**Open Access** **Baghdad Science Journal** **P-ISSN: 2078-8665**
**Published Online First: January 2022** **2022, 19(4): 905-913** **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2022.19.4.0905

# A Novel Technique for Secure Data Cryptosystem Based on Chaotic Key Image Generation

***Mustafa Dhiaa Al-Hassani***

Computer Department, College of Science, Mustansiriyah University, Baghdad, Iraq.
E-mail address: dr_mdhiaa77@uomustansiriyah.edu.iq

Received 30/5/2021, Accepted 16/8/2021, Published Online First 20/1/2022, Published 1/8/2022



## Abstract:

The advancements in Information and Communication Technology (ICT), within the previous decades, has significantly changed people's transmit or store their information over the Internet or networks. So, one of the main challenges is to keep these information safe against attacks. Many researchers and institutions realized the importance and benefits of cryptography in achieving the efficiency and effectiveness of various aspects of secure communication.This work adopts a novel technique for secure data cryptosystem based on chaos theory. The proposed algorithm generate 2-Dimensional key matrix having the same dimensions of the original image that includes random numbers obtained from the 1-Dimensional logistic chaotic map for given control parameters, which is then processed by converting the fractional parts of them through a function into a set of non-repeating numbers that leads to a vast number of unpredicted probabilities (the factorial of rows times columns). Double layers of rows and columns permutation are made to the values of numbers for a specified number of stages. Then, XOR is performed between the key matrix and the original image, which represent an active resolve for data encryption for any type of files (text, image, audio, video, … etc). The results proved that the proposed encryption technique is very promising when tested on more than 500 image samples according to security measurements where the histograms of cipher images are very flatten compared with that for original images, while the averages of Mean Square Error is very high (10115.4) and Peak Signal to Noise Ratio is very low (8.17), besides Correlation near zero and Entropy close to 8 (7.9975).

**Keywords:** Chaotic Cryptosystem, Data Encryption, Double Layer Permutation, Key Image Generation.

## Introduction:

Cryptography provides secure communication among individuals, governmental organization, corporations through the utilizing of codes and it can be used effectively to nullify the value of cyber threats in the presence of malicious third-parties, phishing, interception of information being stored in database or sent via networks. Thus, only those intended parties for whom the information was sent can interpret and analyze it. Certainly, this information relates to multiple areas, such as: financial accounts, civil or military aspects, scientific inventions, medical, educational, business applications, live-broadcast, or any sensitive data that someone wants to keep private … etc [1-4].

Many encryption techniques were developed in the past decades to be adopted as a national standard for secure communication, like: DES, RSA, 3-DES, Two-fish, IDEA, AES. Yet, they are not suitable options for real-time multimedia cryptosystem of large size [4-6]. On the other hand, cryptanalysts are trying to develop their expertise and capabilities to find shortcuts to break the security of these cryptosystems. The AES is considered one of the foremost broadly utilized encryption methods today by the public whether they are individuals, institutions, companies. However, it suffers from longtime calculations in encryption/decryption processes (i.e., low-level efficiency with large multimedia). Therefore, there is a need to develop a fast and strong cryptographic cryptosystems with pseudo-random behavior. Dynamic systems theory and chaos demonstrated promising area within the field of cryptography for research and applications [5-7]. Chaos-based schemes are dominant techniques due to high randomization, simple cryptographic processes, and its sensitivity

to initial control parameters, such that a minor deviation in its input parameters can lead to a large change in the output range values. This will guarantee that the plain-data and/or secret key can't be easily reconstructed [5, 8, 9].

Image encryption techniques acquire the attention of scientists and researchers in order to meet the growing demand for real-time information security. The following survey includes various efforts related to our paper objectives for secure data cryptosystems: In [1], a scrambled plaintext-related image cryptosystem based on improved Josephus traversing and pixel bits permutation is presented to enhance the abilities of resistance against different types of attacks. A combination of image segmentation of chaotic system, bitwise XOR and crossover operations are made to attain higher effects of randomness. In [5], the authors worked on the scrambling of text according to a novel 2D chaotic function that exhibits a uniform bifurcation upon large parameters range. Genetic algorithm is used to optimize the parameters of the map and hence improve the security of textual data. In [9] an encryption algorithm is proposed to improve the security of a cryptosystem by solving the key management problem through a combination of an elliptic curve and chaotic system. In [10], a novel architecture of image encryption algorithm' permutation and diffusion based on DNA rule matrix operations and 2D-LASM chaotic systems is proposed using 256-bit hash value. Security analyses are performed on multiple samples which prove the efficiency of the scheme and it robustness against known attacks. In [11], a perturbed high-dimensional chaotic system is investigated for image encryption according to Devaney conjugate definition to enlarge cycle and manage secure problems. The confusion/diffusion structure is designed based on separated Cat map. The test results prove high security of the technique with fast algorithm. In [12], a framework and an algorithm are introduced based on dual Arnold and logistic chaotic maps for lightweight image encryption scheme. Miscellaneous groups of images have analyzed and produce very good results according to security measures.

This paper aims to build a secure cryptosystem for the transfer of data among entities, whether individuals, companies, or state institutions, and for various military, medical, banking or other fields. A non-standard technique was adopted that aims to generate a two-dimensional chaotic key matrix image that includes enormous number of probabilities based on 1-D range chaos values for given control parameters (selected randomly by the system in order to ensure higher level of information security), which is considered the main target of any cryptosystem to make the mission of any cryptanalyst impossible, those numbers are processed in some way to produce non-repeated set of numbers. Successive processes are then performed on the 2-D key matrix including permutation, repetition, and diffusion. Initially, the values of numbers in both rows and columns are permuted for specified number of stages. After that, XOR operations are carried out between original image data and key matrix values. The resulted chaotic key image with flatten histogram represents the key to encrypt any secret data file.

**Chaotic Theory**

The security of information becomes a significant concern for all internet users. Hence, the data to be shared between any entities must be secure using an encryption technique prior to transmission. Actually, a faster and secure technique that offers good ciphers is a chaotic-system that has many attractive features for secure communications. Chaos theory has been used widely in modern cryptosystems. Its behavior exhibits/creates a random sequence, which is considered as a benefit of using chaos efficiently for real-time multimedia encryption instead of the traditional DES, RSA, AES, … etc [13-15].

Chaos sequences are generated through the use of iterative equations, $x_{n+1} = f(x_n)$, that will be produced randomly, aperiodic and unpredictable. Furthermore, it is important to mention that any little changes in the starting conditions will cause widely varying outcome sequences (i.e., very sensitive to initial conditions). The equations below are used to express it mathematically:

$$x_{n+1} = r * x_n (1 - x_n) \text{ , where } r \in [0, 4] \text{ , } x \in [0, 1] \text{ , } n = 0, 1, 2, \ldots \quad \ldots\ldots\ldots\ldots 1$$

A property of the logistic map can be exhibited when the chaotic parameter (r) value ranges from 3.5 to 4, such that its behavior depends on r's value; otherwise, the values will instantly leave the interval [0, 1] when r exceeds 4. Eq.2 – Eq.4, are the results of substituting the values of *n* into Eq.1 [13-16, 17, 18]:

$$x_1 = r * x_0 (1 - x_0) \text{ , when } n = 0 \quad \ldots\ldots 2$$
$$x_2 = r * x_1 (1 - x_1) \text{ , when } n = 1 \quad \ldots\ldots 3$$
$$x_3 = r * x_2 (1 - x_2) \text{ , when } n = 2 \quad \ldots\ldots 4$$

**The Proposed Cryptosystem**

The proposed cryptosystem is composed mainly of sender and recipient components. Fig.1 displays the block diagram of the sender part. Conversely, the recipient reconstructs the original secret file by performing the decryption processes in reverse order. The system is implemented using Microsoft Visual C#.net 2019 and its performance was

measured according to thousands number of experiments.

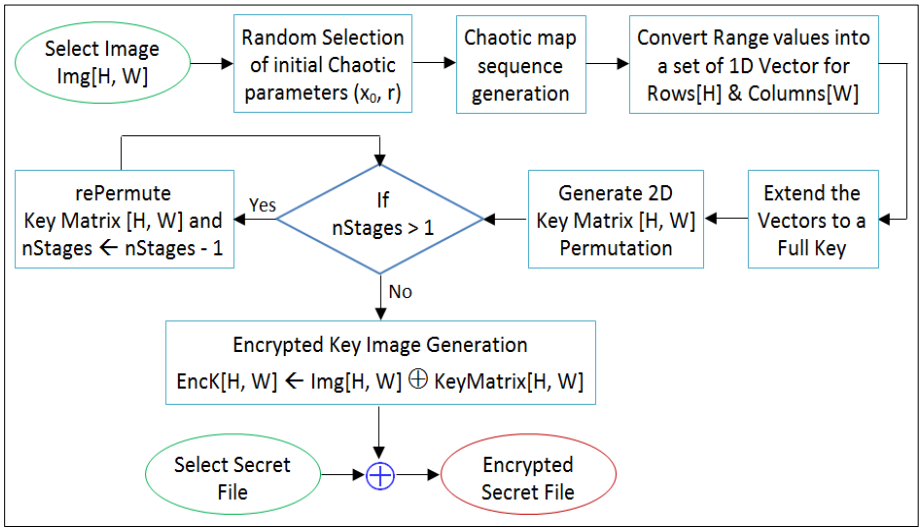



**Figure 1. The Block diagram of the proposed Encryption Technique**

The idea is based originally on generating a cipher image by exploiting the properties of randomness from chaotic-maps, as indicated in Eq.1, which will be considered as a key to encrypt the plain data (i.e., secret file). The system selects randomly the initial parameters of the logistic map ($x_0$, $r$), such that: $x_0 \in [0, 1]$ and $r \in [0, 4]$ in order to create the random sequence that was used in some manipulation to produce the values and ranges whose length is the same as image rows and columns dimensions, which will constitute the 2-D key matrix that will be generated after the extending of key Row and key column to a full keys of non-repeated values. Then, there is a re-permute to the 2-D key matrix according to the number of stages prior to XOR operations that are performed between pixels image data and its equivalent 2-D key matrix so as to obtain an encrypted key image. It is worthwhile that this step is performed in "offline" mode by the system which saves computational time and avoid delay.

To convert the selected secret file (plain-form data) of any extension into a meaningless cipher form, initially the sender must follow the sequence of steps indicated in Algorithm 1 to generate the key image.

**Algorithm 1. The Proposed Key Image Generation**

Input : Image Img[H, W], H refer to height and W for the width; Number of Stages (nStages).
Output: Encrypted Key Image Generation file whose data denoted by EncK[H, W].

a) The proposed system *randomly* select initial chaotic parameters ($x_0$ ,$r$) such that $0.5 \leq x_0 \leq 1.0$ *and* $3.5 \leq r \leq 4.0$.
b) Chaotic sequence values (VL) and ranges (RG) are generated according to a pre-specified range length.
c) Convert VL & RG into a set of 1-D Vectors of non-repeated values after processing their floating-numbers (i.e., 4-decimal points): v1 ← (val / 1000) mod HorW, v2 ← (val / 100) mod HorW, v3 ← (val / 10) mod HorW, v4 ← (val / 1) mod HorW for both rows and columns to produce the non-sorted numbers permutation PermR[ ] and PermC[ ] respectively.
d) For each value from v1 to v4, check if it is not found in the corresponding vector then add it to the key vector and increment its index by 1.
e) Extend PermR[] to a full key by adding the remaining numbers in some order if the obtained R's < H, and equivalently extend PermC[ ] to a full key if the obtained C's < W.
f) Generate a the 2-D KeyMatrix[ , ] whose dimensions are H and W.
g) Permute KeyMatrix[H, W] according to PermR[H] and PermC[W] values.
h) Update nStages ← nStages – 1.
i) While (nStages > 1) goto step g).
j) Perform the XOR operations: EncK[H, W] ← Img[H, W] ⊕ KeyMatrix[H, W], where i = 0 to H – 1 and j = 0 to W – 1.
k) The system automatically create the key image file whose size equivalent to the selected image and its data is EncK[H, W].

The resulted key image will be used to encrypt the selected secret file through another bitwise XOR processes in order to make the confusion more powerful. Then, the 4-tuples header information (keyimageID, x0, r, nStages) which is composed of 13-bytes (i.e., 4-bytes represent the ID of selected key image from a set of common database images between sender and recipient, 4-bytes is dedicated for each floating-point chaos initial parameters (x0, r) respectively, and the last byte for the number of stages allocated for permutation in the encryption phase) will be concatenated with the encrypted secret file to be sent to the intended recipient.

The security of the suggested cryptosystem approach depends on a set of factors (most of them are produced arbitrarily), as indicated in the following points:

- The random selection of initial chaotic parameters $(x_0, r)$ by the computerized program.
- Chaotic sequence values and ranges generation.
- The full key permutations pattern PermR[] and PermC[].
- The 2-D KeyMatrix[H, W] permutation that produce a vast number of probabilities Prob. $= (H \times W)!$ which represent the major goal to make the attempts of cryptanalyst impossible. For example, if the number of Rows (H = 256) and the number of Columns (W = 329), then the probability of Keys = $(256 \times 329)! = 84224! \cong$ infinite number.
- The number of Stages (nStages) permutation.

The window-form program for the proposed encryption system relating to the sender is illustrated in Fig.2, with all parameters utilized to convert a secret image into non-interpreted form.

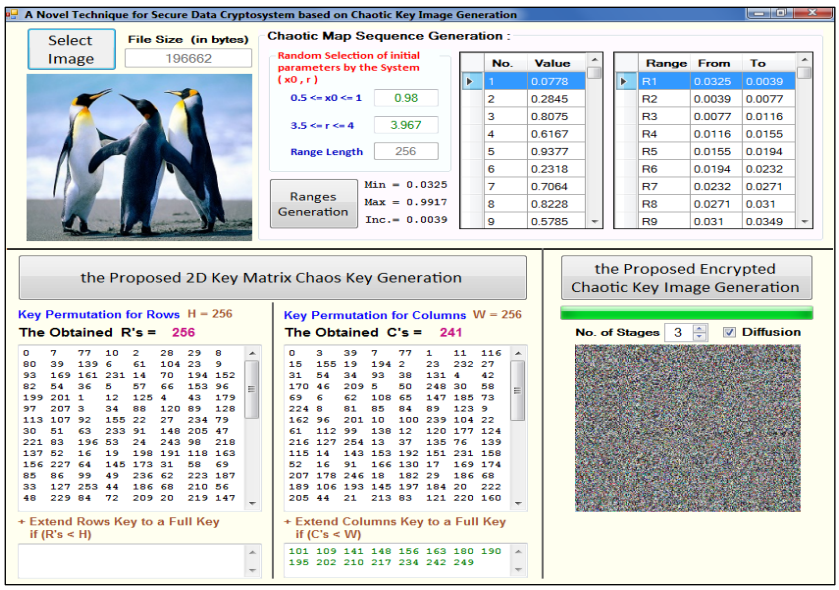



**Figure 2. The Window-Form of the proposed Encryption system**

In order to reconstruct the plain form of original secret file by the intended recipient over the communication channel, decryption processes must be performed in reverse way of what has been implemented during the stages of encryption; such that the 13 bytes header information will be extracted first from the encrypted secret file to obtain the 4-tuples (keyimageID, x0, r, nStages). Then, the same key image, chaotic sequence values besides ranges, and 2D key matrix permutation are all generated by the system accordingly. Consequently, the encrypted key image will be generated by following the same procedure stated in Algorithm 1 which will be diffused with the encrypted secret file to produce the original secret file.

**Security Measurements**

In this work some of security measurements will be applied to compute efficiency of the proposed encryption algorithm.

**a) Mean Square Error (MSE):** is a measurement tool used to compute the difference between two samples as cumulative squared error between original image (OI) and ciphered image (CI) [10, 13-18]:

$$MSE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} ( OI(i,j) - CI(i,j) )^2 \quad ...5$$

where H represents the height and W is the width of the image.

**b) Peak Signal to Noise Ratio (PSNR):** this measurement is utilized to assess an enciphering scheme, which points to the changes in pixel values between plain and cipher images. The lower value of PSNR represents better enciphering quality [10, 13, 18-21].

$$\text{PSNR} = 10 \times \log\left(\frac{255^2}{MSE}\right) / \log(10) \quad \ldots\ldots\ldots 6$$

**c) Correlation Coefficients:** in a plain image, pixels are usually very correlated with their adjacent pixels in any direction, while the relationship between neighboring pixels in an enciphered image should be as low as possible in order to resist correlation analysis. The correlation coefficients are calculated as follows:

$$Corr.(X,Y) = \frac{\sum_i \sum_j (X_{i,j} - \bar{X})(Y_{ij} - \bar{Y})}{\sqrt{\sum_i \sum_j (X_{i,j} - \bar{X})^2 \; \sum_i \sum_j (Y_{i,j} - \bar{Y})^2}} \quad \ldots\ldots 7$$

where *Corr.* refer to the correlation, X is the plain image and its mean is $\bar{X}$, while Y is the cipher image and its mean is $\bar{Y}$. The association image values range from -1 to 1, such that the good encryption should have a correlation value near to 0 [10, 13, 21-26].

**d) Information Entropy:** it is one of the most significant properties of randomness for an encryption planner analysis. It is the average amount of information content generated by a stochastic source of data. It is computed as shown in the following formula:

$$Entr. = -\sum_{i=0}^{255} P(X_i) \times log2\big(P(X_i)\big) \quad \ldots\ldots 8$$

where p(Xi) is the probability of symbol (Xi) and the entropy is expressed in bits. Ideally, the entropy value of the cipher message should to be close to 8 [10, 13, 19-22, 24].

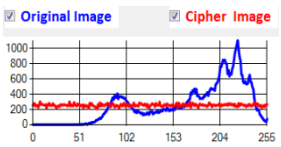
**e) Histogram Analysis:** to avoid the information leakage for an intruder when encrypting an image, it must be made sure that the original and cipher images do not have any statistical similarity. Histogram distribute pixel values in a 2D graphical representation, the vertical axis represent the frequency of each color intensity level (L range from 0 to 255) occurred in image. The more flatten histogram indicates a higher encryption technique [13, 20-24].

$$Hist(L) = \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} Freq(\, pixel(i,j)\,) \quad \ldots 9$$

## Results and Discussion:

To evaluate the efficiency of the proposed encryption technique according to the above security measurements, a number of experimental tests were performed, as shown in Tables.1–3, on more than 500 color/gray image samples collected from different color maps data sets (including: CSet8, CBSD68, Set12, kodak24 …etc) of various dimensions and format types.

**Table 1. Comparison of cipher images according to security measures after applying 2-D key matrix permutation with/without XOR substitution**

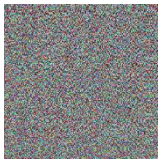
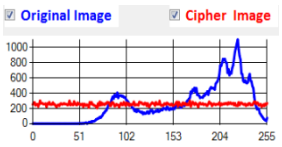
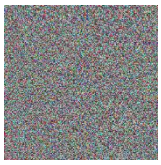
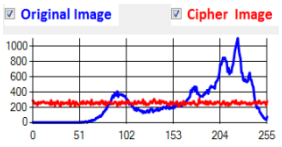
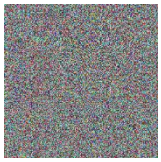
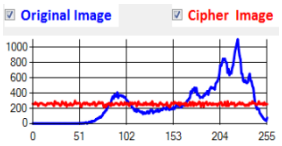
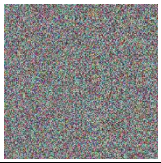
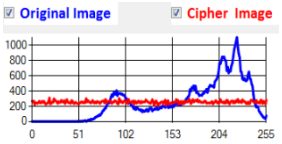
| Original Image (P.) | Cipher Image (C.) | Histogram | MSE | PSNR | Corr. | Entropy | |
|---|---|---|---|---|---|---|---|
| | | | | | | P. | C. |
|  256x256 |  Apply 2D key matrix Permutation on Original Image |   | 4468.724 | 11.935 | -0.0235 | 6.359 | 6.359 |
| |  Apply XOR between the 2D key matrix with Original Image |   | 8979.766 | 8.657 | 0.0012 | 6.359 | 7.997 |

From the results displayed in the previous Table, it is clearly indicated in 1st row that the obtained Histogram and Entropy for both original and cipher images are not changed when just applying the proposed 2-D key matrix permutation. Whereas, the histogram is made flatten (referred by

the red color compared with the original blue color) and the entropy of the cipher image becomes near 8 (7.997) when performing XOR with the original image as shown in the 2nd row. Furthermore, the MSE has increased to (8979.766) instead of (4468.724) while the PSNR has decreased from (11.935) to (8.657). Thus, this experiment proves the advantages of performing the XOR operations between the original image and the key matrix of permuted chaos based values. Consequently, it will be adopted in the subsequent tests.

The following Table compares the effect of applying multiple number of stages on security measures for the same image.

**Table 2. The impact of applying the number of Stages according to security measures**

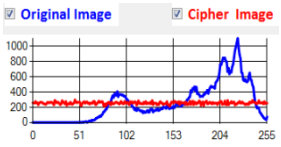
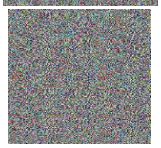
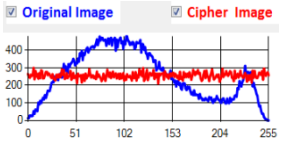
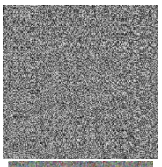
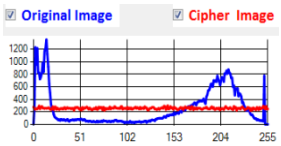
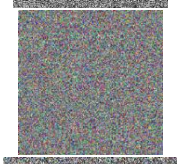
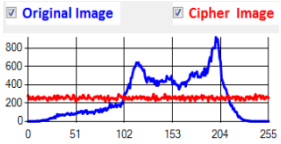
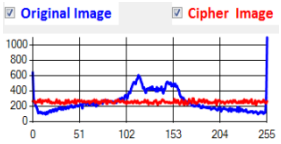
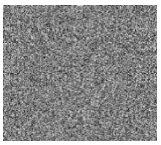
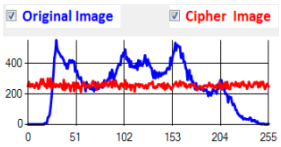
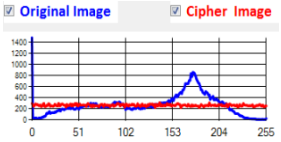
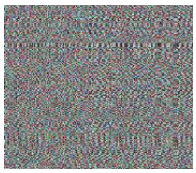
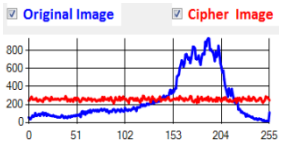
| Original Image (P.) | No. of Stages | Cipher Image (C.) | Histogram | MSE | PSNR | Corr. | Entropy | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | P. | C. |
|  256x256 | 1 |  |   | 8979.766 | 8.657 | 0.0012 | 6.359 | 7.997 |
| | 2 |  |   | 9001.205 | 8.645 | 0.0010 | 6.359 | 7.997 |
| | 3 |  |   | 9032.596 | 8.632 | -0.0038 | 6.359 | 7.997 |
| | 4 |  |   | 8968.613 | 8.66 | 0.0037 | 6.359 | 7.997 |

From the experimental tests in the above Table, it is shown that the optimal results are obtained when the number of stages equal 3 that produce higher MSE = 9032.596 and lower PSNR = 8.632. Therefore, it will be relied upon in the following tests.

The efficiency of the proposed encryption algorithm needs to be investigated according to different image samples of various types and dimensions, as illustrated in Table.3 below:

Baghdad Science Journal
2022, 19(4): 905-913
P-ISSN: 2078-8665
E-ISSN: 2411-7986

**Table 3. Security measurements of the efficiency of the proposed Encryption algorithm for different image samples**

| Original Image (P.) | Cipher Image (C.) | Size | Histogram | MSE | PSNR | Corr. | Entropy | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | P. | C. |
|  |  | 256x256 |  | 9032.596 | 8.632 | -0.0038 | 6.359 | 7.997 |
|  |  | 220x229 |  | 9427.969 | 8.41 | -0.0007 | 7.129 | 7.997 |
|  |  | 256x256 |  | 13206.87 | 6.923 | -0.0043 | 7.207 | 7.998 |
|  |  | 225x225 |  | 10011.47 | 8.178 | -0.0029 | 7.098 | 7.997 |
|  |  | 405x368 |  | 9444.136 | 8.38 | -0.0054 | 7.787 | 7.997 |
|  |  | 192x256 |  | 8636.81 | 8.767 | -0.0033 | 7.635 | 7.997 |
|  |  | 238x410 |  | 8510.982 | 8.835 | 0.00004 | 7.616 | 7.997 |
|  |  | 384x416 |  | 12653.039 | 7.257 | 0.00001 | 6.99 | 7.997 |
| **Average** | | | | **10115.48** | **8.1727** | **-0.0025** | **7.2276** | **7.9975** |

From the results demonstrated in the above Table, it is clearly indicated that the histograms of cipher images are very flatten compared with that for original images, and the average of other measures are very promising, such that the average MSE is very high (10115.48) and the average PSNR is very low (8.17), while correlation near zero and the average Entropy of the cipher image become near 8 (7.9975).

The overall randomness of cipher images can be revealed by information entropy measure, which is used to compare between the efficiency of the proposed method with that in previous related work [1] for the same image samples, as stated in Table .4.

**Table 4. Comparison of Entropy results between the proposed encryption method with that in (1) for the same image samples**

| Image Sample | Entropy values of Cipher Images | |
|---|---|---|
| | as indicated in [1] | the proposed encryption method |
| Lenna | 7.9972 | 7.9978 |
| Cameraman | 7.9969 | 7.9985 |
| Baboon | 7.9972 | 7.9979 |
| **Average** | **7.9971** | **7.9981** |

The security analysis and simulation test results, as indicated by the entropy values in the above table, prove the efficiency of the proposed algorithm are closer to 8 when compared with that in [1] according to the average entropies.

## Conclusions:

This research introduces an extremely secure data cryptosystem based on chaotic logistic map which is used to generate a 2D key-matrix image to encrypt any types of files and information stored in database or sent through a communication channel, and thus nullifies the value of interception. The originated key matrix offers an unbounded number of probabilities that make the process of brute-force attacks impossible. The security of algorithm depends on many factors: the initial control parameters selected randomly by the system to generate the chaotic ranges, the applied mechanism to derive set of unrepeated numbers from range values, the adopted map that convert the 1D chaotic values into 2D key matrix, advancing the number of stages to some extent on 2D key matrix transposition made significantly the key more secure, furthermore the diffusion processes that are performed with a private image selected by the sender.

The experimental results prove the efficiency of the proposed system when tested on more than 500 image samples of various dimensions and types according to many valuable indicators, in terms of hiding the distinctive marks in the histogram of ciphered images (become flatten) when compared with that of their original context, beside that the other security measurements are very hopeful where a highly average of MSE for cipher images is obtained greater than 10000 (i.e. the greater MSE indicators lead to higher quality and strength of the encryption method), whereas the mean PSNR is very low and appropriate (8.17), with correlation near zero and optimal entropy close to 8 (7.9975). Furthermore, the average entropy value of the proposed algorithm method achieves better results when compared with previous related works for a unified data set.

## Author's declaration:

- Conflicts of Interest: None.
- I hereby confirm that all the Figures and Tables in the manuscript are mine. Besides, the Figures and images, which are not mine, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in Mustansiriyah University.

## References:

1. Ying Niu, Xuncai Zhang. A Novel Plaintext-Related Image Encryption Scheme Based on Chaotic System and Pixel Permutation. IEEE Access. 2020; 8(1): 22082-93. DOI:10.1109/ACCESS.2020.2970103 .
2. Wen W, Zhang Y, Su M, Zhang R. Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture. Nonlinear Dyn. 2017; 87(1): 383-90. DOI:10.1007/s11071-016-3049-x.
3. Hossam Diab. An Efficient Chaotic Image cryptosystem based on simultaneous permutation and diffusion operations. IEEE Access. 2018; 6(1): 42227-44. DOI:10.1109/ACCESS.2018.2858839.
4. Mustafa D. Al-Hassani, B. Z. Jaafar. An Innovative Data Encryption Technique through Keys Distributed over Websites using Linked-Lists. International Conference ICASEA – Proceedings. 2018: 85–89. DOI:10.1109/ICASEA.2018.8370961.
5. Unnikrishnan Menon, Atharva Hudlikar, Anirudh Rajiv. A Novel Chaotic System for Text Encryption Optimized with Genetic Algorithm. Int J Adv Comput. Sci Appl. 2020; 11(10): 34-40. DOI:10.14569/IJACSA.2020.0111005.
6. William Stallings. Cryptography and Network Security-Principles and Practice. 7th Edition Pearson Education Limited England; 2017. 767 p.
7. Anchal Jain, Navin Rajpal. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. University School of Information and Communication Technology. Springer Science and Business Media. New York. 2015; 29(1). DOI:10.1007/s11042-015-2515-7.
8. Xiaoqiang Di, Jinqing Li, Hui Qi. A semi-symmetric image encryption scheme Based on the function projective synchronization of two hyper chaotic systems. PLOS ONE. 2017; Available from: https://doi.org/10.1371/journal.pone.0184586. DOI:10.1371/journal.pone.0184586.
9. Luo Y, Ouyang X, Liu J, Cao L. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access. 2019; 7(1): 38507-22. DOI:10.1109/ACCESS.2019.2906052.
10. Chai X, Gan Z, Yuan K, Chen Y, Liu X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput Appl. 2019; 31(9): 219-37. DOI:10.1007/s00521-017-2993-9.
11. Jun Xiao, Wang Zhu, Zhang Miao. An image encryption algorithm based on the perturbed high-dimensional chaotic map. Nonlinear Dyn. 2015; 80(3):1493–508. DOI:10.1007/s11071-015-1957-9.
12. Jannatul Ferdush, Mahbuba Begum, Mohammad S. Uddin. Chaotic Lightweight Cryptosystem for Image Encryption. Adv Multimedia. 2021; 1: 1-16. Available from: https://doi.org/10.1155/2021/5527295. DOI:10.1155/2021/5527295.
13. Yousif Bedir, Khalifa Fahmi. A novel image encryption/decryption scheme based on integrating

multiple chaotic maps. AIP Adv. 2020; 10(7): 075220-9. Available from: https://doi.org/10.1063/5.0009225.
14. Feng W, He Y, Li H. Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. IEEE Access. 2019; 7(14): 12584–97. Available from: https://doi.org/10.1109/access.2019.2893760.
15. Zhou Y, Bao L, Philip C. A new 1D chaotic system for image encryption. Signal Process. 2014; 97(1): 172–82. Available from: https://doi.org/10.1016/j.sigpro.2013.10.034.
16. Liansheng S, Bei Z, Xiaojuan N, Ailing T. Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. Opt Express. 2016; 24(18): 1–17. Available from: https://doi.org/10.1364/oe.24.000499.
17. Tabash F K, Rafiq M Q, Izharrudin M. Image encryption algorithm based on chaotic map. Int J Comput Appl. 2013; 64(13): 1–14. Available from: https://doi.org/10.5120/10691-5600.
18. Khan M, Masood F. A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl. 2019; 78(18): 26203-22. DOI:10.1007/s11042-019-07818-4.
19. Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul. 2012; 17(7): 2943–59. DOI:10.1016/j.cnsns.2011.11.030.
20. Christof Paar, Jan Pelzl, Bart Preneel. Understanding Cryptography: A Textbook for Students and Practitioners. Springer-Verlag. Berlin. Heidelberg 1st edition 2010.
21. Ahmad J, Ahmed F. Efficiency Analysis and Security Evaluation of Image Encryption Schemes. IJVIPNS. 2012; 12(4): 18-31.
22. Chong F, Jun-Bin H, Ning-Ning W. A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy. Entropy ISSN 1099-4300. 2014; 16(2): 770-88. DOI:10.3390/e16020770
23. Mohammed A Shreef, Haider K Hmood. Image Encryption using Lagrange-Least Squares Interpolation. IJACSIT. 2013; 2(4): 35-55. Available from: http://ssrn.com/abstract=2376654
24. Nehal A Mohamed, Mostafa A El-Azeim, Alaa Z. Improving Image Encryption using 3D Cat Map and Turing Machine. IJACSA. 2016; 7(1): 208-15. DOI:10.14569/IJACSA.2016.070129.
25. Salim KG, Al-alak SM, Jawad MJ. Improved Image Security in Internet of Thing (IOT) Using Multiple Key AES. Baghdad Sci J. 2021;18(2):04-17.
26. Tawfeeq FG, Abdul-Hadi AM. Improved throughput of Elliptic Curve Digital Signature Algorithm (ECDSA) processor implementation over Koblitz curve k-163 on Field Programmable Gate Array (FPGA). Baghdad Sci J. 2020 Sep 8;17(3 (Suppl.)):10-29.

# تقنية جديدة لنظام تشفير البيانات الآمن بالأعتماد على إنشاء صورة مفتاح فوضوية

**مصطفى ضياء الحسني**

قسم الحاسوب، كلية العلوم، الجامعة المستنصرية، بغداد، العراق.

**الخلاصة:**

أحدثت التطورات في تكنولوجيا المعلومات والاتصالات، خلال العقود الماضية، تغييراً كبيراً في نمط نقل معلومات الأشخاص عبر الإنترنت/الشبكات أو تخزينها. لذا، فإن أحد التحديات الرئيسية هو الحفاظ على هذه المعلومات بصورة آمنة ضد الهجمات. أدرك العديد من الباحثين والمؤسسات أهمية وفوائد التشفير في تحقيق الكفاءة والفاعلية بمختلف جوانب الاتصال الآمن.يتبنى هذا العمل تقنية جديدة لنظام تشفير البيانات الآمن على أساس نظرية الفوضى. تولد الخوارزمية المقترحة مصفوفة مفاتيح ثنائية الأبعاد لها ذات أبعاد الصورة الأصلية والتي تتضمن أرقاما عشوائية تم الحصول عليها من الخريطة الفوضوية اللوجستية أحادية الأبعاد وفق معطيات معاملات التحكم، والتي تتم معالجتها بعد ذلك من خلال تحويل الأجزاء العشرية منها عن طريق دالة إلى مجموعة من الأرقام غير المتكررة التي تؤدي إلى عدد هائل من الاحتمالات الغير قابلة للتوقع (مفكوك ناتج ضرب الصفوف في الأعمدة). يتم إجراء بعثرة مزدوجة للصفوف والأعمدة لقيم الأرقام لعدد محدد من المراحل. بعد ذلك، يتم تنفيذ عمليات XOR بين مصفوفة المفاتيح والصورة الأصلية، والتي تمثل حلاً فعالاً لتشفير البيانات لأي نوع من الملفات (النصية، الصورية، الصوتية، الفيديوية، ... إلخ).أثبتت النتائج أن تقنية التشفير المقترحة تعتبر جدا واعدة وفقا لمعايير القياسات الأمنية حيث أدت إلى تسطيح Histogram للصور المشفرة مقارنة بما هو عليه بالصور الأصلية، في حين أن متوسطات MSE عالية جدا (10115.48) و PSNR منخفضة جدا (8.17)، إلى جانب مؤشر Correlation هو قريب من الصفر و Entropy القريبة من 8 (7.997).

**الكلمات المفتاحية:** نظام التشفير الفوضوي، تشفير البيانات، البعثرة المزدوجة المراحل، توليد الصورة المفتاحية.