computation

MDPI

Article

Secure Medical Image Transmission Scheme Using Lorenz's Attractor Applied in Computer Aided Diagnosis for the Detection of Eye Melanoma

Daniel Fernando Santos and Helbert Eduardo Espitia *

Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá 110231, Colombia
* Correspondence: heespitiac@udistrital.edu.co

Abstract: Early detection of diseases is vital for patient recovery. This article explains the design and technical matters of a computer-supported diagnostic system for eye melanoma detection implementing a security approach using chaotic-based encryption to guarantee communication security. The system is intended to provide a diagnosis; it can be applied in a cooperative environment for hospitals or telemedicine and can be extended to detect other types of eye diseases. The introduced method has been tested to assess the secret key, sensitivity, histogram, correlation, Number of Pixel Change Rate (NPCR), Unified Averaged Changed Intensity (UACI), and information entropy analysis. The main contribution is to offer a proposal for a diagnostic aid system for uveal melanoma. Considering the average values for 145 processed images, the results show that near-maximum NPCR values of 0.996 are obtained along with near-safe UACI values of 0.296 and high entropy of 7.954 for the ciphered images. The presented design demonstrates an encryption technique based on chaotic attractors for image transfer through the network. In this article, important theoretical considerations for implementing this system are provided, the requirements and architecture of the system are explained, and the stages in which the diagnosis is carries out are described. Finally, the encryption process is explained and the results and conclusions are presented.

Keywords: chaotic attractors; computer vision; disease diagnosis; encryption; computer-assisted diagnosis; convolutional neural networks

Citation: Santos, D.F.; Espitia, H.E. Secure Medical Image Transmission Scheme Using Lorenz's Attractor Applied in Computer Aided Diagnosis for the Detection of Eye Melanoma. *Computation* **2022**, *10*, 158. https://doi.org/10.3390/computation10090158

Academic Editor: Demos T. Tsahalis

Received: 26 July 2022
Accepted: 11 September 2022
Published: 14 September 2022

1. Introduction

Computer assistance in providing disease diagnoses has a broad range of applications, and the development of tools that help to reach this end is of paramount significance. Computer-Assisted Diagnosis (CAD) has been applied in many different contexts, including Digital Imaging and Communications in Medicine (DICOM); in this regard, a web application for disease diagnosis through a browser is shown in [1]. Other examples of medical images transmission can be found in [2,3]. In [4], the authors evaluated a fuzzy clustering algorithm for breast cancer detection, while [5] illustrates developments in the detection of diabetic retinopathy involving computer-aided diagnostic systems.

In Colombia, as well as in other parts of the world, access to an ophthalmologist entails several appointments and procedures, which usually lead to long waits. For this reason, it is essential to create tools to aid in timely diagnosis in order to provide adequate treatment. In [6], the authors proposed a telemedicine system to diagnose stomach diseases. Issues with developing computer-aided diagnosis systems (CADS) have been studied in [7], where the authors explained a new model along with several fundamental CADS techniques. Cloud Computing (CC), TensorFlow (TF), and Django are used as support for the construction of such systems. CC supports the storage and access of information of interest for different parties, while TF (created by Google under an open-source Apache 2.0 license [8]) provides an interface for building and running machine learning algorithms to use and run eye disease prediction models.

Regarding computer-assisted diagnosis, reference [9] presents a diagnostic system for schizophrenia using effective connectivity of resting-state electroencephalogram (EEG) data, while [10] studies the practicality of deep learning algorithms applied to chest X-ray images for COVID-19 detection. In [11], the authors presented a COVID-19 prediction applying supervised machine learning algorithms using the Waikato Environment for Knowledge Analysis (WEKA), which is an open-source software developed at the University of Waikato in New Zealand. Lastly, reference [12] proposed a system for detection of cancer cells using commercially automated microscope-based screeners. Employing supervised machine learning, the authors developed software capable of classifying Feulgen-stained nuclei within eight diagnostically important types.

Regarding eye image processing (classification), in [13], the authors described the implementation of a framework for healthy and diabetic retinopathy retinal image recognition. In [14], the authors presented a framework for eye tracking calibration where features extracted from the synthetic eyes dataset are used in a fully connected network to isolate the effect of a specific user's features. Their work was oriented towards the design of low-cost eye-tracking systems. In [15], the authors performed an Image Quality Assessment (IQA) of eye fundus images in the context of digital fundoscopy with Topological Data Analysis (TDA) and machine learning methods. IQA is a fundamental step in digital fundoscopy for clinical applications, and is considered one of the first steps in the preprocessing stages of Computer-Aided Diagnosis (CAD) systems using eye fundus images. Their research employed cubical complexes to represent the images; the grayscale version was then used to calculate a homology illustrated with persistence diagrams and thirty vectorized topological descriptors were calculated from each image for use as input to a classification algorithm. Finally, Diabetic Retinopathy (DR) is a disease that is one of the main causes of blindness around the world. Therefore, reference [16] employed retinal fundus images as diagnostic tools to screen abnormalities associated with eye diseases. In this regard, article [16] proposed an algorithm to segment and detect hemorrhages in retinal fundus images. The method they described performs preprocessing on retinal fundus images by utilizing a windowing-based adaptive threshold to segment hemorrhages. In this way, conventional features are extracted for each candidate and classified using a support vector machine.

In regards to research related to image encryption based on chaos, developed approaches include specially fractional-order chaotic systems, which exhibit more complex dynamics than integer-order chaotic systems. In [17], a fractional-order memristor was developed, analyzed, and electronically implemented. In this order, a three-dimensional (3D) fractional-order memristive chaotic system with a single unstable equilibrium point was proposed for use in an encryption system applied to grayscale images. Other related research was presented in [18], where the authors proposed using a chaotic oscillator without linear terms as a random number generator for application in biomedical image encryption. They demonstrated the physical realization of the oscillator and carried out a security and performance analysis. In [19], an oscillator with chaotic dynamics was presented and various properties of the oscillator, such as bifurcations, equilibria, and Lyapunov exponents, were studied in order to show the existence of chaotic dynamics (as the oscillator has a chaotic attractor). Using the features of the chaotic oscillator, a method for generating pseudo-random numbers was presented in the context of designing secure substitution boxes applied to an image cryptosystem. In this same orientation, in [20] the authors developed, analyzed, tested, and electronically implemented a 4D fractional-order memcapacitor that observed the nonlinear dynamic properties of a hyperchaotic system. On this basis, they proposed an encryption algorithm for color encryption based on the system's chaotic behavior in which every pixel value of the original image is incorporated into the secret key to strengthen the encryption algorithm. A related work was presented in [21] involving a hyperchaotic 4D fractional discrete Hopfield neural network system. The chaotic dynamics features were analyzed and the chaotic system was used as a pseudo-random number generator for an image encryption scheme based on a fractal-like model

scrambling method. This approach was able to enhance the complexity and security of the encryption algorithm. Finally, in [22], a chaotic oscillator was presented in which the chaotic dynamics were pre-located around manifolds. After analyzing the complex dynamics of the oscillator, this approach was employed in the design of an image cryptosystem, and the results of the cryptosystem were tested while considering different metrics.

The present study proposes a system for computer-aided diagnosis, detection, and classification of eye diseases using chaotic-based encryption for image transmission. The proposal is based on the previous works in [23,24] for image encryption and [25,26] for image diagnostics.

Regarding differences with other related works, references [9–12] display various applications in computer-assisted diagnosis that are not applicable to eye image diagnosis; while [13–16] are focused specifically on eye image processing and classification. Regarding image encryption methods based on chaotic attractors, references [17–22] each describe several different developments, while [18] considers the encryption of medical images and [22] is concerned with Internet of Things (IoT) applications for remote diagnosis. The novelty of the present work is in its integration of an identification system for Uveal melanoma with an encryption mechanism in order to obtain a computer-assisted diagnosis system that can help professionals in improving the diagnostic process. As such, a computer-aided diagnosis system is presented here that integrates an image processing (classification) system based on a convolutional neural network and a mechanism for image transmission using an encryption method based on a chaotic attractor.

The rest of this paper is constructed as follows. Section 2 displays the design of the proposed system. Section 3 specifies the encryption framework and reviews the chaotic Lorenz attractor and its relevant properties for encryption. Section 4 presents the implementation results for the encryption system. Finally, Sections 5 and 6 respectively present the discussion and conclusions.

2. Proposed Diagnosis and Encryption System

This section presents the system architecture and the process used to diagnose the graphic user interface, then explains the system operation employing Convolutional Neural Network (CNN).

The structure of the application is similar to the one proposed in [27] divided into three layers: presentation, domain logic, and data access. The presentation layer comprises the patient and doctor user interfaces and all actions that a user can carry out. The domain logic contains the business module and the process of transferring and ciphering images over the network; this frame uses the data access layer, which stores the data the systems need to operate. Figure 1 shows a graphic of the doctor user interface (presentation layer), providing an example of a result after diagnosis. The specialist interface provides a diagnostic from all the eye images received. Contiguous to each eye, there is a textbox where the specialist can formulate the diagnostic; additionally, it offers options to run the automatic CNN diagnostic model. A button to send the diagnostic is provided. When clicking on the image of the eye, the specialist performs the operations described in Table 1. This interface has a responsive design, allowing it to be used from a smartphone.

The system allows different operations to be executed on the eye; these are shown in Table 1. These operations are aimed at modifying eye the image according to user needs, for instance, zooming in on a particular region or removing noise.

Figure 1. Specialist's interface with different diagnostic options.

Table 1. Operations that the specialist carries out on the images. These operations allow the doctor to perform a more reliable diagnostic.

Operation	Description
Grayscale transformation	Conversion of the $I[x, y, z]$ color image to grayscale $O_1[x, y]$ to reduce noise and improve the performance of the following stages. The conversion of a color image to a grayscale image consists of converting RGB values (24 bits) to grayscale values (8 bits).
Apply median filter	This process is performed to apply smoothing, which is achieved by sliding a window over the image, thus suppressing the higher frequencies. It can be seen as a change of the brightness of the input image.
Apply thresholding	For the present project, this utilizes mean adaptive thresholding and Gaussian adaptive thresholding to clearly define the borders. The main objective of this step is to provide better definition of the edges.
Dilate the image	By applying a morphological operation to reduce noise, dilation allows objects to be expanded, thus potentially filling small holes, in this case reducing pepper noise.
Rotation	The image is rotated at a predefined or random angle. In the case of the iris, 360 different rotations can be performed.
Zooming	This technique creates new versions of an image with different zoom views, in many cases focusing on the region of interest. The resulting images are enlarged or reduced according to a predefined range.

The user takes a picture of the eye and sends it using the application; this image is saved in the server through a request, then the specialist receives this photo and writes a diagnosis. This process can be seen in Figure 2. Before transmitting over the network, images are ciphered using chaotic encryption to maintain privacy. The Diffie–Hellman

algorithm shares the initialization conditions for ciphering and deciphering the server and the client.

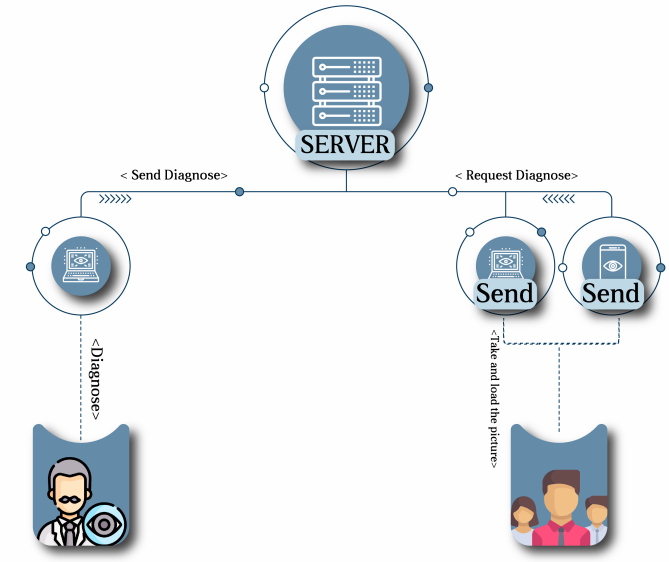


Figure 2. Model explaining communication between the patient and specialist. The patient can send images through their cellphone or computer.

Diagnostic Using Deep Convolutional Neural Network

For implementing the layer corresponding to the diagnostic, preliminary tests were conducted recognizing fuzzy systems neural networks and neuro-fuzzy systems as shown in [25,26]. However, better results are attained utilizing convolutional neural networks. Thus, the diagnostic system employs a famous pre-trained model, Resnet18, which recognizes abnormalities with an accuracy of 99%. Figure 3 presents the Resnet18 architecture.

In order to train the CNN, a data augmentation process was employed obtaining a dataset of 2048 figures, consisting of 1024 healthy and 1024 unhealthy. The original database is taken from [28], consisting of images of 150 healthy and 33 unhealthy patients. Additional details related to the design and training of the CNN can be found in [29].

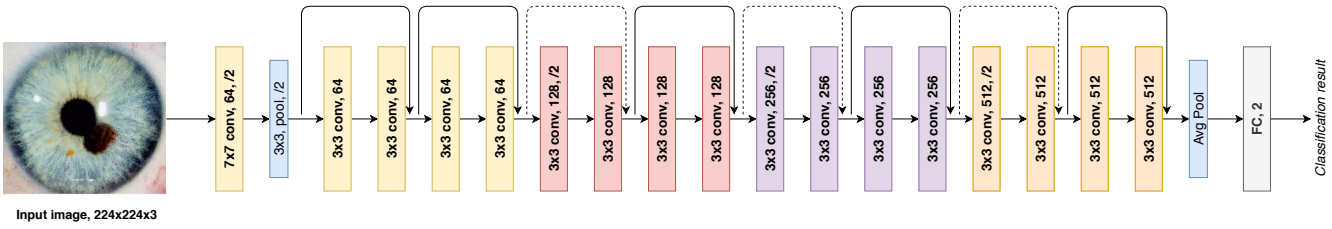


Figure 3. Resnet18 architecture.

The model trained with the Resnet18 architecture receives an image (iris image) and produces a value corresponding to the classification; in addition, there is a second model that produces a bounding box with the location of the detected abnormality. The model is used when the specialist clicks the "Use AI to Diagnose" button. In [29], different convolutional neural networks (CNNs) were used to detect ocular abnormalities with an illustrative case of uveal melanoma (UM), a type of ocular cancer. Thus, this work is a complement to that research, seeking to implement a CAD.

Resnet is a well-known convolutional neural network architecture that allows the training of hundreds or thousands of layers and achieves excellent performance. The biggest advantage of Resnet is its ability to reduce the vanishing gradient problem [30]. Before Resnet, a deep network was hard to train, as the gradients need to back-propagate

through an enormous number of layers in a deep network, which makes the gradient infinitely small. Resnet has solved this problem, as it can skip the backwards connections between layers and create identity shortcuts in the gradients' path, that allows the gradients to flow faster to the initial layer [31].

The model was trained with a cross-entropy loss function to minimize the distance between predicted and ground-truth probabilities. This is defined in Equation (1), where p_i and q_i are the ground-truth and predicted probability, respectively. The loss function was minimized utilizing the Adam optimization algorithm, as it is computationally efficient and works well with noisy or sparse gradient problems.

$$L = -\sum_{i=1}^{N} p_i \log(q_i) \tag{1}$$

3. Security Techniques

This section reviews the chaotic Lorenz attractor and its relevant properties for encryption, and describes notable security techniques.

Privacy is essential for systems that hold patient information, and is indispensable in speeding up the diagnostic process. Various techniques have been introduced, including data encryption standard (DES), Rivest–Shamir–Adleman (RSA), and chaos, among others. Chaos provides high sensitivity to initial conditions and unpredictability. For instance, reference [32] used chaotic Arnold Maps (AM) to randomize the original position of the pixels, causing the image to become noisy. In [33,34], the authors proposed a system for encrypting color using the advantage of chaotic maps. The idea behind these maps is to distribute the pixels with a transformation such that the correlation of adjacent pixels can be reduced. Using compression and security features, this scheme can be applied in public networks. In [35], a feasible system for image encryption was presented using techniques applicable for real-time image transmission and encryption. However, applications in medical image transfer are relatively scarce; one of the few that has been found is the use of Arnold maps for the diffusion stage in a system that allows the encoding of pixels of biometric data [36]. This system uses a chaotic Chen system to change the statistical properties and resist attacks of the same type, achieving a robust system capable of resisting brute force attacks and thus demonstrating that this system is applicable for the transmission of biometric data over open and shared networks. However, AM is not sufficient to protect against statistical attacks. This is why a second phase of encryption is needed using Lorenz' system, as used in different works such as [37,38]. The Lorenz system is a model of thermally induced fluid convection in the atmosphere, which has properties that make it ideal for ciphering images. It is defined by the following set of equations:

$$x_1 = a(x_2 - x_1) \tag{2}$$

$$x_2 = cx_1 + x_2 - x_1x_3 - x_4 \tag{3}$$

$$x_3 = x_1x_2 - bx_3 \tag{4}$$

$$x_4 = kx_2x_3 \tag{5}$$

Figure 4 shows the Lorenz system for x_1, x_2, and x_3, with initial conditions $x_1 = 2.7$, $x_2 = 1.3$, $x_3 = -1.7$, and $x_4 = -5$.

Equations (2)–(5) correspond to the 4D hyperchaotic Lorenz system, where $a, b, c, k > 0$ are the control parameters. Using suitable values can obtain the desired chaotic behavior. In this work, we employ the encryption scheme presented in [23] that utilizes this Lorenz model. In addition, we consider [24], where the 3D Lorenz classical model is used for iris image encryption.

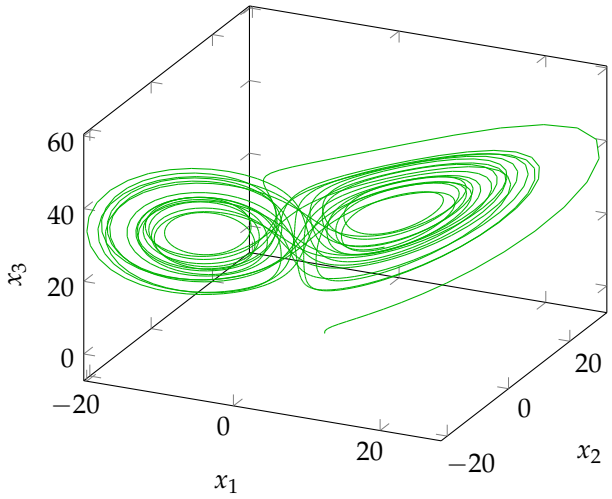


Figure 4. Lorenz system with initial conditions $x_1 = 2.7$, $x_2 = 1.3$, $x_3 = -1.7$, and $x_4 = -5$. Plot of x_1, x_2, and x_3.

Encryption Process

The introduced encryption algorithm uses RGB images of the eye and bases its operation on two means, permutation and diffusion; the first is performed through Arnold's chaotic map, while the second is accomplished through the numerical solutions 4th of Lorenz's system generated by Runge Kutta. In the permutation phase, each pixel is repositioned with one-to-one correspondence, i.e., all pixels composing the permuted image correspond to the group of pixels of the original image, making it possible to recover the actual image without any distortion. Different techniques can be applied in this situation; Arnold's Chaotic Map provides easy and efficient implementation and shows consistent results in terms of the metric used to establish how much the pixels have moved from the original position [39].

To describe the encryption process, the width w and height of the image h are obtained, and three arrays arr_r, arr_g, and arr_b of cardinality $w \times h + \delta$ are generated with values obtained from the Lorenz map using R4. The value δ is a natural number representing the amount of iterations required for the values of x_1, x_2, x_3, and x_4 to enter the chaotic system.

Figure 5 illustrates the image ciphering process and Figure 6 is a subset of images of the CASIA dataset used to perform statistical analysis. First, the image histogram is observed without carrying out the encryption process. Later, the respective encryption allows for observation of cases in which image transmission is susceptible to a "digital attack". In this context, a "digital attack" attempts to reconstruct the transmitted image without authorization.

Figure 5. Image with an abnormality in the bottom right part of the iris (image used for testing).

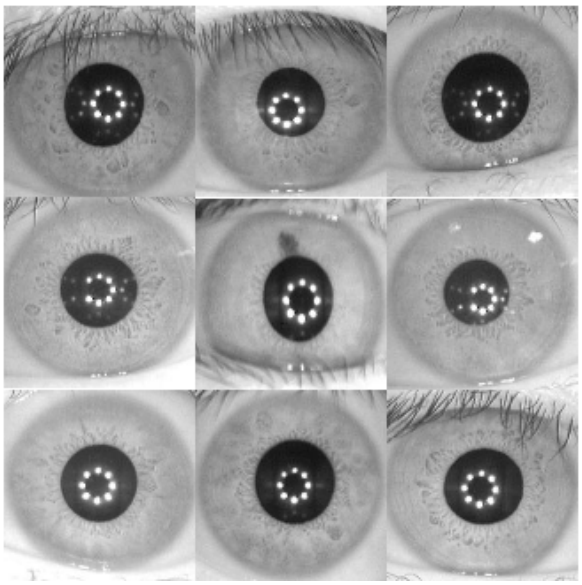
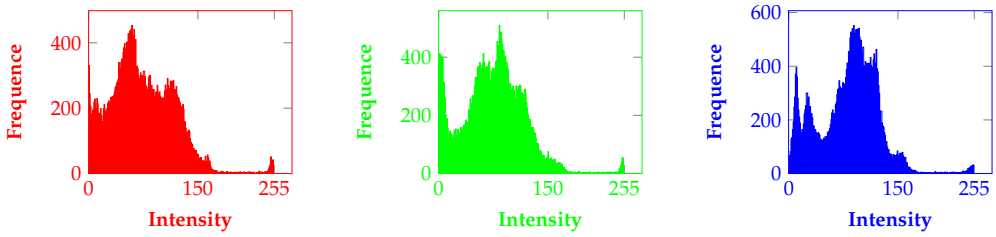


Figure 6. Subset of images from the CASIA Iris dataset used to perform statistical analysis of the proposed ciphering scheme.

The more uniform the histograms are, the more secure the ciphering is against statistical attacks; the histograms of the real image can be seen in Figure 7a–c. If permutation is not carried out, it is feasible that an attacker could gain insights into the original image.

An example of a process of ciphering without using permutation is presented in Figure 8. it can be seen that the ciphering process without a permutation procedure causes the circular structure of the iris to be somewhat recognizable.



(**a**) (**b**) (**c**)

Figure 7. Histograms for RGB channels of the original image (Figure 5): (**a**) red image histogram, (**b**) green image histogram, (**c**) blue image histogram.

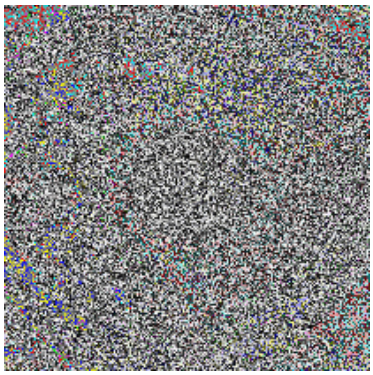


Figure 8. Ciphering process without a permutation process causes the circular structure of the iris to be recognizable.

The patterns displayed in the images permuted with Arnold's map are based on the number of iterations. For instance, Figure 9 shows the images in Figure 6, and with these results Figure 10 displays the diffused images with Lorenz.

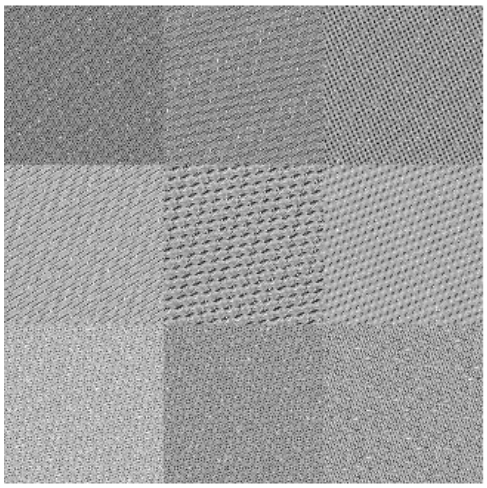


Figure 9. Nine of the ciphered images after Arnold's map.

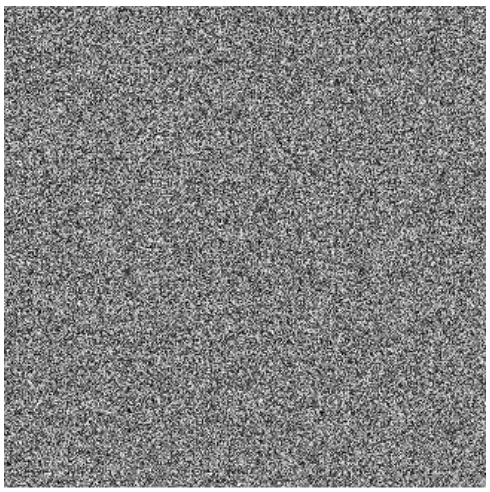
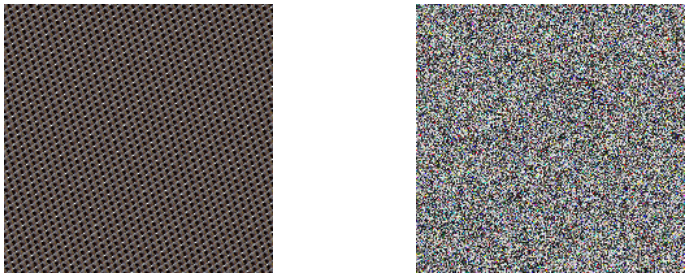


Figure 10. Nine ciphered images with Lorenz' attractor and Arnold's map.

4. Results

A simulated example of a diagnosis carried out over two eyes of the test dataset can be seen in Figure 1. The top image shows a healthy picture corresponding to the diagnosis "Your eye is healthy" and at the bottom, the image contains a potential abnormality, an unhealthy eye. In this case, the option "Use AI to diagnose" was used to produce the results, which triggers the CNN network and produces a number with a probability, which in this case is "Doctor, there is a 98.6% probability" that the eye has Uveal Melanoma. Next, considering Figure 5 to illustrate the process of image ciphering, the module receives an eye image which is permuted using Arnold's Map to produce Figure 11a. Finally, this image is diffused using Lorenz' attractor, generating Figure 11b, which can then be transmitted over the network. The original database used here is taken from [28].



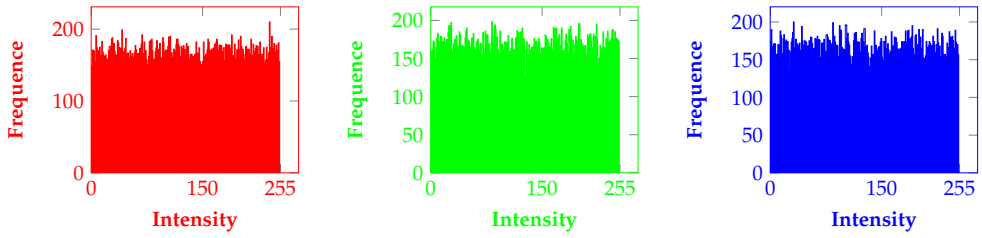
(**a**) (**b**)

Figure 11. Results of the permutation and diffusion processes. The input of the diffusion process is the result of the permutation stage. As can be seen, the shape of the iris is no longer presented. (**a**) Image permuted with seven iterations using Arnold's map. (**b**) Image permuted ciphered using Lorenz' attractor.

As explained in [40], there are different kinds of correlation attacks. Correlation analysis techniques include the Mean Difference Method (MDM) and Pearson Correlation Coefficient Method (PCCM); producing lower values of correlation makes the system more robust against these attacks. Hence, it is a crucial statistical analysis tool based on the frequency distribution of the encrypted pixels illustrated in the histograms (visual representation of such distribution, plotting the number of pixels at each level). After performing the proposed scheme, the results of the correlation can be seen in Table 2, exposing small correlation values for the transmitted images. In addition, the histograms can be seen in Figure 12a–c, showing that the ciphered images have a uniform distribution in the intensity of each color component, which in plain sight would result in an inconsistent or meaningless image. Thus, the possibility of an attacker obtaining the actual image is noticeably low, as the pixels of each color component of the encrypted image are distributed without providing any indication to use in statistical analysis to obtain a possible image.

Table 2. Correlation values for Red, Green, and Blue channels for different images in the encryption process.

Image	Red	Green	Blue
Figure 5 (Image without ciphering)	0.996	0.996	0.995
Figure 11a (Image after Arnold's map)	0.314	0.276	0.274
Figure 11b (Image after Arnold's map and Lorenz' attractor)	0.002	0.001	0.002



(**a**) (**b**) (**c**)

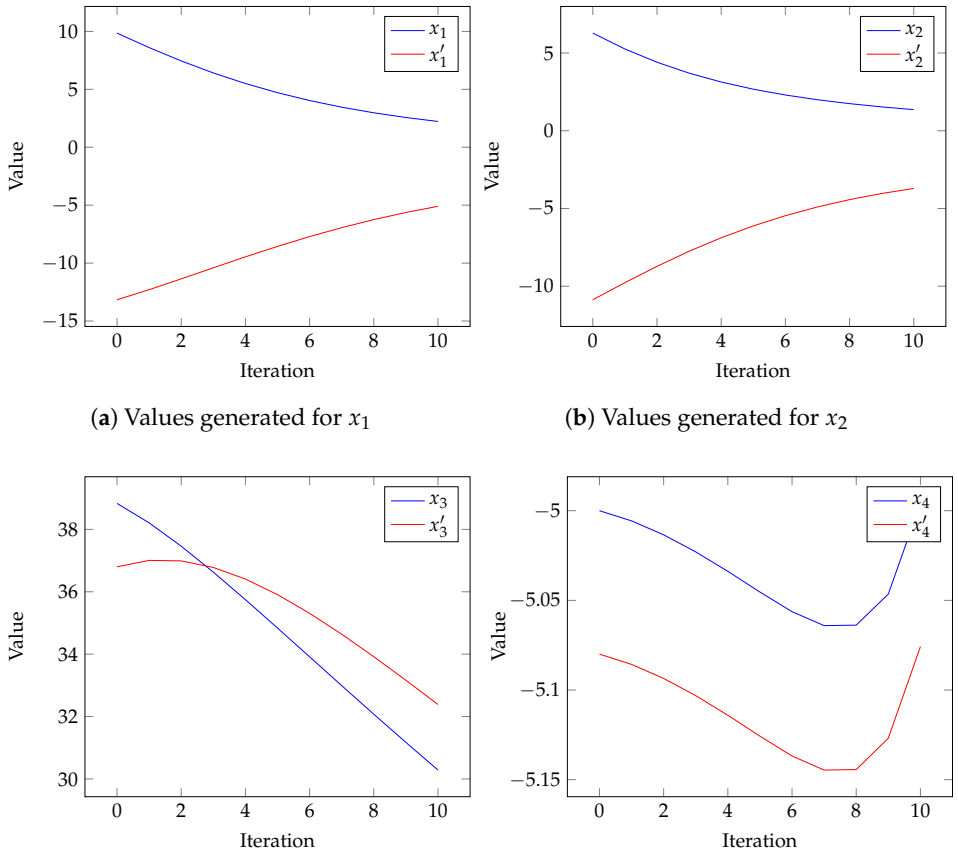
Figure 12. Histograms of RGB channels for a given ciphered image: (**a**) histogram red channel, (**b**) histogram green channel., (**c**) histogram blue channel.

4.1. Sensibility in the Key

As mentioned above, in a chaotic system the initial conditions significantly affect the performance of the Chen system. A security system must be sensitive to a wrong key to ensure that data cannot be obtained without the proper key. To provide an example, the following are the initial conditions: $[x_1 = 2.7, x_2 = 1.3, x_3 = -1.7, x_4 = -5]$, and to

measure to sensitivity, these values are slightly changed to $[x'_1 = 2.71, x'_2 = 1.3, x'_3 = -1.71, x'_4 = -5.08]$. This slight alteration produces large changes, confirming the high sensitivity present in the Lorenz system. In order to observe the sensibility of the initial conditions, Figure 13 shows the values for x_1, x_2, x_3 and x_4. The values of (x_1, x_2, x_3) are used to cipher each of the RGB pixels. Therefore, a small alteration in any of the initial conditions produces remarkably different results.

Sensitivity to initial conditions is one of the requirements defined by Shannon [41] for confusion and diffusion in cryptography; the problem with these systems is that they can be broken due to their small key space [42,43], as the most important part of any encryption algorithm is the key that defines whether the system is sufficiently strong against attacks. However, as shown in [44], the Lorenz system can be used to generate keys that successfully pass the National Institute of Standards and Technology (NIST) statistical test suite.



(**a**) Values generated for x_1

(**b**) Values generated for x_2

(**c**) Values generated for x_3

(**d**) Values generated for x_4

Figure 13. Values generated with initial conditions for x_1, x_2, x_3, and x_4.

4.2. Metrics

According to [45], the NPCR and UACI statistical tests are employed when dealing with base chaos encryption; for example, references [46,47] employed these metrics. The Number of Pixel Change Rate (NPCR), which computes the pixel difference ratio between ciphered and original images, is calculated with Equation (6); in this equation, $D(i,j)$ corresponds to Equation (7):

$$\text{NCPR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{6}$$

$$D(i,j) = \begin{cases} 0, & \text{if } A(i,j) = B(i,j) \\ 1, & \text{if otherwise} \end{cases} \tag{7}$$

where $A(ij)$ is the pixel value of the original image, $B(i,j)$ is the pixel value of the encrypted image, and (M,N) corresponds to image dimensions. A higher NPCR displays better algorithm performance. The range of NPCR values is $[0, 1]$.

Meanwhile, UACI computes the difference between the ciphered image and the original image, allowing the strength of the encryption algorithm to be observed. UACI measures the average change in a pixel's values between the ciphered and original images by employing Equation (8):

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|A(i,j) - B(i,j)|}{255} \times 100\%. \tag{8}$$

A high UACI indicate that the systems is resistant against different attacks. The state of the art shows that a UACI of 0.33 is a secure value [24].

The entropy metric relies on the probability of pixel values and computes the degree of randomness; this metric is calculated using Equation (9), where $P(i)$ is the probability of pixel value i and is computed by Equation (10):

$$E = \sum_{i=0}^{255} \left(P(i) \log_2 \left(\frac{1}{P(i)} \right) \right), \tag{9}$$

$$P(i) = \frac{\text{Frequency of the pixel value } i}{\text{Total number of image pixels}}. \tag{10}$$

The efficiency of the encrypted image is superior if the entropy value is greater. The maximum entropy value is 8.

In this work, the results of these metrics for RGB images are shown in Table 3, in which it can be seen that the NPCR, UACI, and Entropy in the ciphered images have high values of security acceptable for use in image transmission.

Table 3. Results of NPCR, UACI, and Entropy tests for a RGB image after permutation and diffusion.

Measure	Red	Green	Blue
NPCR	0.996	0.996	0.996
UACI	0.310	0.328	0.334
Entropy	7.996	7.996	7.995

In order to ensure that the obtained result was not an outlier, we used the Chinese Academy of Sciences—Institute of Automation (CASIA) database, taking several iris images in grayscale to obtain a dataset that allows a statistical analysis to be performed. For iris recognition research, CASIA contains a free access database; the images were captured using a uniform illumination to obtain an adequate iris image. This database of free access images can be found in [48].

Example images and the results of the iterations are shown in Figures 6, 9 and 10, while the metrics obtained after this process are shown in Table 4 for 145 images. These results show that near-maximum values of NPCR are obtained, as are near-safe values of UACI and high entropy in the different channels for the ciphered images. These values are sufficiently high for encrypted images, and therefore can be considered to have strong resistance to differential attacks.

Table 4. Metrics: median, standard deviation, minimum and maximum of 145 images for NPCR, UACI, and Entropy using CASIA dataset.

Measure	Median	Standard Deviation	Min	Max
NPCR	0.996	0.0004	0.994	0.997
UACI	0.296	0.0196	0.266	0.357
Entropy	7.954	0.0022	7.949	7.961

5. Discussion

Although this article describes a system for medical diagnosis, the main results aim to showing the various aspects of the encryption process; consequently, a user test is outside the scope of this work. This is due to the difficulty of establishing a group of professionals to carry out such tests. Additionally, the details of the convolutional neural networks used for the classification system can be consulted in [29].

As mentioned, there are several different works related to the proposal made in this document, included those on computer-aided diagnosis systems, image classification, and encryption systems. Several references cited in the introduction section were considered here, as follows:

- Computer Aided Diagnosis [9–12];
- Eye Image Classification [13–16];
- Chaotic Encryption [17–22].

It should be noted that [18] considered the encryption of medical images and [22] considered internet of things applications which included the possibility of remote diagnosis.

As observed, a comparison with related works can be made considering different approaches. In this respect, a comparison consists of the process of image encryption taking similar works as reference. Then, considering the average values for the implementations made in other related works, Table 5 displays the NPCR, UACI, and entropy values.

Although all cited works present better values in the metrics considered, the results obtained are close to those reported in [17–22], taking into account that the best values of the indicators are close to 1 for NPCR, around 0.33 for UACI, and 8 for entropy. In addition, in this comparison it should be considered that different numbers of figures with several sizes and features were used to carry out the tests. As displayed in Table 5, in this work 145 figures were used to validate the encryption process, which is more than in the other works. Therefore, to make a uniform comparison, in future works a benchmark must be defined considering standard figures according to the application in consideration.

Table 5. Performance comparison with other related works.

Research	Images Used	NPCR	UACI	Entropy
This work	145	0.9960	0.2960	7.9540
Reference [17]	1	0.9987	0.4996	7.9951
Reference [18]	3	-	-	7.9957
Reference [19]	4	0.9961	0.3347	7.9027–7.9999
Reference [20]	1	0.9981	0.3362	7.9996
Reference [21]	3–10	0.9961	0.3344	7.9983
Reference [22]	4	0.9962	0.3345	7.9993

6. Conclusions

In this paper, we have presented a system for medical image diagnosis using chaotic-base encryption with a particular case for Uveal Melanoma diagnosis. This cipher scheme was assessed using several statistical tests, including entropy test analysis, key sensitivity test, correlation properties, and randomization tests using UACI and NPCR. Although the encryption confirms that the original and encrypted images have no visual correspondence, statistical analysis through histograms reveals uniform distributions. Nonetheless, the correlation coefficients of adjacent pixels are low enough to guarantee that the original image cannot be easily recovered from the image resulting from the encryption process without knowledge of the initial conditions.

It should be noted that the Arnold maps with the Lorenz system are an encryption scheme with suitable results for the transmission of images over public networks, which requires the confidentiality, integrity, and privacy of the message.

The results display adequate performance of the encryption system, with high values obtained for NPCR (0.994 to 0.997), near-safe values for UACI (0.266 to 0.357), and high entropy of 7.949 to 7.961 for the ciphered images.

Considering the results in Table 4 for the 145 images, NPCR describes the lowest variation (standard deviation) of 0.0004 for the tests performed, followed by entropy with 0.0022, and finally UACI at 0.0196. This shows that the experiments carried out do not present greater variation when encrypting the largest number of processed figures in the same way.

In subsequent work, we intend to carry out user tests in order to improve the computer-aided diagnosis system.

Author Contributions: Conceptualization, D.F.S. and H.E.E.; Methodology, D.F.S. and H.E.E.; Project administration, H.E.E.; Supervision, H.E.E.; Validation, D.F.S.; Writing—original draft, D.F.S.; Writing—review and editing, D.F.S. and H.E.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The study was self-financed.

Institutional Review Board Statement: In this work, direct tests were not carried out on individuals (humans). The historical data used for this study can be found in [28].

Informed Consent Statement: The data used were requested from [28].

Data Availability Statement: The original database can be found at [28].

Acknowledgments: We would like to thank Paul T. Finger, the New York Eye Cancer Center, and the Institute of Automation of the Chinese Academy of Sciences for providing the data for the present study. We wish to thank the Universidad Distrital Francisco José de Caldas, the École Nationale Supérieure Mines-Télécom Atlantique Bretagne-Pays and the University of Nantes for encouraging this research.

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

References

1. Wang, L.; Wang, X.L.; Yuan, K.H. Design and implementation of remote medical image reading and diagnosis system based on cloud services. In Proceedings of the 2013 IEEE International Conference on Medical Imaging Physics and Engineering, Shenyang, China, 19–20 October 2013; pp. 341–347. [CrossRef]
2. Coatrieux, G.; Puentes, J.; Roux, C.; Lamard, M.; Daccache, W. A Low Distorsion and Reversible Watermark: Application to Angiographic Images of the Retina. In Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, Shanghai, China, 17–18 January 2005; pp. 2224–2227. [CrossRef]
3. Coatrieux, G.; Le Guillou, C.; Cauvin, J.M.; Roux, C. Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *13*, 158–165. [CrossRef] [PubMed]
4. Ahmad, A. Evaluation of Modified Categorical Data Fuzzy Clustering Algorithm on the Wisconsin Breast Cancer Dataset. *Scientifica* **2016**, *2016*, 4273813. [CrossRef] [PubMed]
5. Amin, J.; Sharif, M.; Yasmin, M. A Review on Recent Developments for Detection of Diabetic Retinopathy. *Scientifica* **2016**, *2016*, 6838976. [CrossRef]

6. Lu, X. A Cooperative Telemedicine Environment for Stomatological Medical Diagnosis. In Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation, Luoyang, China, 25–28 June 2006.
7. Ouyang, H.B.; Liu, S.; You, L.; Huang, W.H.; Zhong, S.Z. Study on the new design of computer-aided diagnosis system. In Proceedings of the 2009 IEEE International Symposium on IT in Medicine Education, Jinan, China, 14–16 August 2009; Volume 1, pp. 50–55. [CrossRef]
8. Abadi, M.; Agarwal, A.; Barham, P.; Brevdo, E.; Chen, Z.; Citro, C.; Corrado, G.; Davis, A.; Dean, J.; Devin, M.; et al. TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems. *arXiv* **2015**, arXiv:1603.04467.
9. Ciprian, C.; Masychev, K.; Ravan, M.; Manimaran, A.; Deshmukh, A. Diagnosing Schizophrenia Using Effective Connectivity of Resting-State EEG Data. *Algorithms* **2021**, *14*, 139. [CrossRef]
10. Alorf, A. The Practicality of Deep Learning Algorithms in COVID-19 Detection: Application to Chest X-ray Images. *Algorithms* **2021**, *14*, 183. [CrossRef]
11. Villavicencio, C.N.; Macrohon, J.J.E.; Inbaraj, X.A.; Jeng, J.H.; Hsieh, J.G. COVID-19 Prediction Applying Supervised Machine Learning Algorithms with Comparative Analysis Using WEKA. *Algorithms* **2021**, *14*, 201. [CrossRef]
12. Böcking, A.; Friedrich, D.; Schramm, M.; Palcic, B.; Erbeznik, G. DNA Karyometry for Automated Detection of Cancer Cells. *Cancers* **2022**, *14*, 4210. [CrossRef]
13. Akande, O.N.; Abikoye, O.C.; Kayode, A.A.; Lamari, Y. Implementation of a Framework for Healthy and Diabetic Retinopathy Retinal Image Recognition. *Scientifica* **2020**, *2020*, 4972527. [CrossRef]
14. Garde, G.; Larumbe-Bergera, A.; Bossavit, B.; Porta, S.; Cabeza, R.; Villanueva, A. Low-Cost Eye Tracking Calibration: A Knowledge-Based Study. *Sensors* **2021**, *21*, 5109. [CrossRef]
15. Avilés-Rodríguez, G.J.; Nieto-Hipólito, J.I.; Cosío-León, M.d.l.A.; Romo-Cárdenas, G.S.; Sánchez-López, J.d.D.; Radilla-Chávez, P.; Vázquez-Briseño, M. Topological Data Analysis for Eye Fundus Image Quality Assessment. *Diagnostics* **2021**, *11*, 1322. [CrossRef] [PubMed]
16. Aziz, T.; Ilesanmi, A.E.; Charoenlarpnopparut, C. Efficient and Accurate Hemorrhages Detection in Retinal Fundus Images Using Smart Window Features. *Appl. Sci.* **2021**, *11*, 6391. [CrossRef]
17. Rahman, Z.A.S.A.; Jasim, B.H.; Al-Yasir, Y.I.A.; Abd-Alhameed, R.A. High-Security Image Encryption Based on a Novel Simple Fractional-Order Memristive Chaotic System with a Single Unstable Equilibrium Point. *Electronics* **2021**, *10*, 3130. [CrossRef]
18. Almatroud, O.A.; Tamba, V.K.; Grassi, G.; Pham, V.T. An Oscillator without Linear Terms: Infinite Equilibria, Chaos, Realization, and Application. *Mathematics* **2021**, *9*, 3315. [CrossRef]
19. El-Latif, A.A.A.; Ramadoss, J.; Abd-El-Atty, B.; Khalifa, H.S.; Nazarimehr, F. A Novel Chaos-Based Cryptography Algorithm and Its Performance Analysis. *Mathematics* **2022**, *10*, 2434. [CrossRef]
20. Rahman, Z.A.S.A.; Jasim, B.H.; Al-Yasir, Y.I.A.; Abd-Alhameed, R.A. Efficient Colour Image Encryption Algorithm Using a New Fractional-Order Memcapacitive Hyperchaotic System. *Electronics* **2022**, *11*, 1505. [CrossRef]
21. Liu, Z.; Li, J.; Di, X. A New Hyperchaotic 4D-FDHNN System with Four Positive Lyapunov Exponents and Its Application in Image Encryption. *Entropy* **2022**, *24*, 900. [CrossRef]
22. Li, L.; Abd El-Latif, A.A.; Jafari, S.; Rajagopal, K.; Nazarimehr, F.; Abd-El-Atty, B. Multimedia Cryptosystem for IoT Applications Based on a Novel Chaotic System around a Predefined Manifold. *Sensors* **2022**, *22*, 334. [CrossRef]
23. Santos, D.F.; Barrera Amaya, I.; Suárez Parra, C.A. Encryption algorithm for color Images based on chaotic systems. *Ingeniería* **2020**, *25*, 144–161. [CrossRef]
24. Santos, D.F. Chaos-based Digital Image Encryption Using Unique Iris Features. *Int. J. Appl. Eng. Res.* **2020**, *15*, 358–363. [CrossRef]
25. Santos, D.F.; Espitia, H.E. Detection of Uveal Melanoma using fuzzy and neural networks classifiers. *Telkomnika* **2020**, *18*, 2213–2223. [CrossRef]
26. Santos, D.F.; Espitia, H.E. Proposal for a Neuro-Fuzzy System for Uveal Melanoma Detection. *J. Eng. Appl. Sci.* **2021**, *16*, 523–531.
27. Sodhi, B.; Agrawal, A.; Prabhakar, T.V. Appification of web applications: Architectural aspects. In Proceedings of the 2012 1st IEEE International Conference on Communications in China Workshops (ICCC), Beijing, China, 15–17 August 2012; pp. 1–7. [CrossRef]
28. New York Eye Cancer Center. Iris Tumors. Available online: https://eyecancer.com/eye-cancer/image-galleries/iris-tumors/ (accessed on 1 February 2021).
29. Daniel-Fernando, S.B.; Binh-Minh, N.; Helbert-Eduardo, E. Towards automated eye cancer classification via VGG and ResNet networks using transfer learning. *Eng. Sci. Technol. Int. J.* **2022**, *in press*. [CrossRef]
30. Goceri, E. Analysis of Deep Networks with Residual Blocks and Different Activation Functions: Classification of Skin Diseases. In Proceedings of the 2019 Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), Istanbul, Turkey, 6–9 November 2019. [CrossRef]
31. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778. [CrossRef]
32. Umamageswari, A.; Suresh, G. Security in medical image communication with arnold's cat map method and reversible watermarking. In Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 20–21 March 2013; pp. 1116–1121. [CrossRef]

33. Fu, C.; Tang, J.; Zhou, W.; Liu, W.; Wang, D. A symmetric color image encryption scheme based on chaotic maps. In Proceedings of the 2013 15th IEEE International Conference on Communication Technology, Guilin, China, 17–19 November 2013; pp. 712–716. [CrossRef]
34. Peng, J.; Jin, S.; Liu, Y. Design and Analysis of an Image Encryption Scheme Based on Chaotic Maps. In Proceedings of the 2010 International Conference on Intelligent Computation Technology and Automation, Changsha, China, 11–12 May 2010. [CrossRef]
35. Chen, D. A Feasible Chaotic Encryption Scheme for Image. In Proceedings of the 2009 International Workshop on Chaos-Fractals Theories and Applications, Shenyang, China, 6–8 November 2009. [CrossRef]
36. Mehta, G.; Dutta, M.K.; SooKim, P. Biometric data encryption using 3-D chaotic system. In Proceedings of the 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS), Mathura, India, 18–20 November 2016. [CrossRef]
37. Zou, C.; Zhang, Q.; Wei, X.; Liu, C. Image Encryption Based on Improved Lorenz System. *IEEE Access* **2020**, *8*, 75728–75740. [CrossRef]
38. Celİk, K.; Kurt, E. A new image encryption algorithm based on lorenz system. In Proceedings of the 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, Romania, 30 June–2 July 2016; pp. 1–6. [CrossRef]
39. Abd-El-Hafiz, S.K.; AbdElHaleem, S.H.; Radwan, A.G. Permutation techniques based on discrete chaos and their utilization in image encryption. In Proceedings of the 2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 28 June–1 July 2016. [CrossRef]
40. Fei, H.; Daheng, G. Two kinds of correlation analysis method attack on implementations of Advanced Encryption Standard software running inside STC89C52 microprocessor. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016; pp. 1265–1269. [CrossRef]
41. 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. [CrossRef]
42. Ye, R.; Guo, W. An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters. *Int. J. Comput. Netw. Inf. Secur.* **2014**, *6*, 37–45. [CrossRef]
43. Guo, W.; Wang, X.; He, D.; Cao, Y. Cryptanalysis on a parallel keyed hash function based on chaotic maps. *Phys. Lett. A* **2009**, *373*, 3201–3206. [CrossRef]
44. Oğraş, H.; Türk, M. A Robust Chaos-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism. *J. Inf. Secur.* **2017**, *8*, 23–41. [CrossRef]
45. Özkaynak, F. Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 621–624. [CrossRef]
46. Shah, D.; Haq, T.U.; Shah, T. Image Encryption Based on Action of Projective General Linear Group on a Galois Field GF(28). In Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), London, UK, 4–6 July 2018; pp. 38–41. [CrossRef]
47. Elkamchouchi, H.M.; Shawky, M.A.; Takieldeen, A.E.; Fouda, I.; Khalil, M.; Elkomy, A.; AbdElrasol, A. A New Image Encryption Algorithm Combining the Meaning of Location with Output Feedback Mode. In Proceedings of the 2018 10th International Conference on Communication Software and Networks (ICCSN), Chengdu, China, 6–9 July 2018; pp. 521–525. [CrossRef]
48. CASIA. Iris Database. Available online: http://forensics.idealtest.org (accessed on 1 February 2021).