Encrypting Image based on Chaotic Map algorithm

Zahraa Salah Dhaief[1], **Dena Nadir George**[2] **& Raniah Ali Mustafa**[3]

[1-3]College of Education, Department of Computer Science

Mustansiriyah University, Iraq

_____

ABSTRACT

Due to the network and multimedia application developments, information security become important since information can be attacked over the transmission channels, and the combination of cryptography and chaotic become an important field of information security, where many encryption algorithms are based on chaotic mapping due to the inherent features of Image like high redundancy and bulk data capacity. In this paper, three chaotic maps are used to achieve a good diffused Image by setting the initial conditions to generate the shuffling sequence randomly by 2D Zaslevskii map and employ them in 2D cat map for shuffling the image pixels positions; also baker map is used to decomposed Image into four rectangles and shuffle them.

For increasing the levels of security related to the encryption algorithm, the Gaffe random key generator is used to generate 128 bits keys and employ it with an exclusive-OR equation to the diffused Image. The results indicated that the combination of chaotic and cryptography proved to be good for the high-security level. The experimental results have shown that the suggested algorithm is secure due to the large key space and the high sensitivity to the secret key. This paper applies a chaotic map algorithm by Mat lab a program.

Key Words: Cryptography, Chaotic map, Image processing, Digital image, Encrypting image.
_____

1. INTRODUCTION

The way humans are working and playing is transformed by the introduction of the internet since it allows communications, sharing data as well as seeking information in just a few seconds. All this can be done via using networks and computers. The internet can be defined as a global network of the computers, while all the computer devices (laptops, PCs, smartphones, and game consoles) which were connected to internet are considered as part of such network. When added together, billions of the computers that are connected to the internet will have the ability to communicate between them. Recently, novel informational technologies and the internet are used in all business areas – service and manufacturing, management Development of society lead toward the importance of data that has been utilized; thus, large amounts of digital visual data have been stored on different media as well as exchanged over many network types today. Images are vital in our lives; their digital form is very important because of the performance enhancements in network bandwidth, media storage, and computer speed. Therefore, the possibility for such information form to be attacked by (fabrication or modification) is high in comparison to paper-based images. A few types of methods were needed for maintaining authenticity, integrity, and privacy.

One of the best ways for ensuring the security features is encryption; it is utilized for protecting the data in transit, for transfer by networks (cellular devices, Palmtops, Internet) [1]. Some encryption algorithms like RC5, IDEA, and DES are considered to be computationally complicated and have low-efficiency levels with large-volume image data [2, 3]. For image encryption, the major primitives are categorized into 3 main types: Positive permutation, value transformation, and combined form [4-8]. Majorly, chaos encryption is utilized for achieving the first 2 primitives for a long-time. Often, the chaotic maps occur in studying dynamic non-linear systems. Mathematical equations rule its behavior as well as insignificant changes in the initial position result in considerably different outcomes and appear disorderly and random; however, they are following certain patterns [9]. Chaotic output signals that are presenting random statistical characteristics were utilized for diffusion and confusion operations in the cryptosystems. This study suggested a key generator and a chaotic image encryption system. The produced key might be utilized as an initial condition in terms of the 1-D logistic map. Furthermore, the plain Image is divided into fixed-size blocks; every one of

the blocks will be encrypted with a distinctive key acquired via 1-D logistic map. The block size is 8bits. Also, the experimental results utilizing image database is showing the strength and efficiency of the suggested chaotic image encryption for different images. Lastly, the security analysis is showing that the suggested system has the ability to generate statistically random encrypted images.

2. IMAGE PROCESSING

Image processing can be defined as a technique by which images are converted into digital form as well as performing a few operations on it for getting an improved image or for extracting certain significant information from it. Also, it is considered as a signal dispensation type where the input was an image, like a photograph or video frame, while the output could be an image or a property related to the Image. Typically, the systems of image processing handling the images as 2D signals while using an already-set signal processing approach to them. Today, image processing is one of the rapidly-growing technologies since it is used in many business aspects. Also, it is fundamental in computer science and engineering. Basically, image processing includes the next 3 steps, importing the Image by digital photography or via optical scanner, manipulating and analyzing images that involve image enhancement, data compression, and spotting patterns that aren't obvious to human eyes, such as photographs. The last stage is the output, where the results might be an altered image or report, which is on the basis of image analysis [10].

2.1 Image Processing Objectives

 1. Visualization: - Observing the not-visible objects.

2. Image restoration and sharpening: - For creating better images.

3. Image retrieval: - Searching for the Image of interest.

4. Pattern measurement: - Measuring different image objects.

5. Image Recognition: - Recognizing the image objects [10].

2.2 Image Processing Types

There are 2 image processing types; digital and analog. The latter is applied for hard copies like the photos and printouts. Image analysts are using many interpretation fundamentals when utilizing such visual approaches. Image processing isn't just limited to the area which must be examined, yet on the analyst's knowledge. Association is considered as one of the other significant image processing tools via visual approaches. Therefore, analysts are using a combination of collateral data and personal knowledge in image processing. On the other hand, digital processing methods allow manipulating digital images via utilizing computers. Since the imaging sensor data from satellite platforms have deficiencies, it must undergo many processing phases for getting the originality of information and overcoming such issues. Preprocessing, display and enhancement, and information extraction are the 3 stages which all the data types must undergo when utilizing the digital technique [10].

2.3 Applications of Image Processing

1. **Intelligent Transportation Systems: -** This method might be utilized for traffic sign recognition and automatic number plate recognition.
2. **Remote Sensing: -** With regard to such application, the sensors are capturing the earth surface pictures in remote sensing satellites or multi-spectral scanner that is mounted on an aircraft. The pictures were processed via transmitting them to the earth station. Also, the methods utilized for interpreting regions and objects were utilized in city planning, flood control, agricultural production monitoring, resource mobilization, and so on.
3. **Moving object tracking: -** This application allows measuring the motion parameters as well as acquiring visual records of the moving objects.
   There are various approaches for tracking objects:

❖ **Motion-based tracking**
❖ **Recognition-based tracking**
4. **Defense surveillance: -** The methods of aerial surveillance were utilized for endlessly focusing on oceans and land. Also, this application is utilized for locating the formation and types of naval vessels regarding ocean surface. The major aim is to

divide the different objects existing in the water body part related to the Image. The various parameters like breadth, length, perimeter, area, and compactness were set up for classifying each one of divided objects. There is high importance in recognizing such objects' distribution in many directions, which were west, east, south, north, northwest, northeast, southwest, and southeast, for explaining all the potential vessels' formations. The whole oceanic scenario can be interpreted from such objects' spatial distribution.

5. **Biomedical Imaging Methods: -** With regard to medical diagnosis, various imaging tools' types, including Ultrasound, X-ray, computer-aided tomography (CT), and so on, were utilized. The diagrams related to MRI, X-ray, and computer-aided tomography (CT) is provided as follows:

Some Biomedical Imaging Applications are:

- **Identification of Heart Diseases: -** The significant diagnostics features like the shape and the size of the heart must be known for classifying heart diseases. For improving heart disease diagnostics, image analysis methods were used in radiographic images.
- **Digital mammograms: -** This is utilized for detecting breast tumors. Also, mammograms might be examined by means of image processing methods like shape analysis, segmentation, feature extraction, contrast enhancement, and so on.
- **Identification of Lung Disease: -** With regard to X- rays, the regions which appear dark contain air, whereas the region which appears light is solid tissues. Also, bones were more radio-opaque compared to tissues. Thoracic spine, heart, ribs, and the diaphragm separating the chest cavity from the abdominal cavity were seen (clearly) on X-ray films.
- **Automatic inspection of incandescent lamp filaments: -** This includes examining the process of bulb manufacturing. Because of the non-uniformity in the pitch related to lamp wiring, the bulb's filament is fused in short-duration. With regard to such application, a binary image slice regarding the filament is formed by which the filament's silhouette is fabricated. Furthermore, silhouettes were examined to recognize the non-uniformity in the wiring pitch in the system utilized via General Electric Corporation.
- **Automatic Visual Inspection System: -** The application enhances the productivity and quality of products in industries.
- **Automatic surface inspection systems:** - With regard to metal industries, there is high importance in detecting surface flaws. For example, there is high importance in detecting any aberration type on the rolled metal surface in cold or hot rolling mills in steel plants. Furthermore, image processing approaches like edge detection, fractal analyses, texture identification, etc. were utilized for detection.
- **Identification of Faulty Components: -** This application is used for identifying the faulty components in electromechanical or electronic systems. High thermal energy amounts are generated via such faulty components. Also, the IR images were formed from the distribution regarding thermal energy assembly. Faulty components might be recognized via examining the IR images [11].

3. CRYPTOGRAPHY

Cryptography is the science of secret writing with the target of transforming readable information into an unreadable form by designing cryptographic systems. Cryptanalysis is the science and sometimes art of breaking cryptographic systems. Cryptology is a term used to embody the study of both cryptography and cryptanalysis [12]. A plaintext is an intelligible message, whereas a ciphertext is the unintelligible form of the message. The process by which the plaintext is converted into ciphertext is referred to as enciphering or encryption, while the deciphering or decryption is the plaintext's retrieval from the ciphertext. Also, the cryptography system ingredients are plaintext, cipher key, encryption algorithm that takes a plain-text and cipher key to be the input and produces cipher-text to be the output and decryption algorithm which is considered as the inverse of encryption algorithm [12].

3.1 Types of Cryptographic Systems

3.1.1 Types of encryption algorithms according to data entry method

a. **Substitution**: A substitution technique changes the characters of plaintext to produce a ciphertext. A simple example of these ciphers is the Caesar cipher. The goal of substitution is the confusion that is preventing the cryptanalyst from discovering any relation between cipher-text and the key [12].

b. **Transposition**: A transposition technique rearranges the places where the plaintext letters sit, where the letters do not change, but rather move them around without introducing any new letters. Using transposition, the cryptography targets to achieve diffusion widely spread the information of the message or the key across the ciphertext. Since a transposition rearranges the symbols of a message, it is also called a permutation. An example of these ciphers is columnar transposition [13].

c. **Product ciphers**: - A product cipher combines substitution and transposition ciphers, where simple transposition and substitution ciphers individually don't give high security. However, when these transformations are combined, it is probable to gain a robust cipher, and then a product cipher can add both confusion and diffusion to the encryption algorithm [13].

3.1.2 Encryption algorithms by a method of encryption key type and decryption

3.1.2.1 Symmetric Cryptography

With regard to symmetric cryptography, just one key is utilized for decryption and encryption. As displayed in Figure (1.1), the sender is using a key and the algorithm to encrypt the plaintext and sends the ciphertext to the recipient. The recipient employs the same algorithm and key for decrypting the message and recovers the plaintext. By this kind of cryptography, it is observable that the key should be known to the sender and receiver. An example about this cryptography is DES [14].
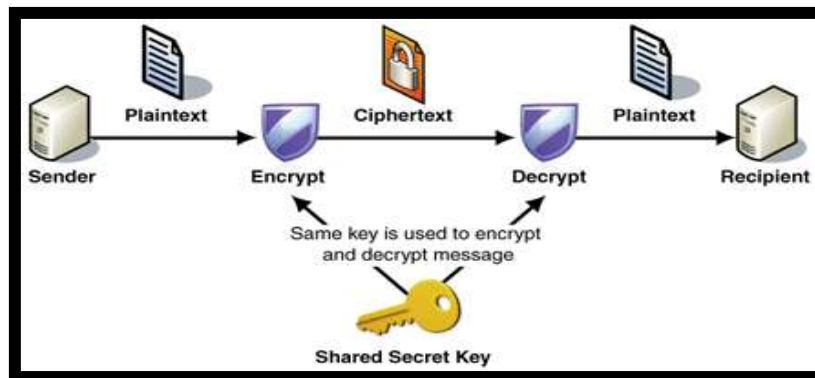
Figure 1.1: Symmetric Cryptography

Symmetric Cryptography can be classified according to the treating way of encrypting a plaintext into the following two types:

a. Stream cipher:- A stream cipher shown in Figure (1.2) encrypts bits independently. This is done by encrypting a bit of a keystream with a bit of a plaintext. RC4 is a popular stream cipher.
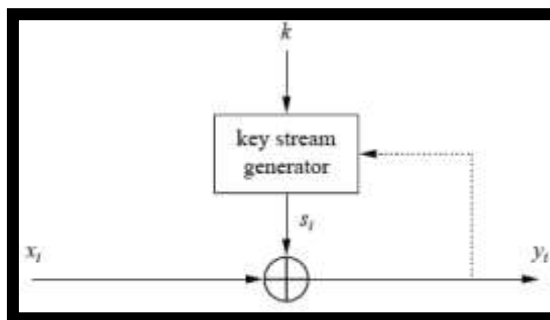

Figure 1.2: Synchronous and Asynchronous Stream Cipher

b. Block cipher: - In a block cipher shown in Figure (1.3), a message is split into a number of blocks, for example, a block with 128-bits length in the AES algorithm or a block length of 64-bits in DES algorithm, and after that each one of the plaintext bit block is transformed into the encrypted block related to cipher bits via a key and algorithm [15].
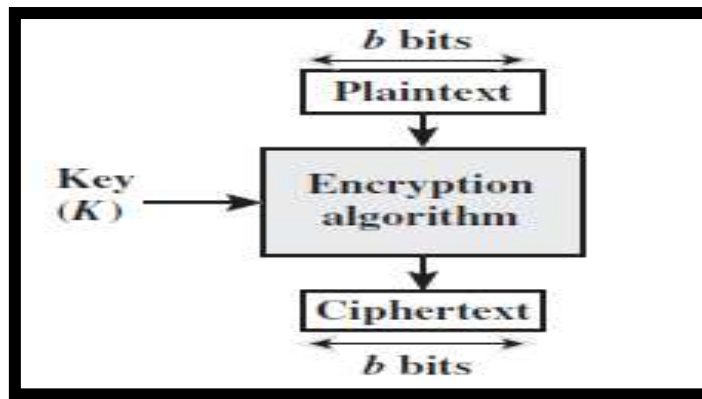
Figure 1.3: Block Cipher

3.1.2.2 Asymmetric Cryptography

In 1976, a totally different type of encryption was produced by Whitfield Diffie, Ralph Merkle, and Martin Hellman. Asymmetric cipher is also called public-key cryptography. In asymmetric cryptography shown in Figure (1.4), the encryption and decryption will be done by two different keys, where just the data which was encrypted via the public key might be decrypted via an identical algorithm and the data that was encrypted via a private key is decrypted by only the same public key. The most known public-key encryption algorithm is the RSA algorithm [16].
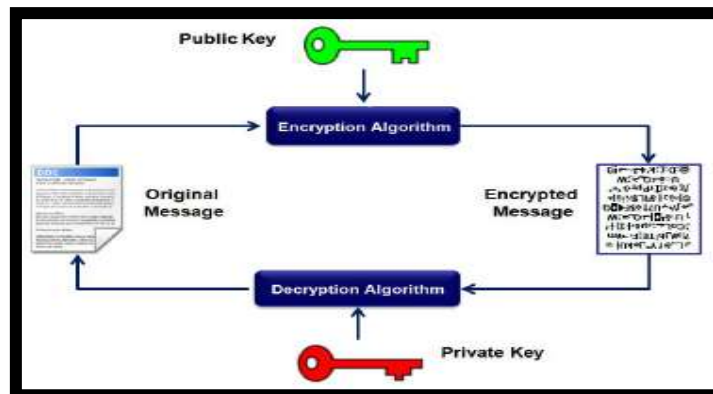
Figure 1.4: Asymmetric Cryptography

4. Chaotic Algorithm

Chaos theory is a branch of non-linear dynamic systems. These dynamic systems with low dimensions have the potential for complex and unpredictable behavior. Here the complexity of determining equations from the source is not a prerequisite for generating random sequences. The short, chaotic system is an overlap between rigid order and unpredictability Probability as described in figure (1.5) Chaos iterative function.
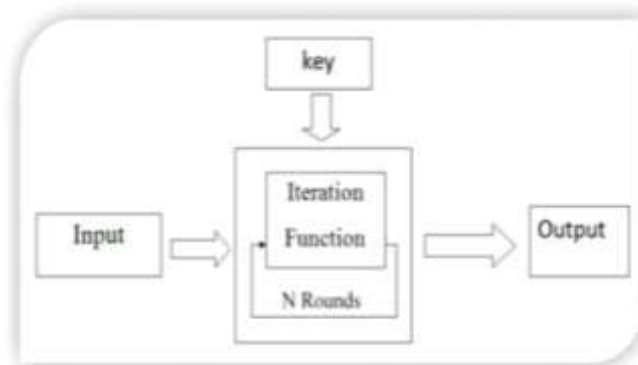

Figure 1.5: Chaos iterative function.

There are a number of definitions of chaos that have some special characteristics to it.

- **Nonlinearity: -** The change in the first element does not affect the change in the first element, and also, the representation can be in a different element or the same.
- **Determinism: -** Here means the possibility of being governed by correct and accurate rules with any element.
- **Sensibility to initial condition:-** means that the resulting final state is completely different because the changes were not mentioned in their initial state
- **Irregularity: -** means that there is chaos in the system.
- **Long-term prediction: -** Because of the initial conditions, the disorder will produce an indefinite long-term forecast.
- **The logistic map: -** The map is a single dimension that gives the parameters of the encryption process and is considered a logistics map Xn + 1 = A Xn (Xn − 1).

4.1 Chaotic Systems

Chaotic systems are non-linear dynamic systems that reveal pseudo-randomness behavior. The Chaotic sequence is created in a simple way through the use of different equations [17].

A concise description regarding a few chaotic systems is provided as follows:

4.1.1 Logistic Map

In the year 1845, Pierre Verhulst suggested the Logistic map, which was a simple and popular chaotic map. Also, the popularity of logistic map was increased when it was used in the year 1979 via the biologist Robert M. May, in which the equation of 1D Logistic map is presented in equation (1):

$$x_{n+1} = a \times x_n \times (1 - x_n) \quad \text{... (1)}$$

In which $x_n \in [0,1]$, x_0 denotes the initial condition, while a represents the constant parameter between 0 and 4. For ($3.5699 < a \leq 4$), Equation (2) shows a chaotic behavior [17]. Figure (1.6) depicts a Logistic map.
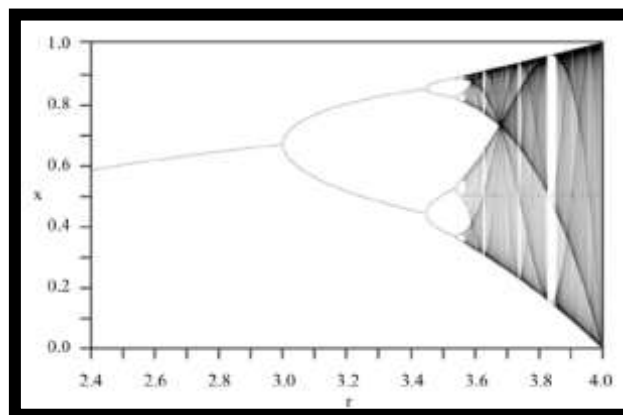

Figure 1.6: Bifurcation diagram of Logistic Map

4.1.2 Hénon Map

Michel Hénon presented the Hénon map, it is considered as 2D discrete-time dynamical chaotic map defined by Equations (2) as follows:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad \text{... (2)}$$

In which (x_n, y_n) and (x_{n+1}, y_{n+1}) are the current and next chaotic states, respectively, where a and b are positive parameters. With regard to the traditional Hénon map, the value of $a=1.4$ and $b = 0.3$, and thus the map exhibits chaotic behavior [18]. Hénon map is shown in Figure (1.7).
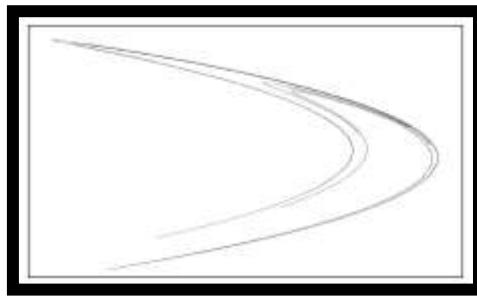

Figure 1.7: Henon Map Attractor

4.1.3 Lorenz System

A professor in MIT, Edward N. Lorenz, introduced the first chaotic system developed via 3-D autonomous equations referred to as Lorenz equation, as can be seen in the equation (3), in his study of weather modeling in 1963 and the chaotic attractor it generates is commonly known as Butterfly Effect .

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \dots (3)$$

Lorenz system shows chaos in the case when $\sigma = 10, \rho = 28$ and $\beta = \dfrac{8}{3}$. Figure (1.8) shows the topology, which looks like a form of a flying butterfly flipping its wings. Thus, it coins the term "Butterfly Effect" [19].
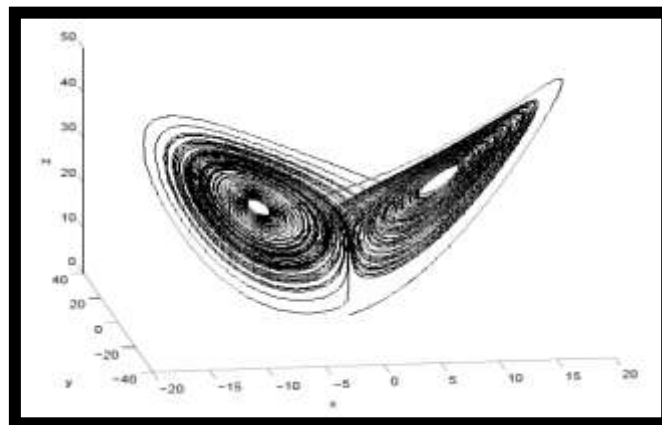

Figure 1.8: Chaotic Attractor of Lorenz Equation

4.2 Chaos and Cryptography

The close association between chaotic systems and cryptography leads to make chaos-based algorithms the best choice for encrypting data. For real-time applications, an encryption scheme that takes lesser execution time but without compromise with the preferable security is desirable. Chaos-based encryption technique is a good mixture of security, high speed, and less power consuming [20].

The properties related to chaotic systems, like sensitivity to initial conditions and parameters, randomness, have attracted the interest of researchers since such properties indeed fulfill the vital principles of cryptographic algorithm design. Take advantage of these favorable features, chaos-based algorithms have revealed superior characteristics in complexity and security [20].

In 1989, Matthews, a British mathematician, firstly employed chaos for encryption, suggesting a novel encryption algorithm generating key streams on the basis of Logistic map and encrypting the information by stream cipher method [21]. In 1998, Fridrich Scharinger suggested the first chaos-based image encryption algorithm with diffusion and confusion design, which were two significant characteristics of a secure cipher as indicated via Claude Shannon in his masterwork "*Communication Hypothesis of Secrecy Systems*" [22].

5. PROPOSED METHOD ARCHITECTURE

The work with the proposed method begins when a user encrypts Image. In the first stage, choose Image. In the second stage, the encryption, in this stage encryption image is implemented by the chaotic algorithm. Image encrypted is decryption using the chaotic algorithm to restore the original image Figures (1.9) and show the process according to the proposed method.
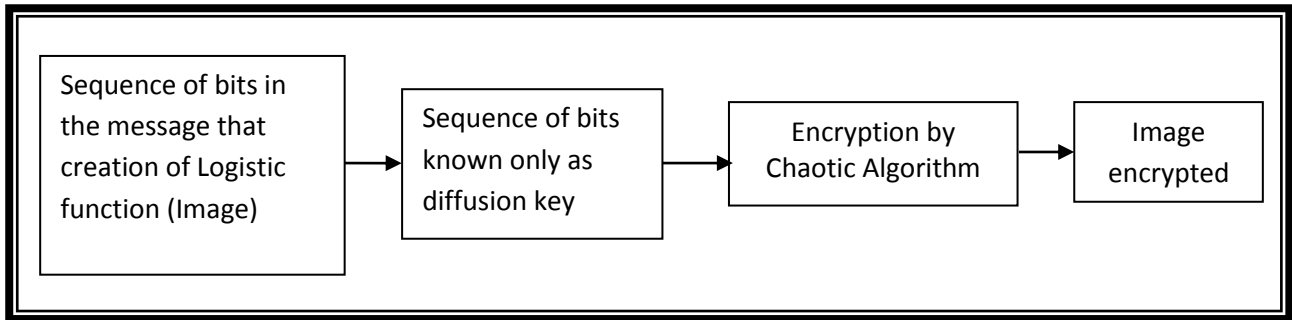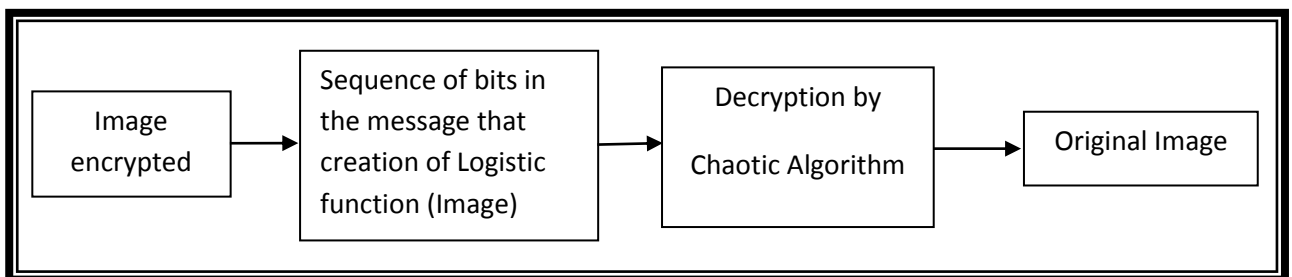

Figure 1.9: Encrypted Image Process.

Figure 1.10: Decrypted Image Process

6. The Suggested Technique for Encryption and Decryption Image

This section will illustrate the proposed method for encryption and decryption images. As can be seen in Figure (1.11) and Figure (1.12) of the General Algorithm.

Input: Massage (Original Image)
Output: Massage (encrypted image)
Process:
Step1: Read Original Image
Step2: Perform chaotic algorithm of original Image
Step3: Resultant Image is encrypted Image.
Step4: End.

Figure 1.11: General algorithm of Proposed *Method* (Encryption image process)

Input: Massage (encrypted image)

Output: Massage (Original Image)

Process:
Step1: Read Encrypted Image.

Step2: Perform chaotic algorithm of encrypted Image for decryption.

Step3: Perform operation to extra the original Image using chaotic algorithm.

Step4: Resultant Image is the original Image.

Step5: End.

Figure 1.12: General algorithm of *Proposed Method* (Decryption image Process)

7. THE IMPLEMENTATION

With regard to the presented study, implementation of the suggested approach is made according to Algorithms (1.11); the proposed method attempts to improve the performance of secure Image will be described in the following example the main interface of the proposed system shown in figure (1.13).

When the user likes to send encrypted Image will using the proposed method will depend on steps in the algorithm (1.11), which describes the sending process as in the following example:

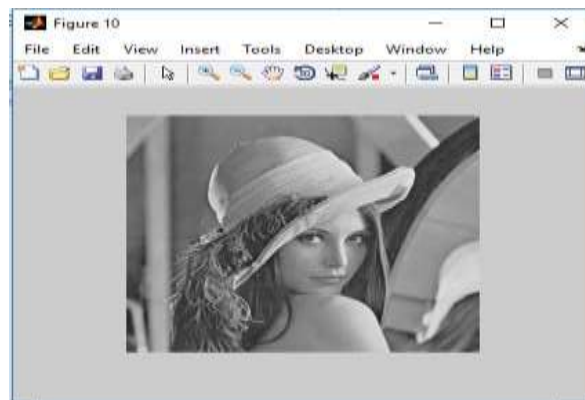**Step1**: Choose the loaded by the user encryption as shown in Figure (1.14).

Figure 1.14: Load Image for Encryption

Step2: The result of encryption is Image encrypted, as shown in figure (1.15).

Figure 1.15: Encrypted Image using XOR Method

Step3: To decrypt the Image, we simply take the encrypted Image using a chaotic algorithm. This yields the original Image, as shown in figure (1.16).
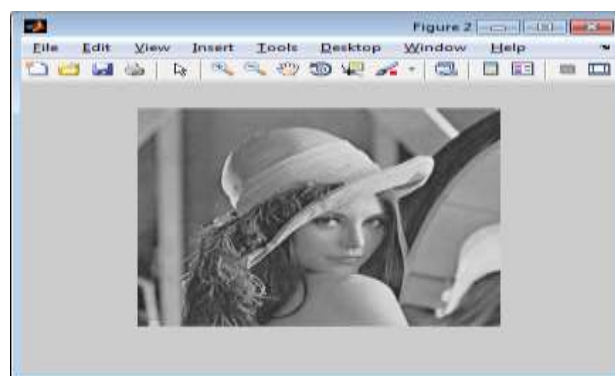

Figure 1.16: Decrypted the Image.

Step5: End.

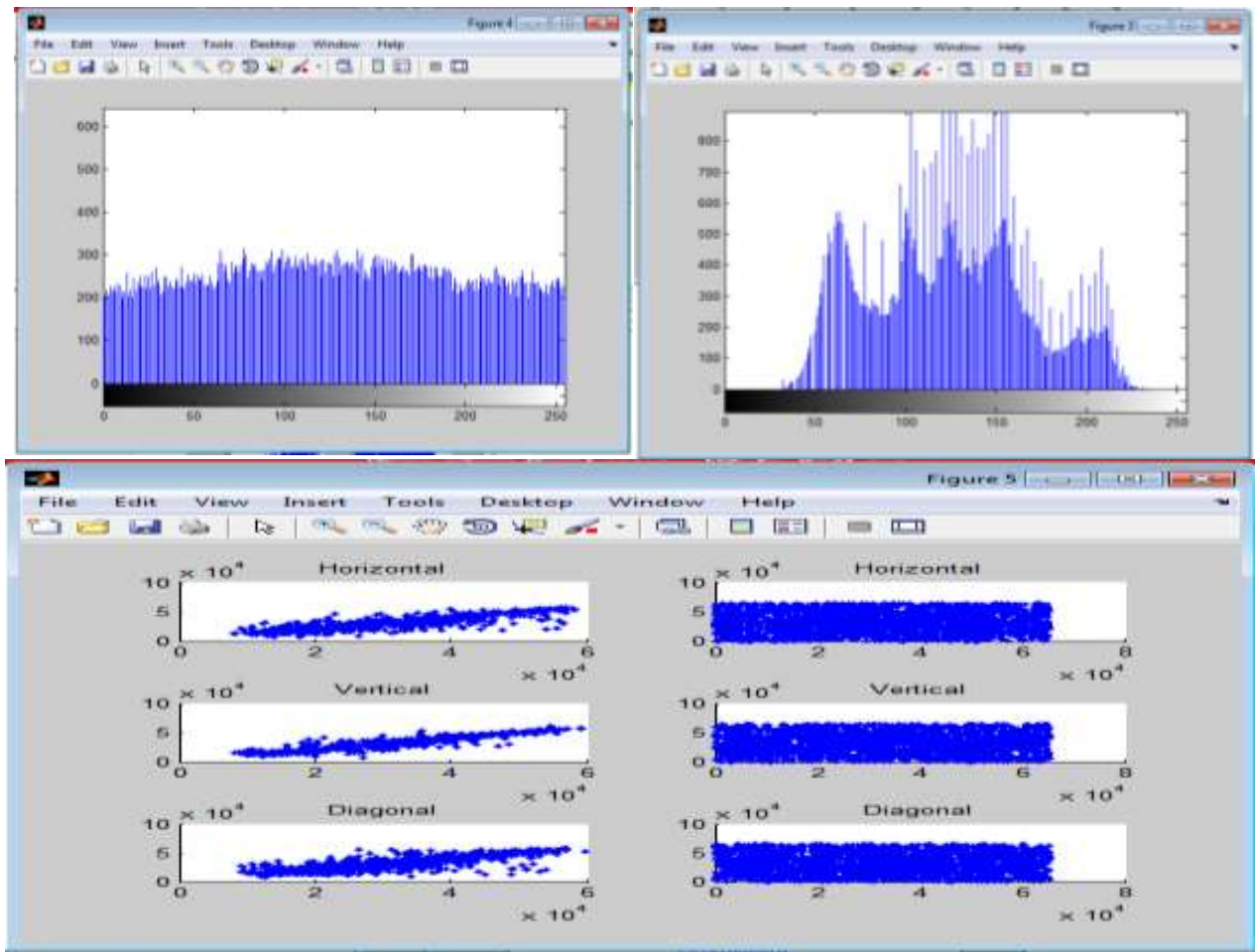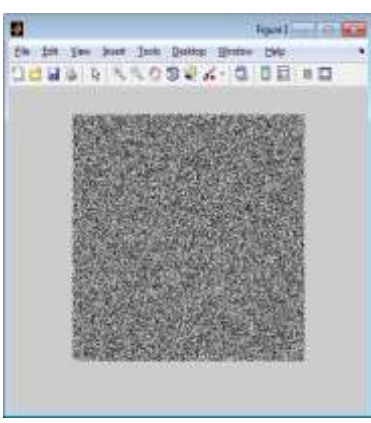After encryption, the image histogram is shown in figure (1.17).

Figure 1.17: Histogram for the Image

In figure (1.18) will show other examples from Image for encryption and decryption based on the chaotic algorithm.

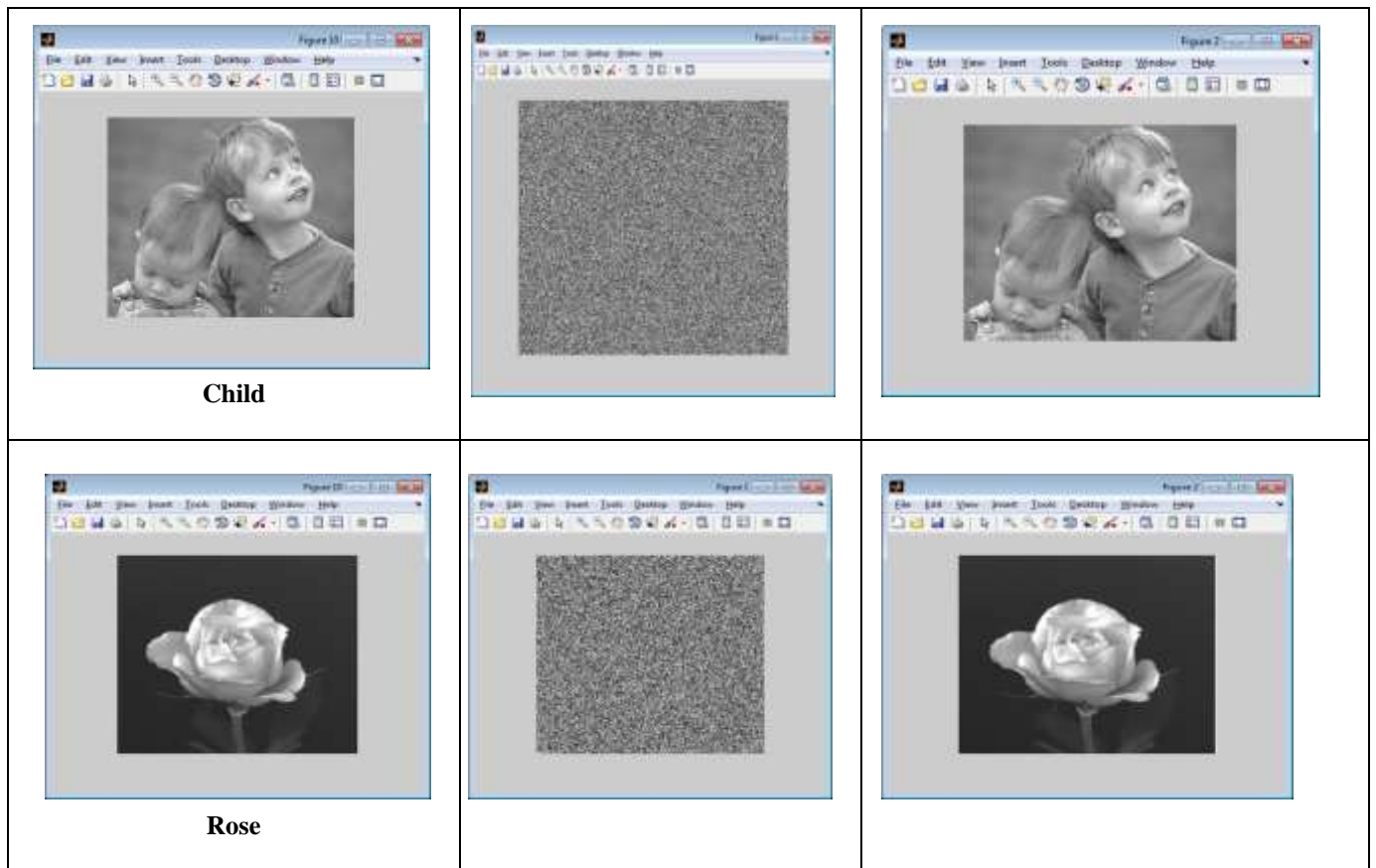| Image Name	Image encrypted	Original Image
Penguins		

Figure 1.18: Encryption and Decrypted Images

After applying the proposed system and calculate the performance measures for each system by encryption image and after the encryption process using both methods (Entropy test, cross-correlation, PSNR) can be obtained on the data described in the tables below, which show that the proposed system is efficient and the results we obtain are more accurate.

Table (1.1): Shows the quality measures for the images after application (PSNR & MES) measures.

Image	Elapsed time	E	CC	PSNR
Lena.	0.672144 seconds	7.9919	- 0.0034	99
Penguins	1.709086 seconds	7.9980	- 0.0031	99
Child	0.772039 seconds	7.9853	049.948-	99
Rose	0.950084 seconds	7.9800	- 0.0058	99

ACKNOWLEDGMENT

CONCLUSIONS

The following are the conclusions derived from this work:

1. The novel scheme of image encryption is developed. An adequate chaotic map preserves the chaos properties following selecting the discretization. With regard to the presented work, such approaches were used in various images, yet such techniques might be effectively utilized for other digital images, yet the newly achieved encryption levels depend on the key image selection.
2. Through selecting a high-dimensional chaotic system, there will be an increase in the key space. Also, the complex non linearity is preserved through selecting adequate chaotic maps. Furthermore, repeated permutations were prevented, yet the pixel values were changed via the diffusion function.
3. Some security analyses have been conducted on the novel algorithm, and simulation results showing the decryption and encryption were good, and the algorithm shows good robustness and security.
4. The suggested encryption approach in the presented work was tested on various gray images of 256*256 and presented excellent results.

REFERENCES

1- https://sisu.ut.ee/imageprocessing/book/1
2- https://images.app.goo.gl/NhTtQ1PZAmfvNdTKA
3- https://www.google.com/search?q=What+is+image+processing+and+its+types%3F&sa=X&ved=2ahUKEwiP_MTlrXoAhWLUhUIHQHZATMQzmd6BAgLEAs&biw=1366&bih=657
4- https://books.google.iq/books?hl=ar&lr=&id=T82qCAAAQBAJ&oi=fnd&pg=PR9&dq=What+is+image+processing+and+its+applications%3F&ots=5SubYcOMO&sig=_za6bT4TZ_iOsf8iqmJvYwkQxFY&redir_esc=y#v=onepage&q=What%20is%20image%20processing%20and%20its%20applications%3F&f=false
5- https://www.geeksforgeeks.org/image-formats/
6- Mahmoud Mohammad Maqableh, "Analysis and Design Security Primitives Based on Chaotic Systems for eCommerce", Ph.D. Dissertation, Durham University, School of Engineering and Computing Sciences, United Kingdom, 2012.
7- A. Prusty, A. Pattanaik and S. Mishra, "An Image Encryption and Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map and Henon Map", International Conference on Advanced Computing and Communication Systems (ICACCS -2013), IEEE, Coimbatore, INDIA, Dec. 19 – 21, 2013.
8- Gary C. Kessler, "An Overview of Cryptography", 17 November 2006, Available at: http://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf.
9- B. Rajan, "Independent Domain of Symmetric Encryption using Least Significant Bit ", M.Sc. Thesis, University of Dalarna, Computer Engineering, 2011.
10- Chong Fu et al., "A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy, 16, 2014.
11- Ali Abdulgader et al., "Enhancement Of AES Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption", Journal of Theoretical and Applied Information Technology, Vol. 71, No.1, January 2015.
12- Mahmoud Mohammad Maqableh, "Analysis and Design Security Primitives Based on Chaotic Systems for ecommerce", Ph.D. Dissertation, Durham University, School of Engineering and Computing Sciences, United Kingdom, 2012.
13- Mahmoud Maqableh, "A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map", Journal of Software Engineering and Applications, 8, December 2015.
14- Mahmoud Maqableh, "A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map", Journal of Software Engineering and Applications, 8, December 2015
15- A. Prusty, A. Pattanaik and S. Mishra, "An Image Encryption and Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map and Henon Map", International Conference on Advanced Computing and Communication Systems (ICACCS -2013), IEEE, Coimbatore, INDIA, Dec. 19 – 21, 2013.
16- A. Prusty, A. Pattanaik and S. Mishra, "An Image Encryption and Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map and Henon Map", International Conference on Advanced Computing and Communication Systems (ICACCS -2013), IEEE, Coimbatore, INDIA, Dec. 19 – 21, 2013.
17- Clyde-Emmanuel Estorninho Meador, "Numerical Calculation Of Lyapunov Exponents For Three-Dimensional Systems Of Ordinary Differential Equations", M.Sc. Thesis, Marshall University, 2011.
18- Clyde-Emmanuel Estorninho Meador, "Numerical Calculation Of Lyapunov Exponents For Three-Dimensional Systems Of Ordinary Differential Equations", M.Sc. Thesis, Marshall University, 2011.

19- Chong Fu et al., "A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy, 16, 2014.

20- Ashwin Raman, "Parallel Processing of Chaos-Based Image Encryption Algorithms", University of California, Irvine, 2016

21- J. Vahidi, "The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos", Journal of mathematics and computer Science, Vol. 9, Issue 4, 2014.

22- J. Vahidi, "The Confusion-Diffusion Image Encryption Algorithm with Dynamical Compound Chaos", Journal of mathematics and computer Science, Vol. 9, Issue 4, 2014.