I. J. Computer Network and Information Security, **2023, 1, 64-80**
Published Online on February 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.01.06

A Secure and Efficient Cryptography System Based on Chaotic Maps for Securing Data Image in Fog Computing

Samaa Y. Tarabay*
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: Samaayasser92@gmail.com
ORCID iD: https://orcid.org/0000-0002-6926-2346
*Corresponding Author

Abeer Twakol
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: abeer.twakol@mans.edu.eg
ORCID iD: https://orcid.org/0000-0003-4223-2144

Ahmed S. Samrah
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: shmed@mans.edu.eg
ORCID iD: https://orcid.org/0000-0003-1801-5895

Ibrahim Yasser
Mansoura University / Communication and Electronics Engineering Department, Mansoura, 35516, Egypt
E-mail: ibrahimyasser14@gmail.com
ORCID iD: https://orcid.org/0000-0001-5411-2567

Received: 07 September 2022; Revised: 20 October 2022; Accepted: 29 November 2022; Published: 08 February 2023

Abstract: The huge availability and prosperity of net technology results in raised on-line media sharing over the cloud platform which has become one of the important resources and tools for development in our societies. So, in the epoch of enormous data great amount of sensitive information and transmission of different media transmitted over the net for communication. And recently, fog computing has captured the world's attention due to their inherent features relevant compared to the cloud domain, but this push to head for many issues related to data security and privacy in fog computing which it's still under studied in their initial juncture. Therefore, in this paper, we will review a security system that relies on encryption as a kind of effective solution to secure image data. We use an approach of using chaotic map plus space curve techniques moreover the confusion and diffusion strategies are carried out utilizing Hilbert curvature and chaotic map such as two-dimensional Henon map (2D-HM) to assert image confusion with pixel level permutation. Also, we relied in our system the way of shuffling the image with blocks and use a key for each block, which is chooses randomly to have a high degree of security. The efficiency of the proposed technique has been tested utilizing different investigations like analysis of entropy [7.9993], NPCR [99.6908%] and finally UACI [33.6247%]. Analysis of results revealed that the proposed system of image encryption technique has favorable effects, and can achieve a good result moreover it fights different attacks and by comparing with another techniques denote that our proposed fulfills high security level with high quality.

Index Terms: Cryptography, Chaotic System, Securing Data, Fog Computing, Image Security.

1. Introduction

The expansion of the Internet of Things (IOT) has led to mass production Data, with massive computing resources, storage space and communication bandwidth. The IOT realizes the interconnection of mature technology equipment from home to vehicle and workplace [1]. So, the term fog computing has emerged as horizontal intermediate layer

between a cloud data centers and IOT devices that distributes storage, computing and data processing nearer to the end users [2]. Fog computing was first introduced by cisco and by pooling available computing, storage, and network resources at the edge of the network, service delivery is closer to the end user [1, 3]. It is a decentralized computing infrastructure, using one or more IOT collaborative execution on devices or edge devices close to the user a lot of communication, control, storage and management. Through the fog node and equipment, fog computing can reduce processing burden Resource-constrained equipment meets latency requirements delay sensitive applications and overcome bandwidth constraints of centralized services [4].In addition to it, fog computing also provides; (1) support for high mobility, (2) high responsiveness computation resources, (3) different communication protocols, (4) multiple data sources and devices can be integrated and moreover heterogeneity of interface within infrastructure, and (5) interoperability which must be able to interoperate and cooperate with different providers with wide range of services and effortlessly support certain services [5].

However, fog computing has not overcome the threats and security weaknesses that it is still exposed to in its system, which may have a significant impact on the system behavior and its exposure to breach and data exposure to repeated risks due to the lack of permanent stability against security issues, and therefore it is necessary to provide the most Effective solutions that resist these security issues, reduce risks to devices, and provide a strong and secure medium for data [1]. “Fig. 1,” shows fog computing architecture.

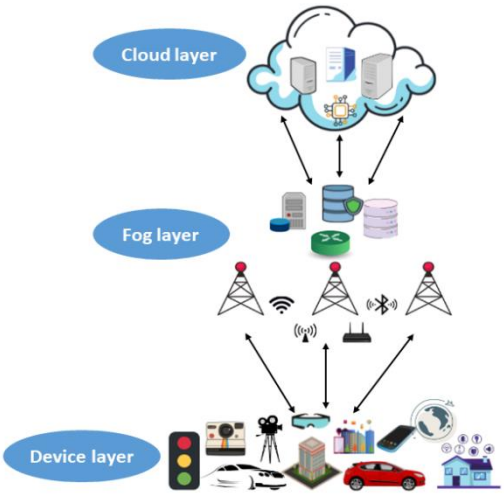


Fig.1. Fog Computing Structure Graph.

Digital image measures utilized in many applications as medical image, and image knowledge base of this digital image have to be compelled to be defend from unauthorized. A significant amount of this data image is private and should remain confidential between the exchanging parties, therefore, most of the ISP's reliance is on encryption and decryption techniques [6]. However, as a result of unlawful wiretapping, revision, or interception, there's a visible lack of security for communication images over the network, significantly [7-9]. Moreover, there're numerous means and tracks in which to emphasize the transference of secured data that compared to other strategies to ensure the safety of images as in medical field as one of the important areas against unauthorized access [7, 9].

Chaos- based secret techniques are thought of to be the foremost necessary because the wonderful features of chaotic system which can pledge the speed and high security [10]. Chaos-depended techniques have lately turn into appealing for shielding image content. Chaotic systems are sensitive, non-liner, deterministic and easy to reconstruct after filling in the image. Use their topmost characteristics like management control parameter, sensitivity to the initial condition, and non-convergence during a chaotic system (or map). Several schemes of image encryption have been proposed using Chaos and their worthiness has been partially demonstrated [11]. The overview of the related work revealed that chaotic systems have been exploited for efficient for multimedia data encryption. In cryptography, having a secure routing is needful to cross data through a secure lines and networks. Chaotic cryptosystem is one of the methods are thought of to be to be one of the essential element necessary because the effective properties of chaotic system which is sensitive, non-liner, deterministic and easy to reconstruct after filling in the image [9].Image encryption process can be categorized as i) position permutation, ii) value transformation. In the first technique it happens permutation for the image position with no changing in the pixel value of the image, and in second technique pixel value is substituted by another with no changing in the image position [12].

2. Related Works

Lately a lot of research represent many schemes of image encryption which is used the cryptosystem of chaotic theory to obtain the strength and the preferable image encryption techniques, here, we will explain and mention some of the research that was presented and received interest in this part. Arwa et al. [13], proposed a technique which based on

pixel shuffling starting by converting the pixel value from a three-dimensional value (R, G, B) to 1D, then generate a row vector from image pixel and make a random permutation of row vector. XOR operation is obtained and finally 3D chaotic map is performed, it is limited by losing some data in the decryption process because of using 3D value of image in encryption steps and restored with 1D value in decryption stage. Yasser et al. [10] suggested hybrid method which the chaotic maps are combined, the author based on the technique of Discrete Wavelet Transform (DWT) and disband the image it to sub-bands. Both confusion and diffusion have procedured in the system. Assorts of chaotic maps types could be related to the image to enhance the encryption process. In recent period a lot of authors are turning to the field of using DNA technique, Shuqin et al. [14] characterized an algorithm that is depend on 5D continuous and chaotic system hybrid type, which adopts DNA dynamic coding mechanism and scrambling process with two rounds of diffusion encryption structure to enhance the security, the weakness point that the ability of cipher text to resist noise, cut and compress attacks is weak , also the more dimensional process used the more complexity and heavy cost will be. Many research has been proposed algorithms depend on scan patterns techniques. Mura Mural, P et al [15] designed a scheme based on Space Filling Curve that make the image scrambled using the mechanism of square wave to obtain confusion with many orders and diffused as well using saw-tooth technique with some various orders. The author doesn't use any chaotic equation or system in his proposed system to achieve confusion and diffusion. Another scheme for image encryption, Zhang, Xuncai, et al [16] this algorithm used a scheme of cryptography that depend on hybrid of Hilbert curve and H-fractal to realize the techniques of confusion and diffusion that achieved scrambling and value exchanging operations. In this work the sequence generator is based on both the piece-wise linear chaotic map (PWLCM) and Rossler chaotic. Shahna, K. U.et. al [17] proposes an encryption technique using Logistic map and Z-order curve, pixel scrambling is performed using Z-order curve and random matrix is generated using Logistic map and the results show us that the system does not have a high quality of security and vulnerable. Fu, C.et. al [7] suggested a technique which is bit permutation to overcome the drawbacks of conventional permutation-only type image cipher a significant diffusion effect in permutation procedure through a two-stage bit-level shuffling, scheme has a comparable security level and a much lower computational complexity.

Raza, et. al [18] used a new approach mixing the chaotic system and the method of z-order technique through 3D puzzle. The author achieved the confusion and diffusion mechanism with bit permutation. The analysis of the npcr & uaci is higher as well as the execution timing is somewhat low enough. Also Ahmad Pourjabbar Kari, et al [19] designed an algorithm which is based on hyper chaoty state, the confusion is subject to Arnold's cat map while the diffusion is achieved through the interchange operation using the types of sine, tent and logistic map. The scheme need to improve to be more reliable and practical cryptographic applications. Moreover Farah, M.A Ben et al. [20] propose a new image encryption based on a new optimized substitution box, it's generated function through the mechanism of chaotic jaya, confusion and diffusion obtained in the scheme, the effect of changing the chaotic property on the system strength and rigidity could be studied for achieving more enhancement, moreover it might be visualized by handling and manage the keys in various protocols.

3. Problem Statement

As it was mentioned previously, the encryption of data images is one of the most important issues that must be highlighted and worked to improve and develop in a superior manner, so we are trying to develop a solution to establish a secure and effective encryption system. The major purpose of our project is providing an effective and powerful mechanism to secure image data through an encryption system based on chaotic maps that has results of high sensitivity and quality level, moreover the used of scan patterns properties as the results based on this work showed the effectiveness of the system and its impact on encryption and the difficulty of being exposed to the attacks.

Usually, the cryptography processes which depend on chaotic techniques consists of two main ways includes confusion and diffusion, scrambling is the core meaning of confusion stage, the one that handle with pixels position, while diffusion technology is a technique for pixel value changing and diffuse pixels that has impact of changing the values of another pixel. And here in our proposed algorithm we use a hybrid between both confusion and diffusion in order to enhance and have a high quality of security system. To realize the scrambling operation, we use the Hilbert curve, as considered as popular and it's widely used in many applications because of its continuity as a continuously mapping, scalability and stability as the level increases, the distance of each point on the graph will become smaller and smaller, and as the level increases, the graphics will become more and more the larger, the point movement becomes no longer important. So, it can be regarded as no movement. Besides that, it's worth for mention that Henon map is a good chaotic map that its trajectory of it is simple and have something determined, thus the maps can be easily predicted with super quality plus it has superior features in generating perfect random sequence with regularly and constant allocation. The proposed system ensures high quality of resistance with better security cryptosystem due to both confusion and diffusion technology through two times of scrambling, once for pixel permutation, and another for value permutation using cyclic bit shifting technique. Now we can define the main and effective contributions of this paper in an understandable and summary form:

- The proposed system in our work uses bit permutation for realizing diffusion and the confusion can be actioned through applying pixel permutation mechanism.

- In this scheme, the Henon chaotic map is 2D which is more efficient and used for the generation of permutation sequences for realizing diffusion.
- The Hilbert curve is used for the generation of masking sequences for realizing confusion.
- The approached work proved that cipher image with high keys sensitivity with any changes in the original image.
- The outcome of the proposed algorithm is compared with existing results and validated by different cryptanalysis through many performance evaluation metrics that are usually used to evaluate the efficiency of image encryption approaches.

There are some experiments, tests and comparisons that are presented to prove the performance of the proposed system algorithm.

The residuum of this paper is orderly as follows: Section 4 shows flowchart of the proposed system and the proposed approach fully explained below in "Fig. 2," Section 5 and section 6 discusses the results and the analysis of our results. Conclusion and future works are given in Section 7.

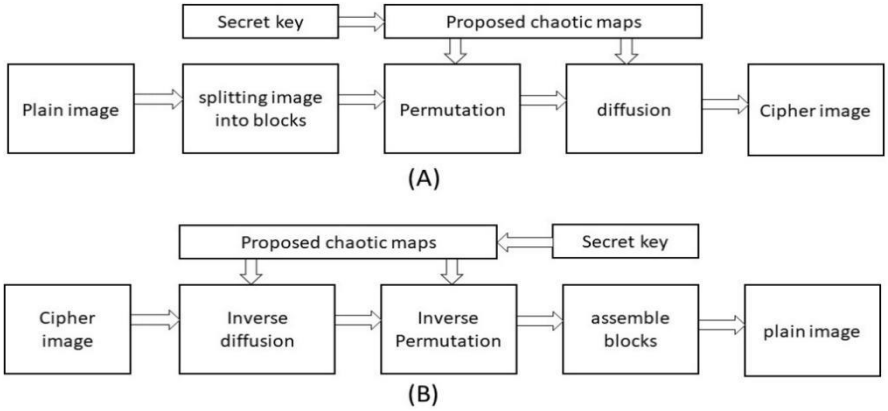


Fig.2. Proposed System Flowchart.

4. Block Diagram of the Proposed System

4.1. Hilbert Scrambling (Space Filling Curve)

The Hilbert curve is a continuous fractal space-filling curve first described by the German mathematician David Hilbert in 1891 [16]. Hilbert curve is used to make a shuffling process of the pixels position of the original image to get a new scrambled image. According to the characteristics of its own space filling curve, the Hilbert curve can linearly traverse each discrete unit in two dimensions or higher dimensions, and only traverse once, and linearly sort and code each discrete unit, which is the only one of the unit Logo. Since the Hilbert code does not have a large step jump, the aggregation performance of the Hilbert space arrangement is better, that is, the adjacent points on the Hilbert curve must be adjacent in the original space. The Hilbert curve is an FASS curve, that is, space-filling, self-avoiding, self-similar, and simple one. These curves are situated in a Euclidean space and have a dimension higher than 1 and have non-hollow internal in the space [16].

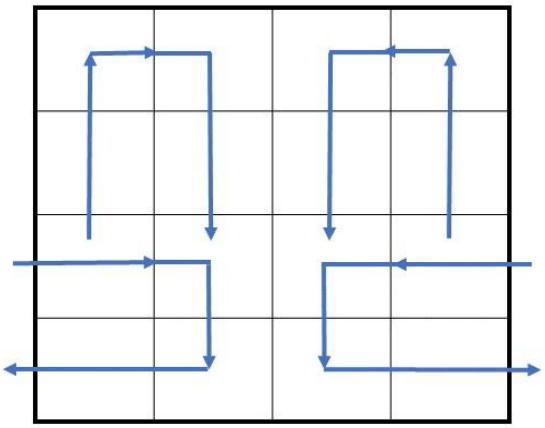


Fig.3. Process of Hilbert Scrambling 4x4.

Now we will discuss the first iteration / order of Hilbert curve: the main square is splatted into four parts each part is as mini square starting the curve from the square's center in the southwest then to the square's center in the northwest corner heading to the square's center in northeast ending to the square's center of southeast, here we finished the main cycle, The places of the beginning stage and the ending point of the Hilbert curve refer to the direction of it [16], "Fig. 3,"refer to the description of Hilbert curve process.

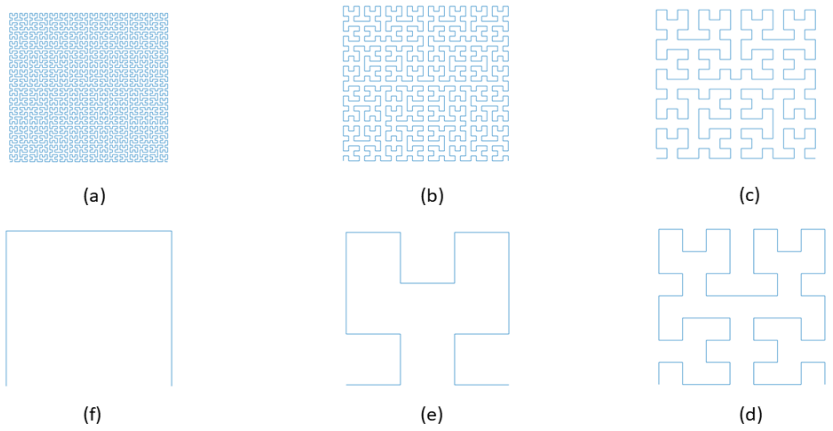


Fig.4. Hilbert Curve Shapes where Fig (a) Refer to Order 6, Fig(b) Refer to Order 5, Fig (c) Refer to Order 4, Fig (d) Refer to Order 3, Fig (e) Refer to Order 2, Fig (f) Refer to Order 1.

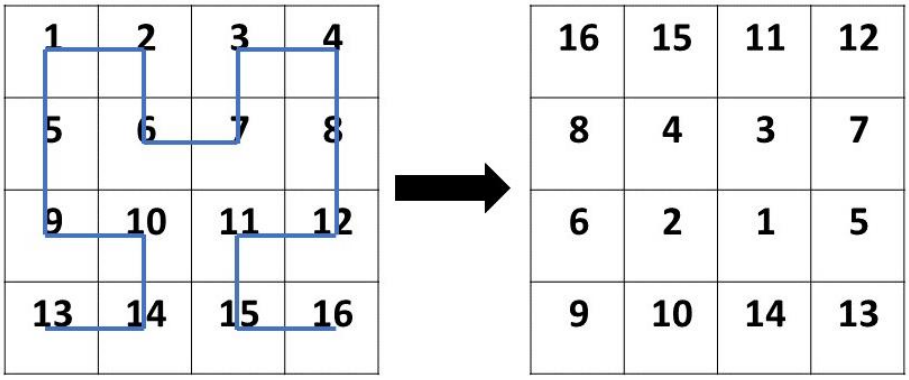


Fig.5. Example of Hilbert Scrambling with Order 2.

4.2. Henon Map

It is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior [21]. The Henon map takes a point (x_n, y_n) in the plane and maps it to a new point. The map was introduced by Michel Hénon as a simplified model of the Poincaré section of the Lorenz model, using the following equations: -

$$x_{n+1} = 1 - \alpha x_n^{\,2} + y_n \tag{1}$$

$$y_{n+1} = \beta x_n \tag{2}$$

There're two main parameters the Henon map is based on, for the standard Henon map have values of $\alpha = 1.4$ and $\beta = 0.3$. For these classical values the Henon map considered as chaotic, the graph of this map is obtained in "Fig. 6," Also the simulation of Henon bifurcation map of a chaotic diagram is shown in "Fig. 8& 9,". Bifurcation diagram plots output sequences of a chaotic map along with the change of its system parameter(s) [22]. From the bifurcation diagram in "Fig. 8&9," it is clear that Henon map is chaotic for the range of parameter (a) $1 \in [1.06, 1.22] \cup [1.27, 1.29] \cup [1.31, 1.4]$ [22]. Moreover, Chaotic motion is very sensitive to initial conditions and lyapunov gives a set of values called (λ) where one of the values of it must be positive and this means that the system is chaos and has a chaotic movement as we see in "Fig. 7," when the chaotic system is extremely very small in two different differential its motion path progressively generates indicator separation.

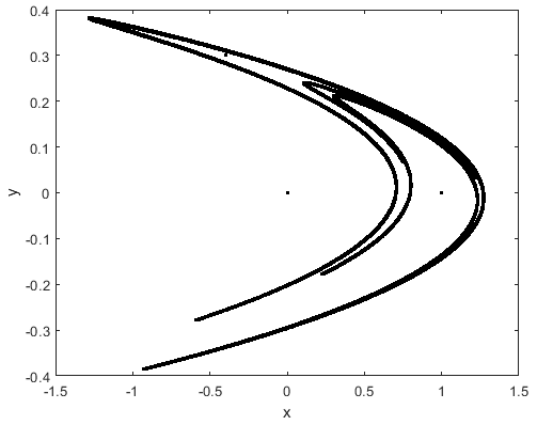


Fig.6. Henon Map with α = 1.4 and β = 0.3.

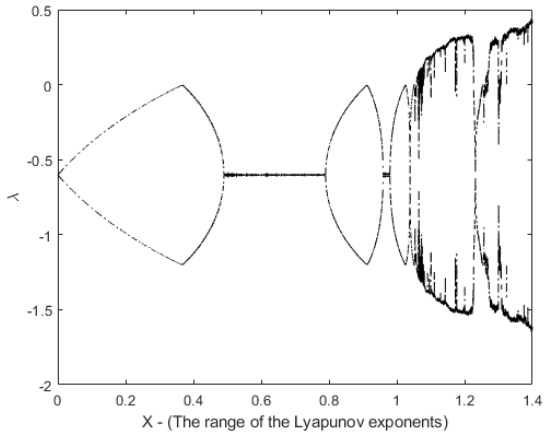


Fig.7. Henon Map Lyapunov Diagram.

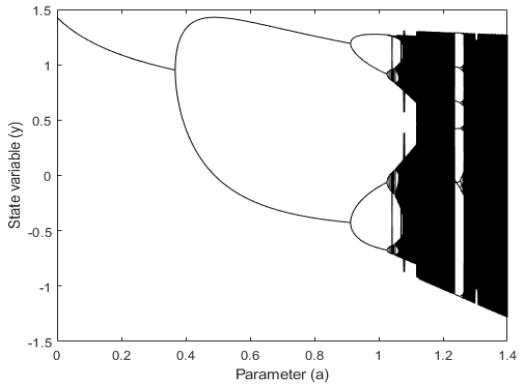


Fig.8. Henon Bifurcation Map x Component Component.

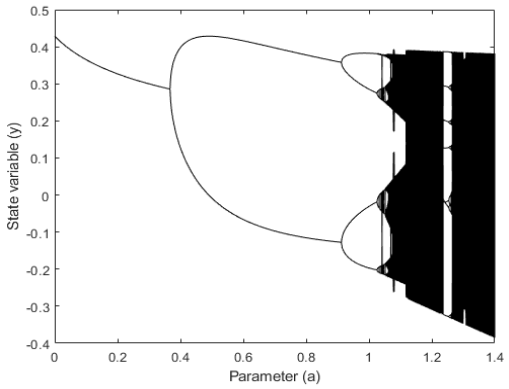


Fig.9. Henon Bifurcation Map y Component.

4.3. Encryption Algorithm Steps

The proposed cryptosystem starts with dividing the plain image into blocks then shuffling the pixels of this blocks indices with Hilbert maps key generation, then these shuffles blocks goes through two further encryption steps to strengthen algorithm, the first step is scrambling the images in a confusion process using the key generation of Hilbert scan then the diffusion step which takes the output of the confusion step and performs pixel value alterations based on the Henon map, the Henon maps follows the Henon formulas for generation of the keys the diffusion performs the encryption by altering the current pixel value based on the previous pixel to create a more robust encryption. The decryption process is done by a process of reversing all the previous steps in the encryption process to get the original image again and perform all the steps in order to get the original version of the data as we see below in details:

Our Proposed Algorithm Procedure:

1-Read the plain image (PI) with the size (W × H) where W and H respectively, are width and height of the plain image pixels.

2-Splitting the plain image (PI) into blocks.

3-Shuffling the blocks by Hilbert key generation.

4- Generating "Henon key" for each block separately as in the following: -

$$\left.\begin{matrix} a1 = 0.00000012547 \\ b1 = 0.00006122 \end{matrix}\right\} \longrightarrow \text{Initial values of Henon map}$$

Popularize parameters with introducing their initial values: -

$$a_1 = 0.000001235544789, \hat{b}_1 = 0.003578891472566, u = 73834772913855, p = 71277967533485$$

Now upgrading values by these following equations:

$$u = u + floor(e^{2\Pi} * 10^5) \tag{3}$$

Here we get:

$$S1 = \frac{u * 256}{\sqrt{v}} - e^{2\Pi} \tag{4}$$

$$p = p + floor([S1] * 10^5) \tag{5}$$

Here we get:

$$S2 = ((x_1 * 10^7) - floor(x_1 * 10^7)) \tag{6}$$

which;

$$a_1 = a_1 + ((S1 - floor(S1)) * 10^{-5}) \tag{7}$$

$$b_1 = \hat{b}_1 + \frac{S2}{\Pi 10^2} \tag{8}$$

- The new values of a_1 & b_1 is presented for repetition henon map (t=500).
- Now, two chaotic sequences is obtained x , y.
- Through the upgrading of a_1 & b_1 , process the chaotic sequence to get sequences of C1 & C2 by the equations below:

$$C1 = [C1, round(\text{mod}((x^2) - floor(x^2) u * 10^9, 255) + 1)] \tag{9}$$

$$C2 = [C2, round(\text{mod}((y^2) - floor(y^2) p * 10^9, 255) + 1)] \tag{10}$$

$$x = 1 - \alpha x^2 + y \tag{11}$$

$$y = \beta * y \tag{12}$$

- Then we get the two Henon keys:

$$Key1 = (C1(t+1end), [M, N]) \tag{13}$$

$$Key2 = (C2(t+1end), [M, N]) \tag{14}$$

Which [M, N] is considered as key size.

5-Then the scrambling step:

1) First according to the Hilbert curve mechanism set up the Hilbert pattern due to the description that mentioned above, "Fig. 4," shows the different orders of Hilbert scrambling curve. ii) second iterate every pixel in the shuffled image from the step 3 in order to get the whole bits and represented in a matrix form (Matrix A), iii) third as the same way of second step, recur the values of the key1 in "(13)," and represented in a matrix form as the size of the key1 (Matrix B).

Now, carry out circular shifting for the pixels of both (Matrix A & Matrix B), "Fig. 10," refer to an example of shifting bits process mechanism.

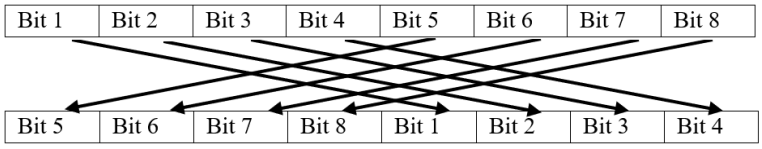


Fig.10. Example of Shifting Bits Process Mechanism.

6-here we get the confusion form of the encrypted image using Key1 and represented a new matrix after completing several procedures on the image to obtain an opaque version that does not have any clear features, let's named it by (IMG).

7-The key2 which is generated in "(14)," is used in this step which is called diffusion step.

$$G1 = [\mathrm{mod}\, IMG + U + V, 255] XORKey2(1)] \tag{15}$$

$$G1_{i+1} = \{\mathrm{mod}\, G1 + IMG_{i+1} + V, 255] XORKey2_{i+1]} \tag{16}$$

Where: i=1,2,…

8- Now, after the final encryption process, the decryption on the other hand reverses all of these steps backwards, it starts by inverting the diffusion step using the same key used for encryption, then it reverses to the encryption step and restores the pixels indices caused by confusion using the same Hilbert maps as in the encryption step and finally assembling the blocks to return to the plain version of the data.

$$IMG = \mathrm{mod}[XORG1(1), Key(1) - r - v)255] \tag{17}$$

$$IMG_{i+1} = \mathrm{mod}[XORG1_{i+1}, Key2_{i+1} - G1(1) - r, 255] \tag{18}$$

5. Performance Metrics

There are some performance measures that we use to get to know the impact of the proposed system and its effectiveness in achieving the best expected results from its performance, through some several parameters which cover the statistical, differential and efficiencies metrics.

5.1. Histogram Analysis

This histogram is a graph that describes the graphical representation of the image and it is showing the number of

pixels in an image at each different intensity value found in that image [20].

5.2. Correlation Analysis

Correlation measures the degree of matching between two adjacent pixels of an image [23]. For the image in naturally, there is usually a high degree of correlation in most cases Due to pixel continuity, adjacent pixel pairs [24]. The following equation used for correlation calculation coefficient, the correlation of the original and encrypted images of our proposed system:

$$r = \frac{\sum_{i=1}^{N}(\mathrm{x}_i - \bar{x})(\mathrm{y}_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(\mathrm{x}_i - \bar{x})^2 (\mathrm{y}_i - \bar{y})^2}} \tag{19}$$

$r =$ Correlation coefficient, $x_i =$ values of the x-variable in a sample, $\bar{x} =$mean of the values of the x-variable, $y_i =$values of variable in a sample, $\bar{y} =$mean of the values of the y-variable.

5.3. Information Entropy Analysis

It is a statistical merit for gauging the randomness's degree [25], and it describes the confusion properties of the original and the cipher image.

The ideal value is always equal to 8 for which the pixel values of the image always fall in the range of 0-255 [26]. The entropy value may fluctuate for the various pixel values of the image falls. Hence the suggested cryptosystem has 256 states so the maximum information entropy will be approached to 8 [7]. The following equation Used to calculate the information entropy:

$$H(m) = -\sum_{i=0}^{2^l - 1} p(m_i)\log_2(p(m_i)) \tag{20}$$

Where L indication to the total number of pixels values, $p(m_i)$ is refers to the probability to m_i.

As we can see, the above statistical parameters have a strong influence in judging the robustness and resistance of the proposed system towards any screening, in order to ensure that it enjoys a robust encryption level.

5.4. Mean Square Error

It measures the variation of two images. When its result is low that's indication to the less of the variation between both original and encrypted image [10].

$$MSE = \frac{1}{m_x n_x f}\sum_{k=1}^{f}\sum_{i=1}^{m}\sum_{j=1}^{n}\ (p(i,j) - c(i,j))^2 \tag{21}$$

Where $p(i,j)$ is mentioned for original image, $c(i,j)$ is mentioned for encrypted image, m,n is mentioned for total number of rows and columns.

5.5. Peak Signal-to-Noise Ratio

PSNR is measuring the ratio and the conformity between original and encrypted image [27].

$$PSNR = 10\log_{10}\left(\frac{Max_{01}^{\ 2}}{MSE}\right)dB \tag{22}$$

Where Max_{01} refer to the max conceivable pixel value of the original image.

5.6. Number of Pixels Change Rate

NPCR is used to measure the change rate of pixel's number of encrypted image when adjusting a pixel in the original image [10].

$$NPCR = \left[\frac{1}{MxN}\sum_{i,j} D(i,j)\right] X\,100\% \tag{23}$$

Where $\begin{Bmatrix} 0, \mathrm{D1(i,\ j) = D\,2(i,\ j)} \\ 1, \mathrm{D1(i,\ j) \neq D\,2(i,\ j)} \end{Bmatrix}$

5.7. Unified Average Changing Intensity

UACI is for the average change intensity of differences between both original and ciphered images [28].

$$UACI = \left[\sum_{i,j} \frac{|D1(i,j) - D2(i,j)|}{MNx255} \right] X100\% \tag{24}$$

Where N, M is referred to the columns and rows respectively, D2 is decrypted image, and D1 is the original image. In this part, we will make a comparison between our proposed system and the other different algorithms through the results of NPCR and UACI that ensure our proposed system accomplished a better result compared to the others.

When analyzing the influence on the system in terms of its sensitivity and flexibility towards the attacker changing some features of the original image to obtain a difference in the content of the encrypted image, the need for the availability of differential parameters (the above mentioned) to maintain such attacks will protect the system from activating or forming any changes by any stranger. So, these differential aggressions will not be of any use.

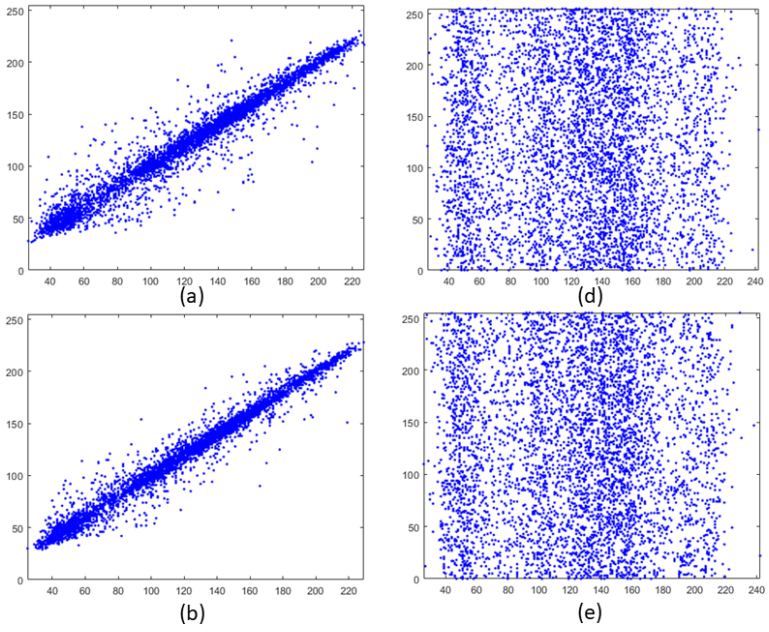
Therefore, performance measures dominate very much in influencing the strength of the system and the extent of the impact of each parameter separately, and therefore the rigidity of the system is subject to such parameters to know the difference between the effect of routine methods and the proposed system. In Table 1 it's shown the various parameters that illustrate the analysis of the effectiveness of performance measures in our system, with a mention of the speed of performance in terms of time, as it is one of the most important parameter that reflect efficiency, especially with regard to real-time applications.

Table 1. The factors of the Encryption Goodness for Some Various Image Tested.

Images	Entropy	PSNR	T(sec)	MSE
cameraman	7.9992	8.4061	0.219399	9385.717
Baboon	7.9993	9.8148	0.14299	6785.7811
Peppers	7.9993	8.256	0.18481	9715.8455
Lena	7.9993	9.2376	0.17867	7750.3625
Mean	7.999275	8.928625	0.18147225	8409.426525

Table 2. Refers to the Parameters of NPCR (%) and UACI (%) of our Proposed System.

Images Parameters	Cameraman	Baboon	Peppers	Lena
NPCR (%)	99.6779	99.6908	99.5376	99.6908
UACI (%)	33.6204	33.6247	33.5736	33.6247



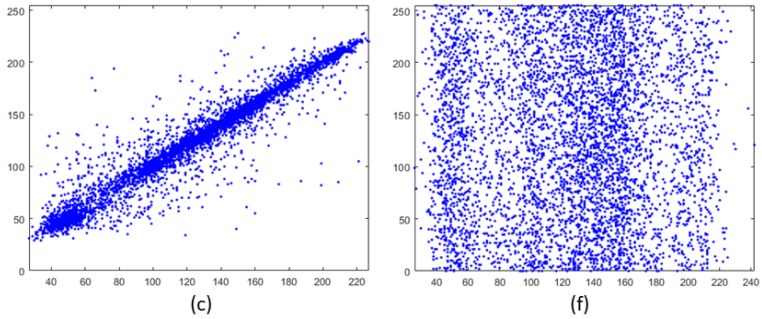


Fig.11. The Correlation of Plain Image and Cipher Image of Lena Test Image, 1st Column for Plain Image & 2nd Column for Encrypted Image.

Table 3. Correlation Coefficient of the Original Images and their Encrypted Images.

Images	Directions	Horizontal	Vertical	Diagonal
cameraman	Plain image cipher image	0.98448 -0.016364	0.99074 0.0048909	0.97558 -0.0082512
Baboon	Plain image cipher image	0.98075 0.0094014	0.97453 -0.030857	0.95822 0.0058893
Peppers	Plain image cipher image	0.97767 -0.018014	0.97125 -0.00072265	0.97886 -0.020445
Lena	Plain image cipher image	0.97576 -0.0025414	0.98412 0.00091759	0.96208 -0.0019035

For an image there's adjacent pixels have some degrees of correlation in horizontal, vertical and diagonal directions, so it can be seemed that in the original image the correlation is very vigorous regarding to the linearity linkage in all directions and it has a high correlation while the ciphered image has a very low one with random shape. In order to obtain an excellent cryptography algorithm to conserve the data from attackers whom manage statistical onslaught by exploiting correlation values of the original image, therefore it supposed to breakdown this linkage in the encrypted image. from Table 3, it's clear that the correlation value of plain image is close to value 1 and that's refer to the strength of its adjacent pixel correlation, and the opposite for the correlation value of encrypted image is close to value 0 which means the adjacent pixel correlation is extremely weak, and for the negative values it's confirming that there's no rapport between the original and the encrypted image. “Fig. 11,” refer to the simulation of correlation in our proposed algorithm.

Table 4. The Parameters of NPCR (%) and UACI (%) of our Proposed System Compared to another References.

References Number	NPCR (%)	UACI (%)
Yasser, I et al. [10]	99.6287	33.6124
Benlashram, A et al. [13]	99.6506	33.6096
Murali, P [15]	99.93	33.38
Patro, K. et al. [24]	99.6089	33.4214
Lu, Q et al. [25]	99.5743	33.3941
Diab, H. et al. [27]	99.62	33.90
Girdhar, A et al. [29]	99.587	33.463
Abdelfatah, R. I et al. [30]	99.6227	33.51964
Idrees, B et al. [31]	99.5758	33.3227
Arab, A, [32]	99.6368	33.4724
The proposed	**99.6908**	**33.6247**

Security analysis is utilizing for assessment the rigidity and durability of the proposed system. And its success can be deemed through the factors that we used previously. Table 1, show multiple parameters of our work. This section gives the analysis of ENTROPY, MSE, PSNR and TIMING (T). Moreover, the scheme obtained larger values NPCR >99.5 and UACI > 33.3 thereby resisting differential offensive as it seemed in Table 4, and when we look closely, we will find that our results get the highest performance than others. This has been shown through the comparisons mentioned in the above Table 4, such as [24,25]. Based on this analysis and figures, we can show the extent of the regime's strength and distinction, as it has not been subjected to various attacks.

6. Experimental Results

In view of our proposed algorithm in our paper, all the steps are obtained using MATLAB R2018a software to

establish eventuality of the system. All of our experiments have been implemented using core i7-2670QM ,2.20GHz with RAM 6.00 GB windows 10 Machine, fulfillment of proposed algorithm is applied where all the proposed operations were done in both encryption and decryption techniques. We applied the standard images Lena, Cameraman, Peppers, baboon, each of them is 512 × 512 as original images which all are passed all the tests related to the proposed system.

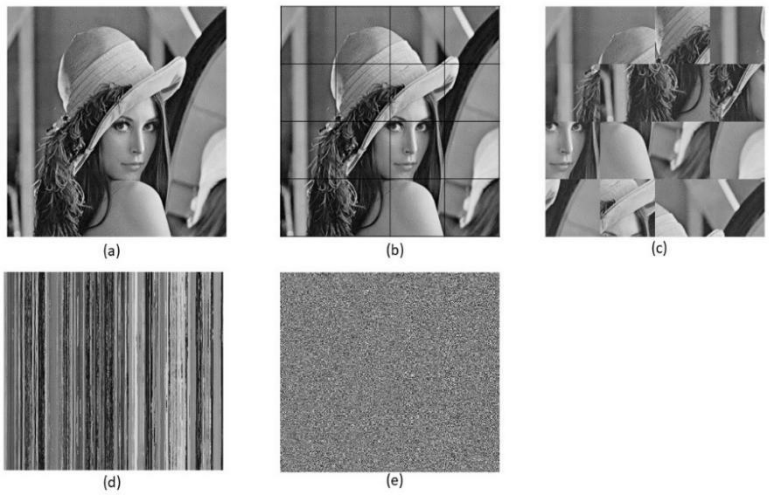


Fig.12. Encoding Results Simulation Using Lena Image as a Sample Test: (a) Original Image; (b) Sub Blocks Image; (c) Shuffled Blocks Image; (d) Confusion Step Image (e) Diffused & Final Encrypted Image.

According to “Fig. 12,” the proposed cryptosystem uses grayscale image with a gray scale output, and as it seemed the stages of the all entire encryption mechanism using a "Lena" image, including the stages of diffusion and confusion to obtain a final image that does not indicate clear evidence of the real image. If there is unreliable interference without awareness of the real control parameter the pseudorandom sequences can't be known. And that promote chaos mechanism features where when any change is issued in the initial values, then a complete change will be produced in the chaotic sequence of the chaotic curve through the parameters [31]. Our control factor of u= 5.29925609906277e+14, p= 6.78901762962345e+14.

After looking at “Fig. 13,” as we used four test images, it becomes clear that the encrypted image resulting from following the encryption steps of the proposed system that hides all its features and does not give any disclosure about its content or its implicit data, which confirms the effectiveness and durability of the proposal, and similarly when going to the decryption process, using the appropriate secret keys used in the encryption process, we directly get the original image, complete and with restoring its clear features.

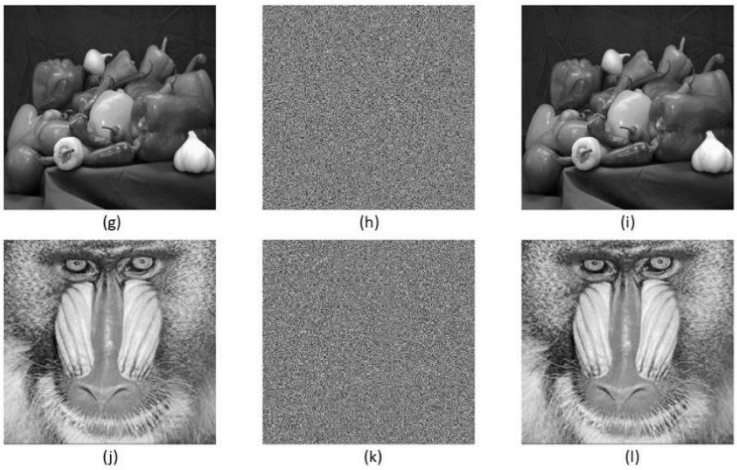


Fig.13. Encrypted &Decrypted Process: 1st Column Refer to Original Images, 2nd Column Refer to Final Encrypted Images, 3rd Column Refer to Decrypted Images.

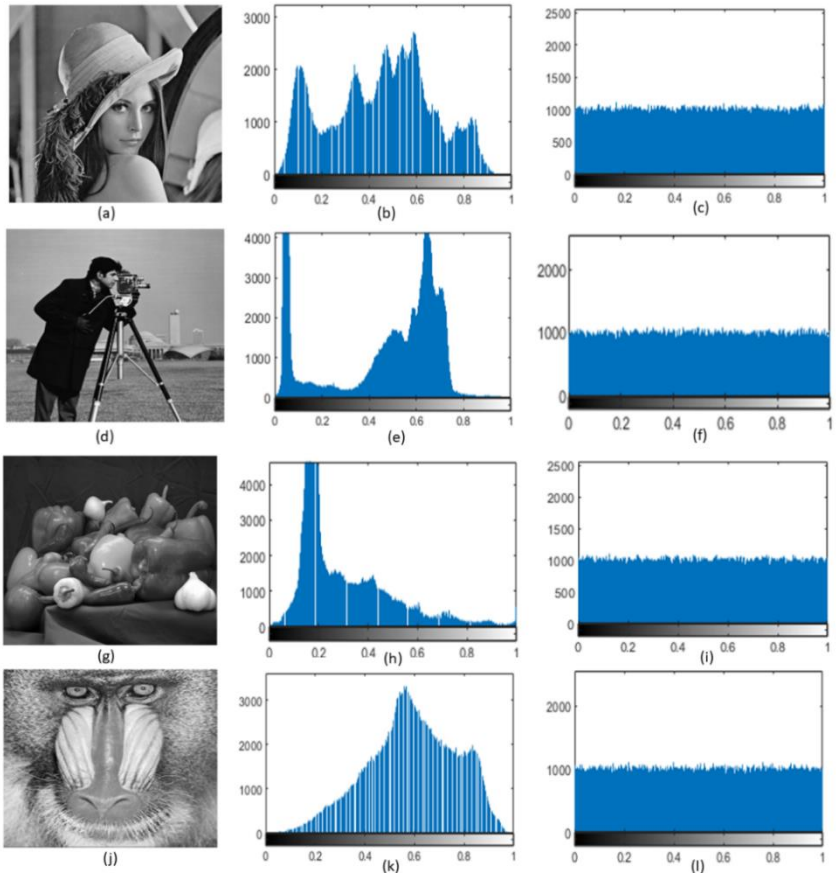


Fig.14. Several Test Images with their Histogram through Encryption and Decryption Process, 1st Column is Plain Images, 2nd Column Histogram of Plain Images, 3rd Column Histogram of Cipher Images.

Usually, the distribution of the gray values of plain images can be known by the statistical characteristics of the images, and its changing is considered as a very significant sign to estimate the effective of the encryption process. The histograms for the plain and cipher image are illustrated in "Fig. 14," The histogram of the image shows the distribution of the image pixel value and it can be noticed that the histogram distributions of the encrypted images are almost uniform, that conceal the statistical characteristics of the images and do not reveal the real content against any attack on the system.

6.1. Effectiveness of the Proposed System

After performing all the operations and executing them on all the previously mentioned images, it turns out that in the encryption process, all the normal image data has turned into a vague and unclear image where no information can be known at all, and this is confirmed by the graphical distribution of the image after encoding it, as the approximation

of the distribution of the encrypted data or information as in "Fig. 14," is an indication of the efficiency and quality of the system.

6.2. Key Space

The security process of the encryption scheme depends on the key spaces used in the system not only to the sensitivity to the secret key. The larger the key space, the higher and strong the security resistance to obtain an encrypted system algorithm that can expel and attack any brute interference, and that's could be fulfilled when a key space is more than 2^{100} [18], here in our proposed algorithm we have parameters (a_1,b_1, u, p) and the overall secret key has a length of 512 bits with a range of 0, 1 obtained from Hilbert key and Henon map. When the length of every key is 14 decimal so key space is considered as $10^{14} \, x \, 10^{14} \, x \, 10^{14} \, x \, 10^{14}$, $(10^{14})^4 > 2^{100}$ which is much big enough to resist thorough attacks [21,34].

6.3. Key Sensitivity Analysis & Attacks

Key sensitivity is a means of finding out if the system can resist forcefully the brute attack, as the efficiency of the key sensitivity reflects the ability of the proposed system to challenge the attack exposed to it in the encryption and decryption operations, which through the production of encrypted images through any simple change in any of the system parameters[35,36], where it is assumed that when the data is attacked or stolen with any of the wrong keys, the attacker will not be able to access the real and legitimate data of the image [30,31].Let we assume that we have two different keys, one of them is the right one [K1] and the other one is the wrong key [K2] by making a changing in the [K1]; we will note that the image encrypted using the [K1] is extremely different compared to the image encrypted using the [K2].

Here in "Fig. 15," referred the key sensitivity of the proposed system where it shows that (a & c) is reflects encrypted image with the [K1] and (b) reflects decrypted image with the [K1] but in (d) it shows decrypted image with the [K2] which it couldn't be turned to the original image as in the other right case, so we approved that the proposed algorithm has high key sensitivity; [K1: is refer to Right Key/ K2: is refer to Wrong Key].

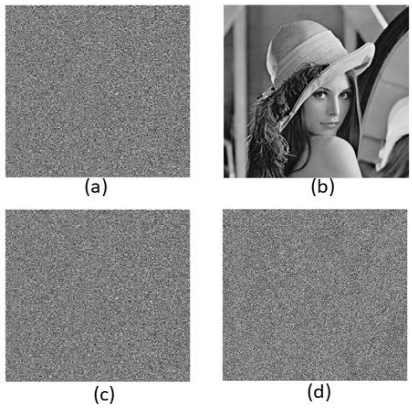


Fig.15. Key Sensitivity Process (a & c) Shows the Encrypted Image, (b) Decrypted Images with the Right Key, (d) Decrypted Image with the Wrong Key.

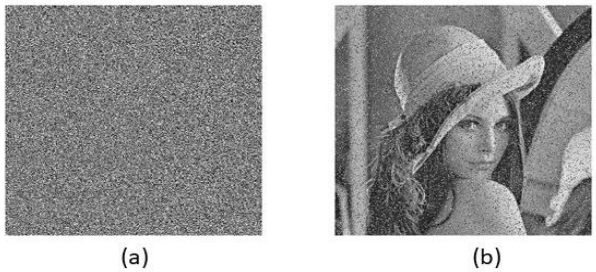


Fig.16. The Effect of Noise Attack; (a) Encrypted Image with, (b) Decrypted Image with 0.1 Salt & pepper Noise.

There're two factors used for analysis of attacks against the security system which are "UACI & NPCR" [33, 37, 38], and in order for the system to be successful against any brute force and controlling the security system of the algorithm, it must have a high degree of susceptibility for frequent attacks on the data [39]. Therefore, high sensitivity must be required, which leads to a noticeable and clear difference between the original and encrypted image [40]. Here in "Fig. 16," it's found that the system can resist the salt and pepper attack. Which results in its great ability to resist all different attacks.

7. Conclusion and Future Work

Newly, fog computing occupies a large place in the current technology due to its outstanding efficiency, with some loopholes related to the security of sensitive data transmission. Therefore, data image encryption is one of the legal mechanisms for maintaining image confidentiality on such reliable and unrestricted public media. The proposed system was based on encoding grayscale images with the help of confusion and diffusion utilizing Hilbert curve and 2D-Henon map technicality. We have approved through several analytical and statistical procedures and it is indispensable to examine differential attacks that reflect the strength of the proposed algorithm, including its high sensitivity and resistance to various violations, and this is given by the result of UACI (33.6247%) and NPCR (99.6908%) which indicates the quality and superiority of our system from While we prove the presented results and their impact in the formation of a complex proposal. Moreover, the encryption time and speed of system performance are suitable for using this technology in real-time application such as the wireless field and sensitive systems related to digital image transmission, for example, but not limited to medical images. The keys in our system are chosen randomly and this reflects the guarantee of the level of security in our algorithm. In the future, we will present further work and propose a more robust system to improve the encryption mechanism and performance based on the use of color images to keep pace with the fast-paced technical and working life of our society, which needs more comprehensive and effective security.

References

[1] Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials, 20(1), 601-628.

[2] Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture, 98, 289-330.

[3] Guan, Y., Shao, J., Wei, G., & Xie, M. (2018). Data security and privacy in fog computing. IEEE Network, 32(5), 106-111.

[4] Ashi, Z., Al-Fawa'reh, M., & Al-Fayoumi, M. (2020). Fog computing: security challenges and countermeasures. Int J Comput Appl, 975, 8887.

[5] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6(1), 1-22.

[6] M. N. Alenezi, H. Alabdulrazzaq, "Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish," International Journal of Communication Networks and Information Security, Vol. 14, No. 1, 2022

[7] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., & Buchanan, W. J. (2021). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Personal Communications, 1-28.

[8] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[9] Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., & Hussain, I. (2020). A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. Entropy, 22(3), 274.

[10] Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity.

[11] Albahrani, E. A., & Alshekly, T. K. (2017). New chaotic substation and permutation method for image encryption. International Journal of Applied Information Systems, 12(4), 34-39.

[12] Teng, L., Wang, X., & Meng, J. (2018). A chaotic color image encryption using integrated bit-level permutation. Multimedia Tools and Applications, 77(6), 6883-6896.

[13] Benlashram, Arwa, et al. "A novel approach of image encryption using pixel shuffling and 3D chaotic map." Journal of Physics: Conference Series. Vol. 1447. No. 1. IOP Publishing, 2020.

[14] Zhu, S., & Zhu, C. (2020). Secure image encryption algorithm based on hyper chaos and dynamic DNA coding. Entropy, 22(7), 772.

[15] Murali, P., & Sankaradass, V. (2019). An efficient space filling curve based image encryption. Multimedia Tools and Applications, 78(2), 2135-2156.

[16] Zhang, X., Wang, L., Zhou, Z., & Niu, Y. (2019). A chaos-based image encryption technique utilizing hilbert curves and H-fractals. IEEE Access, 7, 74734-74746.

[17] Shahna, K. U., & Mohamed, A. (2018, July). An image encryption technique using logistic map and Z-order curve. In 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research IEEE (ICETIETR) (pp. 1-6).

[18] Raza, S. F., & Satpute, V. (2019). A novel bit permutation-based image encryption algorithm. Nonlinear Dynamics, 95(2), 859-873.

[19] Kari, A. P., Navin, A. H., Bidgoli, A. M., & Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. Multimedia Tools and Applications, 80(2), 2753-2772.

[20] Farah, M. A., Farah, A., & Farah, T. (2020). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4), 3041-3064.

[21] Wu, J., Liao, X., & Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. Signal Processing, 153, 11-23.

[22] Sheela, S. J., Suresh, K. V., & Tandur, D. (2017). A novel audio cryptosystem using chaotic maps and DNA encoding. Journal of Computer Networks and Communications.

[23] Yousif, S. F. (2018, January). Grayscale image confusion and diffusion based on multiple chaotic maps. In 2018 1st International scientific conference of engineering sciences-3rd scientific conference of engineering science (ISCES) (pp. 114-119).
[24] Patro, K. A. K., Soni, A., Netam, P. K., & Acharya, B. (2020). Multiple grayscale image encryption using cross-coupled chaotic maps. Journal of Information Security and Applications, 52, 102470.
[25] Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, 8, 25664-25678.
[26] Belazi, A., Abd El-Latif, A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. Signal Processing, 128, 155-170.
[27] Diab, H. (2018). An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. IEEE access, 6, 42227-42244.
[28] Benlashram, A., Al-Ghamdi, M., AlTalhi, R., & Laabidi, P. K. (2020). A novel approach of image encryption using pixel shuffling and 3D chaotic map. In Journal of Physics: Conference Series (Vol. 1447, No. 1, p. 012009). IOP Publishing.
[29] Girdhar, A., Kapur, H., & Kumar, V. (2021). A novel grayscale image encryption approach based on chaotic maps and image blocks. Applied Physics B, 127(3), 1-12.
[30] Abdelfatah, R. I., Nasr, M. E., & Alsharqawy, M. A. (2020). Encryption for multimedia based on chaotic map: Several scenarios. Multimedia Tools and Applications, 79(27), 19717-19738.
[31] Idrees, B., Zafar, S., Rashid, T., & Gao, W. (2020). Image encryption algorithm using S-box and dynamic Hénon bit level permutation. Multimedia Tools and Applications, 79(9), 6135-6162.
[32] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75(10), 6663-6682.
[33] Zhu, S., Zhu, C., Fu, Y., Zhang, W., & Wu, X. (2020). A secure image encryption scheme with compression-confusion-diffusion structure. Multimedia Tools and Applications, 79(43), 31957-31980.
[34] Cheng, G., Wang, C., & Chen, H. (2019). A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. International Journal of Bifurcation and Chaos, 29(09), 1950115.
[35] Hosny, K. M. (Ed.). (2020). Multimedia security using chaotic maps: principles and methodologies (Vol. 884). Springer Nature.
[36] Nkandeu, Y. P. K., & Tiedeu, A. (2019). An image encryption algorithm based on substitution technique and chaos mixing. Multimedia Tools and Applications, 78(8), 10013-10034.
[37] Zhang, X., Zhou, Z., & Niu, Y. (2018). An image encryption method based on the feistel network and dynamic DNA encoding. IEEE Photonics Journal, 10(4), 1-14.
[38] Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dynamics, 83(3), 1123-1136.
[39] Slimane, N. B., Bouallegue, K., & Machhout, M. (2017). Designing a multi-scroll chaotic system by operating Logistic map with fractal process. Nonlinear Dynamics, 88(3), 1655-1675.
[40] Li, C., Luo, G., & Li, C. (2019). An Image Encryption Scheme Based on the Three-dimensional Chaotic Logistic Map. Int. J. Netw. Secur., 21(1), 22-29.

Authors' Profiles

Samaa Y. Tarabay received the B.S degree in Electronics and Communications Engineering Department, Faculty of Engineering from Misr higher institute of Engineering and Technology, Mansoura, Egypt and prepostgraduate from the Electronics and Communications Engineering Department, Mansoura University, Egypt, in 2015 and 2017, respectively.

Abeer T. Khalil received the B.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, in 2001 and 2013, respectively. She is currently working as an Associate Professor at the Electronics and Communications Department, Faculty of Engineering, Mansoura University. She has published more than 30 articles and supervised ten postgraduate students in many universities. She is interested in wireless networking and hardware realizations of digital systems.

Ahmed S. Samra Received the B.Sc. and the M.Sc degree in communications engineering from Menoufia University 1977, 1982 respectively, and the PhD. degree in optical communications and integrated optics from ENSEG, Grernoble, France in 1988, France in 1988. Reviewer for some international journals and conferences; (Optical engineering journal, Optoelectronic Review journal, Optoelectronics and advanced

Materials rapid communication journal, Optik journal, and the six international conference on wireless and optical communication networks WOCN 2009). Supervisor for about 70 M.Sc. and Ph.D. Thesis, and more than 90 accepted papers in a national and international journals and conferences. Head of communication and computer Department, Faculty of Technology, El-madina El-monawara, Saudi Arabian. Head of Electronics and Communication Engineering Department, Faculty of Engineering, Mansoura University. Director of Biomedical Engineering Program, Faculty of Engineering, Mansoura University. Director for Training unit, Faculty of Engineering, Mansoura University.He is now a professor at the faculty of engineering, Mansoura University. His research interests are in the field of optical communications, integrated Optics and optical measurement techniques.

Ibrahim Yasser received the B.Sc. degree in electronics and communications from Benha University, Egypt, and the M.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Mansoura University, Egypt, in 2016 and 2020, respectively. His research work has been materialized in books and ISI index articles in international specialty journals. His research interests include neutrosophic sets, security, multimedia, fog and cloud computing, chaotic maps, machine learning, big data, artificial intelligent, medical image analysis, computer-aided diagnosis, and flexible education. Future research interests include design security techniques for the cloud requiring little user awareness and computer-aided diagnosis medical images analysis. He is a member of chief editors for Neutrosophic Knowledge journal.

How to cite this paper: Samaa Y. Tarabay, Abeer Twakol, Ahmed S. Samrah, Ibrahim Yasser, "A Secure and Efficient Cryptography System Based on Chaotic Maps for Securing Data Image in Fog Computing", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.1, pp.64-80, 2023. DOI:10.5815/ijcnis.2023.01.06