength. Its value is based on the image's format and size [61,62]. Through

UACI, the average variation in intensity between the ciphered and original images is assessed. The greatest UACI indicates that the suggested technique has resistance against various attacks. UACI is determined for the grayscale image of size M × N as follows:

$$UACI = \frac{1}{N \times M}\left[\sum_{ij-1}^{N \times M} \frac{C_1(i,j) - C_2(i,j)}{MAX(C_2)}\right] \times 100\% \quad (10)$$

3.5. Correlation Coefficient

Digital Image Correlation (DIC) is a key and extensively utilized non-contact method to measure material deformation. In recent years, there has been a significant development in developing novel experimental DIC methods and in improving the relevant computational algorithms' performance [63,64]. Thus, a relation is indicated among the same pixels of the encrypted and the original images as follows:

$$NC = \frac{\sum m \times \sum n(A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(A_{mn} - \bar{A})^2 (B_{mn} - \bar{B})^2}} \quad (11)$$

where A and B, respectively, denote the original image and the encrypted one, as well as their means. The lower correlation coefficient value is optimal.

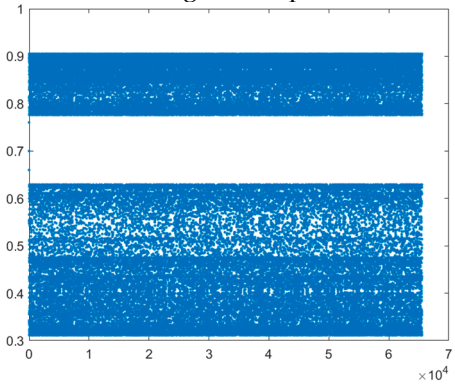
4. Experimental and Numerical Results

The results of the presented algorithm steps are indicated in Figure 2. In the first step, the input grayscale image with a size of m × n is imported. Based on Figure 2, a chaotic sequence is created with the two logistic maps used. Finally, in the diffusion step, the secure key is generated for encryption. For the encryption of the input image, the secure key must be inserted between the wavelet decomposition sub band. The sub bands of the DWT method are indicated in Figure 2. Upper to lower and left to right images in the DWT sub-bands are Low-Low, Low-High, High-Low and High-High sub bands. Utilizing a two-dimensional hyper-chaotic map CML, the chaotic sequence is produced and the confusion is performed. In the final step, the confused image is generated. Finally, the image consists of an encrypted matrix with the use of an input image and secure key.

Input Image

Diffusion (Secure Key)

Logistic map



CWT and DWT

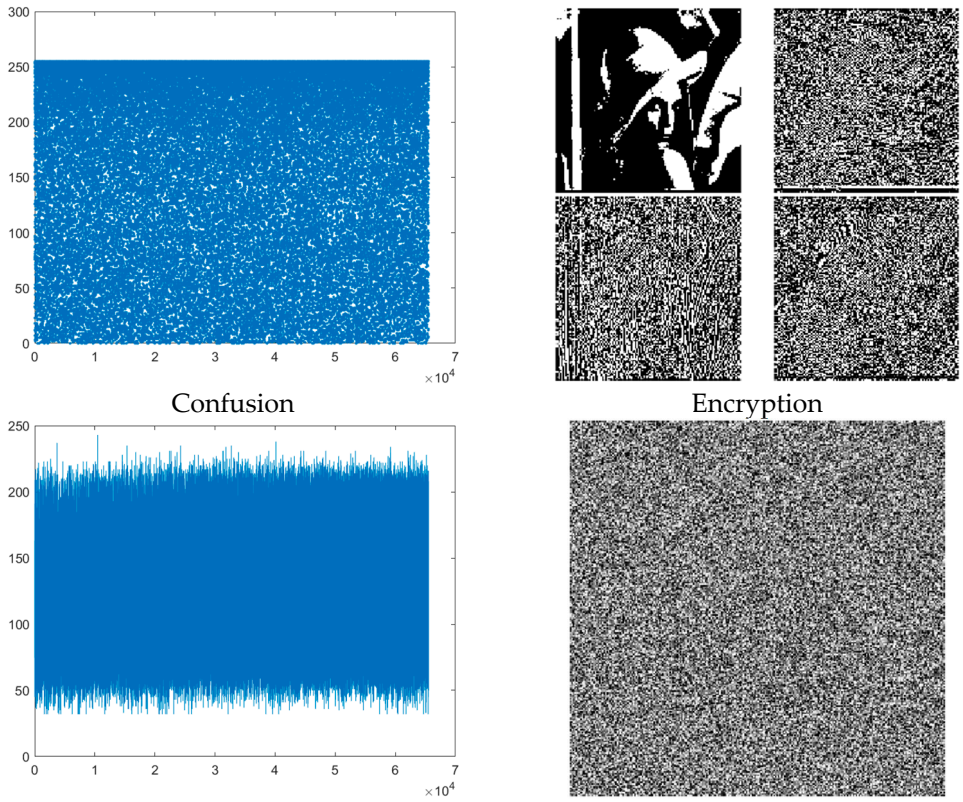


Figure 2. Results of the proposed method steps.

Evaluating the suggested algorithm with numerical results indicates that this algorithm is robust. Numerical results for the proposed algorithm are displayed in Table 1.

Table 1. The numerical results of the proposed algorithm.

Image	Type of Image	PSNR	NPCR	UACI	NC
Lena Image	Jpg	42.612	99.757	33.120	0.9548
Peppers Image	Jpg	39.220	99.787	33.621	0.9934
Barbara Image	Jpg	36.841	99.626	33.126	0.9809
Baboon Image	Jpg	39.134	99.881	33.415	0.9137
Boat Image	Jpg	38.223	99.625	33.671	0.9001

First, the diffusion operation is performed for the encryption of the primary image (original image). The primary key value is taken from Table 2; then, the confusion operation is performed while taking the primary key value from Table 2. The findings of encryption are the same as the noise (Figure 3). No information on the original image is acquired from the encrypted image. A decrypted image is acquired via the key for decrypting the encrypted image, followed by diffusion and confusion operations (Figure 3, decrypted image).

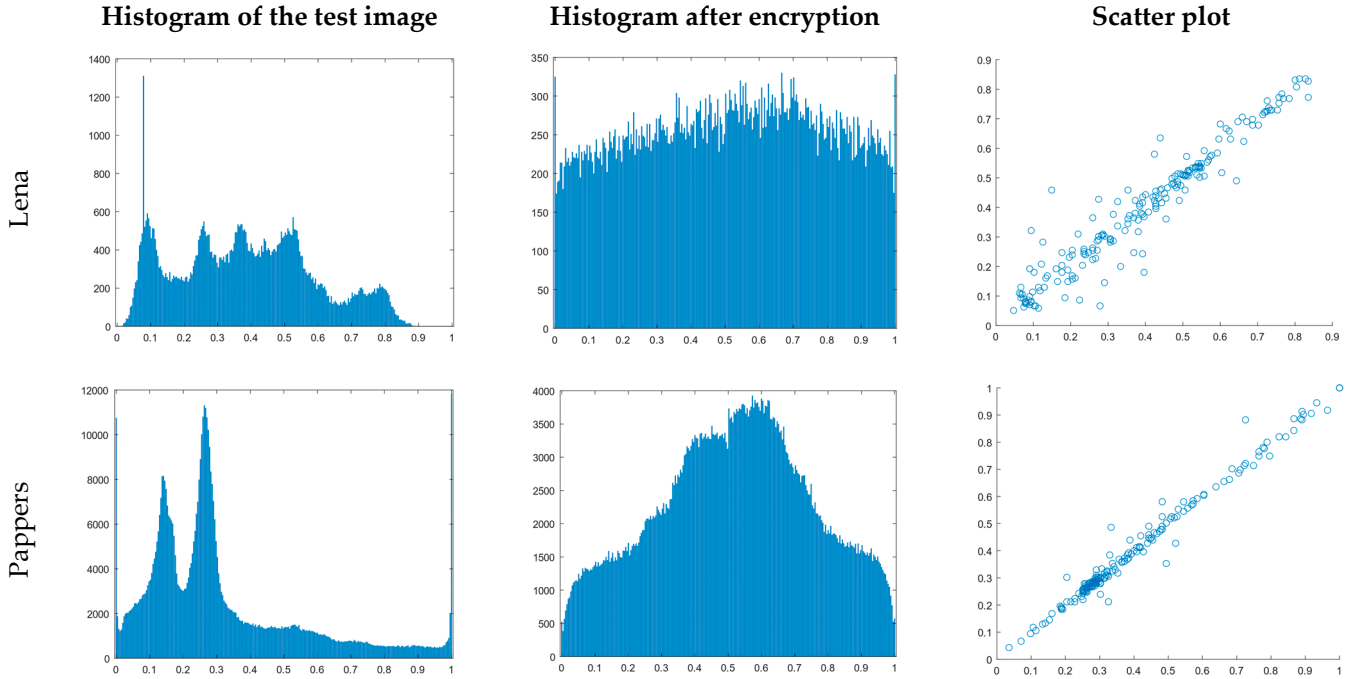
Table 2. Key initial value for diffusion and confusion operations.

x1(1)	x2(1)	μ 1	μ 2
0.5	0.5	4	3.9
x3(1)	y3(1)	μ 1	μ 2
0.3	0.3	4	3.9

Figure 3. The visual results for applying the proposed algorithm to some images. (**a**) Original images. (**b**) Encrypted images. (**c**) Reconstructed images.

4.1. Histogram Analysis

The first test is the histogram analysis of the encrypted, decrypted, and original images. Here, respective images' image histograms represent the vast differences between encrypted and original images, while they are the same. With the evaluation of the histogram of the test image and histogram after encryption, it is observed that the encrypted image is distributed uniformly in the entire interval of the histogram. Therefore, the original image's distribution regularity is covered. Hence, the encryption is implemented effectively (see Figure 4).



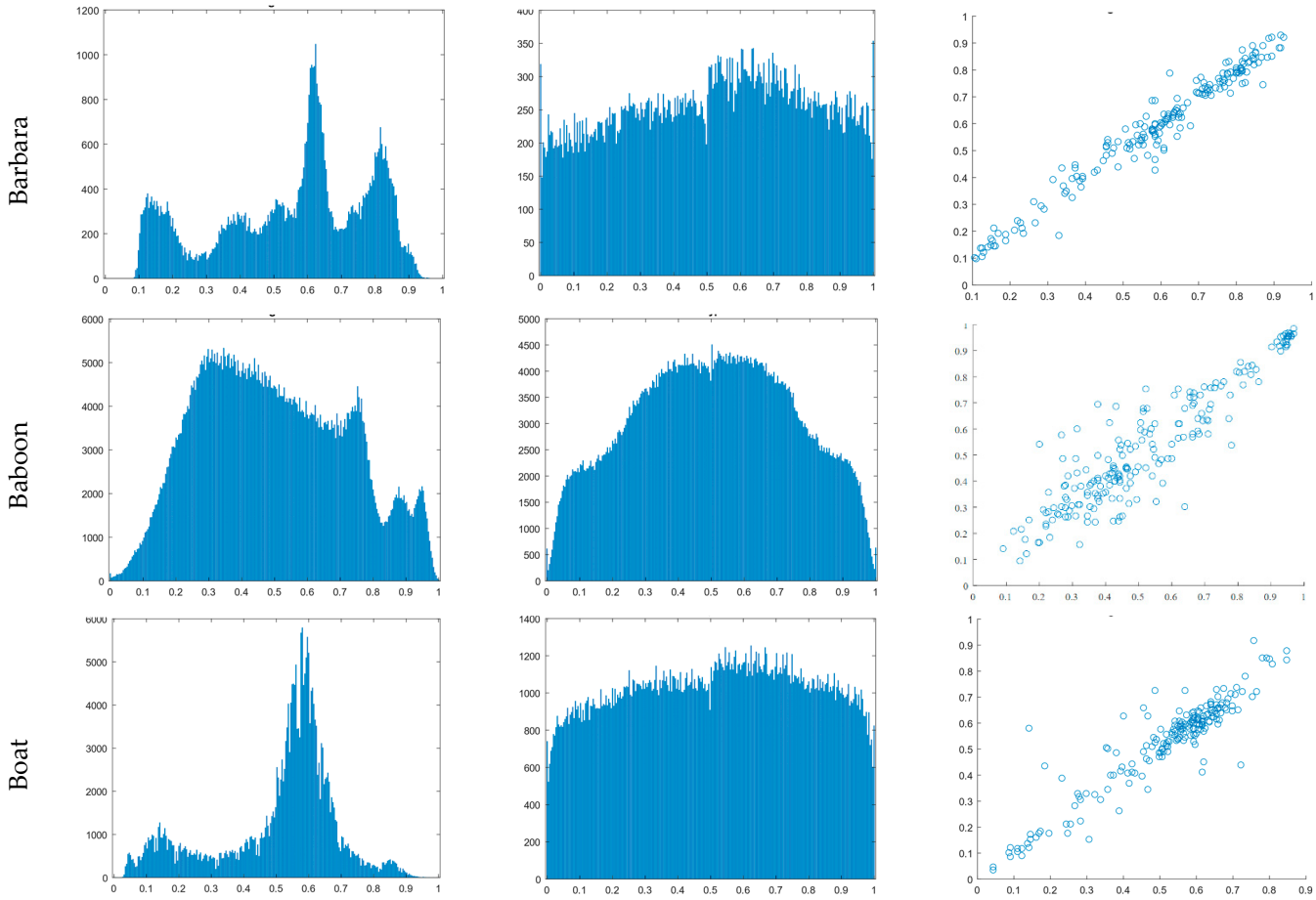


Figure 4. The histogram analysis for original Lena image.

4.2. Complexity

Using the proposed algorithm, by encrypting an image A of M × N, the algorithm using the chaotic map should produce an M × N number of random numbers R1. Hence, the complexity to produce M × N numbers of the random number is O (n). By increasing the time using the same chaotic map, the algorithm should produce a random chaos sequence of M × N bits. Hence, the complexity is repeated to produce M × N numbers of random bits as O (n). Afterward, it builds series (M × N) of chaos sequence additions or subtractions with a complexity of O (n). Lastly, it builds a chain XOR of operations as O (n). Thus, the algorithm's whole complexity is O (n).

4.3. Robustness

We evaluated the correlation between two vertically, two horizontally, and two diagonally adjacent pixels in the input image and encrypted image in addition to the histogram analysis in Figure 5. The values of two adjacent pixels in the image are represented by the x- and y-axes. In both the input and cipher images, Figure 5 depicts the correlation distribution of two horizontally adjacent pixels. Both the plain image and the cipher image have correlation coefficients of 0.99 and 0.02, respectively. The diagonal and vertical directions both yield similar results. The simple picture has a high correlation of two neighboring pixels.

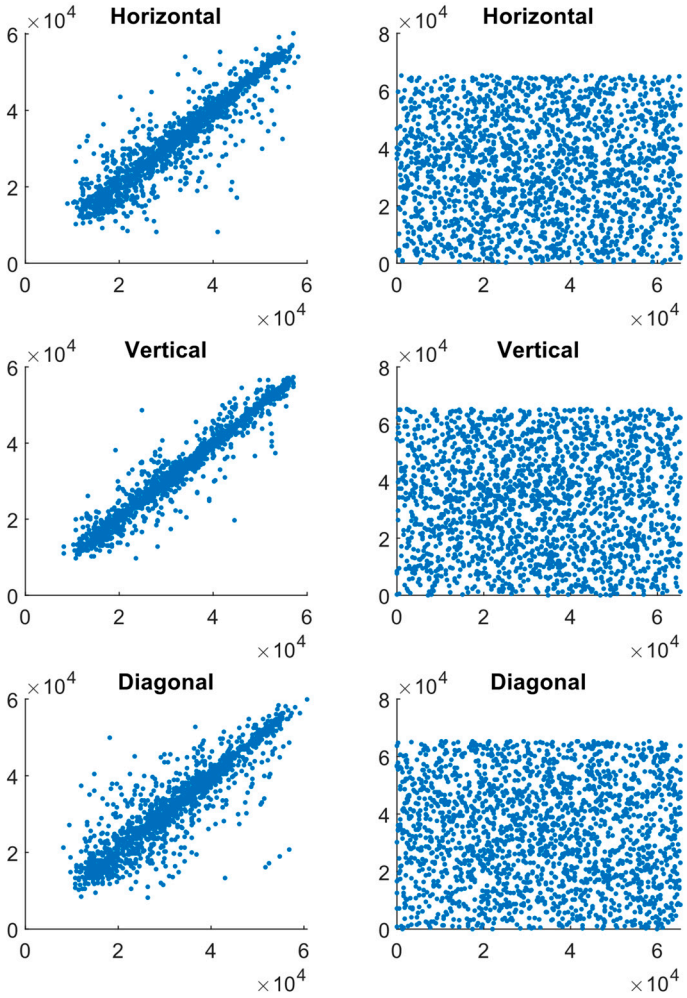


Figure 5. Plots of pixel horizontal, vertical and diagonal, correlation for input (**Left**) and encrypted images (**Right**) in Lena image.

To evaluate the proposed approach's robustness, the test images are tested against four types of image processing attacks: rotation, Gaussian noise, median filtration, and histogram equalization. The results show that the proposed design is associated with higher robustness and normalized correlation. Based on the results, input attack does not affect image encryption and decryption. Regarding the Normalized Correlation (NC) value for different types of images, median filter, rotation, and Gaussian noise have higher NC values. This means that the robustness of the presented method resists these types of attacks. However, the impact of histogram equalization is remarkable (see Table 3).

Table 3. The NC value of the proposed algorithm with different types of attack.

Image	Median Filter	Histogram Equalization	Rotation	Gaussian Noise
Lena Image	0.984	0.987	0.999	0.999
Peppers Image	0.704	0.280	0.923	0.964
Barbara Image	0.914	0.497	0.980	0.991
Baboon Image	0.960	0.629	0.991	0.996
Boat Image	0.976	0.746	0.995	0.998

5. Discussion

Here, a novel algorithm was presented for image encryption oriented by chaos. The provided algorithm in this paper has the following benefits in comparison with other

chaos-based algorithms. The chaotic sequence system structure is more complicated than the low-dimensional one, producing an integration of multivariate or univariate chaotic sequences [65]. This algorithm uses two one-dimensional chaotic systems. One-dimensional chaotic maps became an attractive field with the first detection of the Logistic Map in 1976. A very simple map by May [66] indicated that chaotic behavior could be exhibited using even a very simple nonlinear equation (a one-dimensional quadratic equation). Hence, our primary objective, as well as the ratio of taking this kind of map, is to discover a novel discrete time-series, the same as the logistic map exhibiting chaotic performance for unique parameters with elementary equations. The proposed method, in comparison with a low-dimensional chaotic sequence, is very secure for generating the chaotic sequence.

Moreover, compared to the high-dimensional chaotic sequence, this algorithm has a smaller calculation burden. The reason is that through the chaos model reconstruction, a low-dimensional chaotic sequence is simply attacked. Low-dimensional chaos was utilized for image encryption; however, its chaotic orbit was simple and might be simply predicted through the methods such as regression mapping, nonlinear prediction, and phase space reconstruction. Thus, the image encryption scheme utilizing low-dimensional chaos is simply exposed to the attacks [67]. However, the proposed method can transform the dynamic performance of the original chaotic system through dynamic comparison while completely resisting the model reconstruction attack, therefore developing its security. Compared to a high-dimensional chaotic sequence, the one-dimensional sequence has a lower amount of calculation. The reason is that the low-dimensional chaotic system is usually demonstrated with an algebraic equation, and it has a rapid solution. However, the high-dimensional chaotic system is a complex differential equation with relatively more considerable complexity and calculation burden. Utilizing the high-dimensional chaotic systems in some image encryption algorithms, the encryption procedure was straightforward. Moreover, the encryption algorithm was not sensitive to the secret keys and plain image alterations exposed to selective plaintext attacks or plaintext attacks [68]. By performing confusion encryption after diffusion encryption, we can develop the capability against the confusion encryption attack. Since the diffusion outcome becomes hidden by confusion encryption, the cipher is impractical through gathering the specific image. Classical encryption is commonly used just in the frequency-domain or air-domain. Our research, air-domain, and frequency-domain simultaneously perform encryption to improve the effects of encryption and enhance the encryption intensity.

Moreover, it is difficult to break in the frequency-domain or air-domain. Since the two-dimensional hyper-chaotic map is utilized in confusion encryption, there is a more considerable calculation burden for this algorithm. The findings obtained from the experimental values for the various standard images obtained by applying some existing methods, including our presented model, are shown in Table 4. These findings indicate that our approach is highly vulnerable to the alteration of the plain image bit, thereby making void differential attacks. In the presented model, input images consist of a 2D matrix of grayscale images. The main advantage of these types of images is to reduce both process time and storage volume. However, there are some disadvantages. Sometimes, the encryption should be implemented on a color image or video. In color pictures, video files, and voice files, encryption plays an important role. Therefore, the main limitation of this method is incompatibility with other types of files. For future hypotheses and research, we suggest extending the presented method and testing on other types of presentative files.

The suggested scheme's encrypted picture has a uniform histogram, a near-to-zero correlation coefficient, and entropy close to the full entropy. All of this shows that the scheme can withstand statistical attacks very well. The NPCR scores are appropriate for avoiding differential attacks, and the UACI scores are similar to the optimal result. Furthermore, the processing time for encryption and decryption is strictly proportional to the magnitude of the original image's correlation coefficient. A simple image with a lower

correlation coefficient takes less time to encrypt and decode, and vice versa. The proposed scheme has a broad chaotic regime for a wide variety of parameters, provides good security, and can withstand typical attacks, according to the dynamical analysis and assessment findings.

Table 4. The numerical results of the proposed algorithm in comparison with state-of-the-art methods.

References	Image	NPCR	UACI
Presented model	Lena Image	99.757	33.120
Presented model	Peppers Image	99.787	33.621
Presented model	Barbara Image	99.626	33.126
Presented model	Baboon Image	99.881	33.415
Presented model	Boat Image	99.625	33.671
Amina et al. [69]	Lena Image	99.646	33.625
Amina et al. [69]	Peppers Image	99.632	33.507
Amina et al. [69]	Baboon Image	99.602	33.629
Yavuz et al. [70]	Lena Image	99.620	33.410
Zhang and Zhao [71]	Lena Image	99.605	33.411
Assad and Farajallah [72]	Lena Image	99.607	33.463
Assad and Farajallah [72]	Boat Image	99.615	33.465
Kari et al. [38]	Lena Image	99.646	33.625
Kari et al. [38]	Peppers Image	99.713	33.541
Kari et al. [38]	Baboon Image	99.623	33.416
Kari et al. [38]	Boat Image	99.619	33.556

6. Conclusions

Recently, various chaos-based image cryptosystems have been presented. The present work deals with a chaotic-based algorithm using characteristics of the chaotic map and wavelet transform. The encryption process in this algorithm includes two stages. At first, we performed the image diffusion operation. Moreover, by performing the wavelet transform, the calculation amount in confusion was considerably reduced by hyper-chaotic sequences. The simulation results with the standard metrics show that the proposed algorithm has a high dependence on keys. This algorithm includes a decent encryption effect. Moreover, it can resist noise and cut attacks. We have tested the presented method for Lena, Peppers, Barbara, Baboon, and Boat Images from benchmark MATLAB test images. Moreover, the histograms of both input images and encrypted images are depicted. In addition, the encryption performance analysis criteria such as PSNR, NPCR, UACI and NC are recorded. Based on the results, the correlation value for Lena, Peppers, Barbara, Baboon, and Boat is 95.48%, 99.64%, 98.09%, 91.37% and 90.01%, respectively. To evaluate the proposed approach's robustness, the test images are tested against four types of image processing attacks: rotation, Gaussian noise, median filtration, and histogram equalization. The results show that the proposed design is associated with higher robustness and normalized correlation. Based on the results, input attack does not affect image encryption and decryption. Regarding the NC value for different types of images, median filter, rotation, and Gaussian noise have higher NC values. It means that the robustness of the presented method resists these types of attacks. However, the impact of histogram equalization is remarkable. For future work, we suggested implementing the presented method for other types of files such as voice, video, and color 3D images.

Author Contributions: Y.P.; Conceptualization, methodology, validation, formal analysis, R.R.; Investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, A.M.; supervision, project administration, funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: In this study we used MATLAB benchmark images for academic studies. Available in MATLAB software samples.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hamzenejad, A.; Ghoushchi, S.J.; Baradaran, V.; Mardani, A. A Robust Algorithm for Classification and Diagnosis of Brain Disease Using Local Linear Approximation and Generalized Autoregressive Conditional Heteroscedasticity Model. *Mathematics* **2020**, *8*, 1268, doi:10.3390/math8081268.
2. Filelis-Papadopoulos, C.K.; Endo, P.T.; Bendechache, M.; Svorobej, S.; Giannoutakis, K.M.; Gravvanis, G.A.; Tzovaras, D.; Byrne, J.; Lynn, T. Towards simulation and optimization of cache placement on large virtual content distribution networks. *J. Comput. Sci.* **2020**, *39*, 101052, doi:10.1016/j.jocs.2019.101052.
3. Bendechache, M.; Kechadi, M.T. Distributed clustering algorithm for spatial data mining. In Proceedings of the 2015 2nd IEEE International Conference on Spatial Data Mining and Geographical Knowledge Services (ICSDM), Fuzhou, China, 8–10 July 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 60–65, doi:10.1109/ICSDM.2015.7298026.
4. Bendechache, M.; Svorobej, S.; Endo, P.T.; Lynn, T. Simulating Resource Management across the Cloud-to-Thing Continuum: A Survey and Future Directions. *Future Internet* **2020**, *12*, 95, doi:10.3390/fi12060095.
5. Saračević, M.H.; Adamović, S.Z.; Miškovic, V.A.; Elhoseny, M.; Maček, N.D.; Selim, M.M.; Shankar, K. *Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures*; IEEE Transactions on Reliability: Piscataway, NJ, USA, 2020.
6. Saračević, M.; Adamović, S.; Miškovic, V.; Maček, N.; Šarac, M. A novel approach to steganography based on the properties of Catalan numbers and Dyck words. *Future Gener. Comput. Syst.* **2019**, *100*, 186–197.
7. Jafarzadeh, S.G.; Rahman, M.N.A.; Wahab, D.A. Optimization of supply chain management based on response surface methodology: A case study of iran khodro. *World Appl. Sci. J.* **2012**, *20*, 620–627.
8. Jafarzadeh-Ghoushchi, S. Qualitative and quantitative analysis of Green Supply Chain Management (GSCM) literature from 2000 to 2015. *Int. J. Supply Chain Manag.* **2018**, *7*, 77–86.
9. Jafarzadeh Ghoushchi, S.; Khazaeili, M.; Amini, A.; Osgooei, E. Multi-criteria sustainable supplier selection using piecewise linear value function and fuzzy best-worst method. *J. Intell. Fuzzy Syst*. **2019**, *37*, 2309–2325.
10. Dorosti, S.; Ghoushchi, S.J.; Sobhrakhshankhah, E.; Ahmadi, M.; Sharifi, A. Application of gene expression programming and sensitivity analyses in analyzing effective parameters in gastric cancer tumor size and location. *Soft Comput.* **2020**, *24*, 9943–9964, doi:10.1007/s00500-019-04507-0.
11. Ramalingam, B.; Ravichandran, D.; Annadurai, A.A.; Rengarajan, A.; Rayappan, J.B.B. Chaos triggered image encryption—A reconfigurable security solution. *Multimed. Tools Appl.* **2017**, *77*, 11669–11692, doi:10.1007/s11042-017-4811-x.
12. Svorobej, S.; Endo, P.T.; Bendechache, M.; Filelis-Papadopoulos, C.; Giannoutakis, K.M.; Gravvanis, G.A.; Tzovaras, D.; Byrne, J.; Lynn, T. Simulating Fog and Edge Computing Scenarios: An Overview and Research Challenges. *Future Internet* **2019**, *11*, 55, doi:10.3390/fi11030055.
13. Bendechache, M.; Kechadi, M.-T.; Le-Khac, N.-A. Efficient Large Scale Clustering Based on Data Partitioning. In Proceedings of the 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), Montreal, QC, Canada, 17–19 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 612–621.
14. Khan, J.S.; Ahmad, J. Chaos based efficient selective image encryption. *Multidimens. Syst. Signal Process.* **2019**, *30*, 943–961, doi:10.1007/s11045-018-0589-x.
15. Wang, Y.; Wong, K.-W.; Liao, X.; Chen, G. A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* **2011**, *11*, 514–522, doi:10.1016/j.asoc.2009.12.011.
16. Patidar, V.; Pareek, N.; Purohit, G.; Sud, K. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Opt. Commun.* **2011**, *284*, 4331–4339, doi:10.1016/j.optcom.2011.05.028.
17. Wang, X.; Liu, L.; Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt. Lasers Eng.* **2015**, *66*, 10–18, doi:10.1016/j.optlaseng.2014.08.005.
18. Volos, C.; Kyprianidis, I.; Stouboulos, I. Image encryption process based on chaotic synchronization phenomena. *Signal Process.* **2013**, *93*, 1328–1340, doi:10.1016/j.sigpro.2012.11.008.
19. Xu, Y.; Wang, H.; Li, Y.; Pei, B. Image encryption based on synchronization of fractional chaotic systems. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 3735–3744, doi:10.1016/j.cnsns.2014.02.029.
20. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt. Lasers Eng.* **2014**, *56*, 83–93, doi:10.1016/j.optlaseng.2013.12.003.
21. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25, doi:10.1016/j.optlaseng.2015.09.007.
22. Kaur, M.; Kumar, V. Beta Chaotic Map Based Image Encryption Using Genetic Algorithm. *Int. J. Bifurc. Chaos* **2018**, *28*, doi:10.1142/s0218127418501328.

23. Nematzadeh, H.; Enayatifar, R.; Motameni, H.; Guimarães, F.G.; Coelho, V.N. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Opt. Lasers Eng.* **2018**, *110*, 24–32, doi:10.1016/j.optlaseng.2018.05.009.
24. Javidi, M., Hosseinpourfard, R. Chaos Genetic Algorithm Instead Genetic Algorithm. *Int. Arab, J. Inf. Technol.* **2015**, *12*, 2.
25. Zhen, P.; Zhao, G.; Min, L.; Jin, X. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimed. Tools Appl.* **2016**, *75*, 6303–6319, doi:10.1007/s11042-015-2573-x.
26. Wang, X.; Zhang, H.-L. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. *Nonlinear Dyn.* **2016**, *83*, 333–346, doi:10.1007/s11071-015-2330-8.
27. Li, C.-L.; Li, H.-M.; Li, F.-D.; Wei, D.-Q.; Yang, X.-B.; Zhang, J. Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik* **2018**, *171*, 277–286, doi:10.1016/j.ijleo.2018.06.029.
28. Satish, T.J.; Theja, M.N.S.; Kumar, G.G.; Thanikaiselvan, V. Image Encryption Using Integer Wavelet Transform, Logistic Map and XOR Encryption. In Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 704–709.
29. Kanso, A.; Ghebleh, M. An algorithm for encryption of secret images into meaningful images. *Opt. Lasers Eng.* **2017**, *90*, 196–208, doi:10.1016/j.optlaseng.2016.10.009.
30. Ravichandran, D.; Murthy, B.K.; Balasubramanian, V.; Fathima, S.; Amirtharajan, R. An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Med. Biol. Eng. Comput.* **2021**, *59*, 589–605, doi:10.1007/s11517-021-02328-8.
31. Kovalchuk, A.; Izonin, I.; Kustra, N. Information Protection Service using Topological Image Coverage. *Procedia Comput. Sci.* **2019**, *160*, 503–508, doi:10.1016/j.procs.2019.11.057.
32. Kovalchuk, A.; Lotoshynska, N.; Izonin, I.; Berezko, L. An Approach towards an Efficient Encryption-Decryption of Grayscale and Color Images. *Procedia Comput. Sci.* **2019**, *155*, 630–635, doi:10.1016/j.procs.2019.08.089.
33. Kovalchuk, A.; Izonin, I.; Lotoshynska, N. An Approach Towards Image Encryption and Decryption using Quaternary Fractional-Linear Operations. *Procedia Comput. Sci.* **2019**, *160*, 491–496.
34. Kovalchuk, A.; Izonin, I.; Strauss, C.; Podavalkina, M.; Lotoshynska, N.; Kustra, N. Image Encryption and Decryption Schemes Using Linear and Quadratic Fractal Algorithms and Their Systems. In *DCSMart*; Researchgate: Berlin, Germany, 2019; pp. 139–150.
35. Kovalchuk, A.; Izonin, I.; Riznyk, O. An Efficient Image Encryption Scheme using Projective Transformations. *Procedia Comput. Sci.* **2019**, *160*, 584–589, doi:10.1016/j.procs.2019.11.043.
36. Kovalchuk, A.; Lotoshynska, N. Elements of RSA Algorithm and Extra Noising in a Binary Linear-Quadratic Transformations During Encryption and Decryption of Images. In Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 21–25 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 542–544.
37. Hafsa, A.; Gafsi, M.; Malek, J.; Machhout, M. FPGA Implementation of Improved Security Approach for Medical Image Encryption and Decryption. *Sci. Program.* **2021**, *2021*, 6610655.
38. Kari, A.P.; Navin, A.H.; Bidgoli, A.M.; Mirnia, M. A new image encryption scheme based on hybrid chaotic maps. *Multimed. Tools Appl*. **2021**, *80*, 2753–2772, doi:10.1007/s11042-020-09648-1.
39. Shaukat, S.; Arshid, A.L.; Eleyan, A.; Shah, S.A.; Ahmad, J. Chaos theory and its application: An essential framework for image encryption. *Chaos Theory Appl.* **2020**, *2*, 17–22.
40. Guo, J. Basic theories and applications of digital image processing. In Proceedings of the 2017 2nd International Conference on Mechatronics and Information Technology, Dalian, China, 13–14 May 2017; Francis Academic Press Ltd.: London, UK, 2017.
41. Bendechache, M. Study of Distributed Dynamic Clustering Framework for Spatial Data Mining. Available online: http://oatd.org/oatd/record?record=handle%5C%3A10197%5C%2F10614 (accessed on 17 December 2020).
42. Gad, M.; Hagras, E.; Soliman, H.; Hikal, N. A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption. *Int. Arab J. Inf. Technol.* **2021**, *18*, 227–236.
43. Yang, J.; Gao, J.S.; Sun, B.Y. An improved approach of logistic chaotic series encryption. *Tech. Autom. Appl.* **2004**, *23*, 58–61.
44. Hao, Z.; Xing-Yuan, W.; Si-Wei, W.; Kang, G.; Xiao-Hui, L. Application of coupled map lattice with parameter q in image encryption. *Opt. Lasers Eng.* **2017**, *88*, 65–74, doi:10.1016/j.optlaseng.2016.07.004.
45. Pisarchik, A.; Zanin, M. Image encryption with chaotically coupled chaotic maps. *Phys. D Nonlinear Phenom.* **2008**, *237*, 2638–2648, doi:10.1016/j.physd.2008.03.049.
46. Lu, G.; Smidtaite, R.; Navickas, Z.; Ragulskis, M. The Effect of Explosive Divergence in a Coupled Map Lattice of Matrices. *Chaos Solitons Fractals* **2018**, *113*, 308–313, doi:10.1016/j.chaos.2018.06.016.
47. Rai, H.M.; Chatterjee, K. Hybrid adaptive algorithm based on wavelet transform and independent component analysis for denoising of MRI images. *Measurement* **2019**, *144*, 72–82, doi:10.1016/j.measurement.2019.05.028.
48. Eftekhari, H.R.; Ghatee, M. Hybrid of discrete wavelet transform and adaptive neuro fuzzy inference system for overall driving behavior recognition. *Transp. Res. Part F Traffic Psychol. Behav.* **2018**, *58*, 782–796, doi:10.1016/j.trf.2018.06.044.
49. Wu, F.; Hao, Y.; Zhao, J.; Liu, Y. Current similarity based open-circuit fault diagnosis for induction motor drives with discrete wavelet transform. *Microelectron. Reliab.* **2017**, *75*, 309–316, doi:10.1016/j.microrel.2017.05.036.
50. Ranjbarzadeh, R.; Saadi, S.B. Automated liver and tumor segmentation based on concave and convex points using fuzzy c-means and mean shift clustering. *Measurement* **2020**, *150*, 107086, doi:10.1016/j.measurement.2019.107086.
51. Mokhtari, Z.; Melkemi, K. A New Watermarking Algorithm Based on Entropy Concept. *Acta Appl. Math.* **2011**, *116*, 65–69, doi:10.1007/s10440-011-9629-3.

52. Ali, W.A.; Aljunid, M.; Bendechache, M.; Sandhya, P. Review of Current Machine Learning Approaches for Anomaly Detection in Network Traffic. *J. Telecommun. Digit. Econ.* **2020**, *8*, 64–95, doi:10.18080/jtde.v8n4.307.
53. Karimi, N.; Kondrood, R.R.; Alizadeh, T. An intelligent system for quality measurement of Golden Bleached raisins using two comparative machine learning algorithms. *Measurement* **2017**, *107*, 68–76, doi:10.1016/j.measurement.2017.05.009.
54. Yan, X.; Wang, S.; Li, L.; El-Latif, A.A.A.; Wei, Z.; Niu, X. A New Assessment Measure of Shadow Image Quality Based on Error Diffusion Techniques. *J. Inf. Hiding Multimed. Signal Process.* **2013**, *4*, 118–126.
55. Fu, C.; Chen, J.-J.; Zou, H.; Meng, W.-H.; Zhan, Y.-F.; Yu, Y.-W. A chaos-based digital image encryption scheme with an improved diffusion strategy. *Opt. Express* **2012**, *20*, 2363–2378, doi:10.1364/oe.20.002363.
56. Mera, C.; Orozco-Alzate, M.; Branch, J.; Mery, D. Automatic visual inspection: An approach with multi-instance learning. *Comput. Ind.* **2016**, *83*, 46–54, doi:10.1016/j.compind.2016.09.002.
57. Ranjbarzadeh, R.; Saadi, S.B.; Amirabadi, A. LNPSS: SAR image despeckling based on local and non-local features using patch shape selection and edges linking. *Measurement* **2020**, *164*, 107989, doi:10.1016/j.measurement.2020.107989.
58. Ahmadi, M.; Jafarzadeh-Ghoushchi, S.; Taghizadeh, R.; Sharifi, A. Presentation of a new hybrid approach for forecasting economic growth using artificial intelligence approaches. *Neural Comput. Appl.* **2019**, *31*, 8661–8680, doi:10.1007/s00521-019-04417-0.
59. Chen, C.-Y.; Chen, C.-H.; Lin, K.-P. An automatic filtering convergence method for iterative impulse noise filters based on PSNR checking and filtered pixels detection. *Expert Syst. Appl.* **2016**, *63*, 198–207, doi:10.1016/j.eswa.2016.07.003.
60. Orozco, E.R.; Guerrero, E.E.G.; González, E.I.; Bonilla, O.R.L. Image Encryption Based on Improved Rosslerö Hyper chaotic Map. 2015. Available online: https://pdfs.semanticscholar.org/8e23/a3dc5c12d5d52c8f76084906ac68cc7b40b5.pdf (accessed on 30 March 2015).
61. Zhou, N.; Wang, Y.; Gong, L.; He, H.; Wu, J. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. *Opt. Commun.* **2011**, *284*, 2789–2796, doi:10.1016/j.optcom.2011.02.066.
62. Salem, S.; Jafarzadeh-Ghoushchi, S. Estimation of optimal physico-chemical characteristics of nano-sized inorganic blue pigment by combined artificial neural network and response surface methodology. *Chemom. Intell. Lab. Syst.* **2016**, *159*, 80–88, doi:10.1016/j.chemolab.2016.10.006.
63. Ranjbarzadeh, R.; Baseri Saadi, S. Corrigendum to 'Automated liver and tumor segmentation based on concave and convex points using fuzzy c-means and mean shift clustering' [Measurement 150 (2020) 107086]. *Meas. J. Int. Meas. Confed.* **2020**, *151*, 107230, doi:10.1016/j.measurement.2019.107230.
64. Blaber, J.; Adair, B.S.; Antoniou, A. Ncorr: Open-Source 2D Digital Image Correlation Matlab Software. *Exp. Mech.* **2015**, *55*, 1105–1122, doi:10.1007/s11340-015-0009-1.
65. Niu, Y.; Zhang, X.; Han, F. Image Encryption Algorithm Based on Hyperchaotic Maps and Nucleotide Sequences Database. *Comput. Intell. Neurosci.* **2017**, *2017*, 1–9, doi:10.1155/2017/4079793.
66. May, R.M. Simple mathematical models with very complicated dynamics. In *The Theory of Chaotic Attractors*; Springer: New York, NY, USA, 2004; pp. 85–93.
67. Solak, E.; Çokal, C.; Yildiz, O.T.; Biyikoğlu, T. Cryptanalysis of fridrich's chaotic image encryption. *Int. J. Bifurc. Chaos* **2010**, *20*, 1405–1413, doi:10.1142/s0218127410026563.
68. Rhouma, R.; Solak, E.; Belghith, S. Cryptanalysis of a new substitution–diffusion based image cipher. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 1887–1892, doi:10.1016/j.cnsns.2009.07.007.
69. Amina, S.; Mohamed, F.K. An efficient and secure chaotic cipher algorithm for image content preservation. *Commun. Nonlinear Sci. Numer. Simul.* **2018**, *60*, 12–32, doi:10.1016/j.cnsns.2017.12.017.
70. Yavuz, E.; Yazıcı, R.; Kasapbaşı, M.C.; Yamaç, E. A chaos-based image encryption algorithm with simple logical functions. *Comput. Electr. Eng.* **2016**, *54*, 471–483.
71. Zhang, X.; Zhao, Z. Chaos-based image encryption with total shuffling and bidirectional diffusion. *Nonlinear Dyn.* **2013**, *75*, 319–330, doi:10.1007/s11071-013-1068-4.
72. El Assad, S.; Farajallah, M. A new chaos-based image encryption system. *Signal Process. Image Commun.* **2016**, *41*, 144–157.