Al-Qadisiyah Journal of Pure Science

Volume 25 | Number 4 Article 12

10-7-2020

New Image Encryption Based on Pixel Mixing and Generating Chaos System

Mohaimen Hassan
Computer Science Department, University of Technology, Baghdad, Iraq, cs.19.61@grad.uotechnology.edu.iq

Alaa Kadhim
Computer Science Department, University of Technology, Baghdad, Iraq, 110030@uotechnology.edu.iq

Recommended Citation

Hassan, Mohaimen and Kadhim, Alaa (2020) "New Image Encryption Based on Pixel Mixing and Generating Chaos System," *Al-Qadisiyah Journal of Pure Science*: Vol. 25: No. 4, Article 12.
DOI: 10.29350/qjps.2020.25.4.1182
Available at: https://qjps.researchcommons.org/home/vol25/iss4/12

Al-Qadisiyah Journal of Pure Science

QJPS

ISSN(Printed): 1997-2490 ISSN(Online): 2411-3514

DOI: /10.29350/jops.

http://qu.edu.iq/journalsc/index.php/JOPS

New Image Encryption Based on Pixel Mixing and Generating Chaos System

Authors Names

a. Mohaimen Hassan
b. Alaa Kadhim

Article History

Received on: 5/8/2020
Revised on: 27/9 /2020
Accepted on: 2/ 10/ 2020

Keywords:

Encryption Image,

Lorenz map,

dispersion of color points.

DOI: https://doi.org/10.29350/jops.2020.25.4.1182

ABSTRACT

This paper presents new encryption by utilizing the image dispersion principle, depending on the Lorenz chaotic Map, the chaos theory is unpredictability and vulnerable initial states as one of the dynamic cryptography methods as suitable for using cryptographic applications. to disengage the color of pixels (Red, Green, Blue). The encryption process is divided into three basic steps. The first step is the process of mixing pixels for each color channel vertically and horizontally. The second step is to split the image into four regions for each color channel where the color pixels are mixed for each region (horizontal, vertical, main diameter, and secondary diameter) finally was used the XOR process. Because the three-channels (R, G, B) encryption process is simultaneous, the process takes only Milliseconds to encryption and decryption images. The experiments demonstrate that the information security capabilities will be both safe more efficient, the result of our analysis of picture quality evaluation, differential attacks number of changing pixel rate (NPSR) and unified averaged changed intensity (UACI), Pixels correlation shows the quality and strength of encryption processing, Entropy show good results.

1. Introduction

The security of information is an enduring topic. In ancient times, when valuable text content was spread over a long period to other individuals, it became a complicated and necessary task to avoid a leak of original text information. Many steganographic and encryption approaches have been suggested to deal with this problem. However, the visual image, a media file, is increasingly used, stored, and interacted with the advancement of new technologies, For eg, medical image, grayscale, color, binary image, etc. Hence it is an important and urgent task to secure this sort of information [5, 14]. Chaos structures provide several features for cryptographing, including pseudo-randomness [13], flexibility to the initial value, responsiveness to parameters, ergodicity, and unpredictability [10]. Encryption algorithms that incorporate the properties of chaos processes have thus been one of the highlights in informatics and cryptography over the last few years. Encryption applications like DNA [21] and hash function [3] also can using for encryption images. In addition, the system of space-time chaos has better properties than those of low-dimensional chaos, to protect digital images, researchers have developed a number of techniques, such as data hiding [31], watermarking [15], and encryption [18,31]. And protracted with multiple images [29], existing chaotic maps [2] can be divided into two categories: one-dimensional (1D) chaotic maps [4,25] and multi-dimensional (MD) chaotic maps [27,2,4]. 1D chaotic maps normally include one variable and a number of parameters. For instance, the Logistic, Sine, and Tent maps, and can combine multiple chaotic maps as hybrid chaotic maps [33,16,17].

According to Mohamed et al. [12] proposed new confusion and diffusion method depending on skew tenet map, he separates the plain image in sectors each sized 1×256 pixel and encrypted the MSE and PSNR show good result. Finally, according to Priya et al. [26] suggested a new way for image encryption she makes a new chaotic

a Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: cs.19.61@grad.uotechnology.edu.iq.

b Computer Science Department, University of Technology, Baghdad, Iraq, E-Mail: 110030@uotechnology.edu.iq.

map by enhanced logistic map and scrambled and zigzagged RGB image (255×255x3) by rotated anti-clockwise 90 degrees PSNR and UACI has been good results.

Here, in this paper shows how to create a new proposal in the image encryption process, and this proposal distracting pixels after separating the image into three channels and rotated each channel, rotated operation based on the sequence of three-dimensional Lorenz map outcome, this proposed added a higher degree of security and more accurate encoding, in time analysis experimental of proposal recorded only take few milliseconds for image encryption and decryption, the differential attacks' analysis NPCR and UACI show fair result, and the MSE and PSNR had shown also good results, our proposal make the parameters of the permutation and diffusion process related with cipher image so that the encryption algorithm can resist with the plain image so that the encryption algorithm can resist chosen ciphertext attack.

the rest of paper shown as following, Section 2 show the methods using contain methods that used in our algorithm, Section 3 described our algorithm for encryption image processing, Section 4 represent show experimental results of our proposed method and compare with previous works, finally discussion a conclusion remarked in Section 5.

2. Chaos Theory

Chaos theory depend on initial conditions sensitively. This means that when two copies of the system differ very small, the two systems will differ and become very distinct after a reasonably short period of time.

•Lorenz map

The Lorenz system [24], which Edward Lorenz researched for the first time in 1960, is a dynamic system defined by the nonlinear system of ordinary equations:

$$\begin{aligned} x_{n+1} &= \alpha(y_n - z_n), \\ y_{n+1} &= rx_n + x_n z_n - y_n, \\ z_{n+1} &= x_n y_n - bz_n \end{aligned} \quad \dots (1)$$

these variables α, r, b is referred to as control parameters while x, y, z is referred to as status variables, Equation (1) is describe a specified control parameters and initial values x_0, y_0, z_0 of the state variables; other methods that also apply.

3. Proposal algorithm for image Encryption

Our proposal contains and extracting the three channels from the image and rotate each channel difference directions as see illustrate in figures and algorithms.

• Encryption Method

In encryption process pike plain image, in figure 1, the work encryption technique was illustrated, every pixel in an image was divided into three channels for the purpose of increasing dispersion in the image to achieve the principle of diffusion after that each channel present (red, green, and blue), after that entered to the first step of the process. Dispersing each row or column was rotated sequentially so that the rotation of the first column was dependent on the output of the first-row rotation this process is done until the end of all rows and columns as shown in figure 3, then in the second step the image was divided equally into four regions for each channel Chromatic (left upper, right upper, right lower, left lower) so that the first region all row ware rotated the left, and the second region all the secondary diameter is rotated to the left, and the third region all the columns are rotated upward and finally the fourth part are all the main diameter is rotated towards the left as shown in figure 4. Finally, xor was done with all channels to increase the dispersion strength as shown in figure 5. Finally, the three channels are reconfigured into a color image to be the encoded image. As figure 6 shows all the steps where the original image 6.a and 6.b the step one and tow,6.c show the third step and 6.d The encoded images represent the final encryption image. The decoding process is the same mechanism, but the sequence of steps from bottom to top show in figure 2, algorithm 1 shows the encryption system and algorithm 2 shows a decryption system.

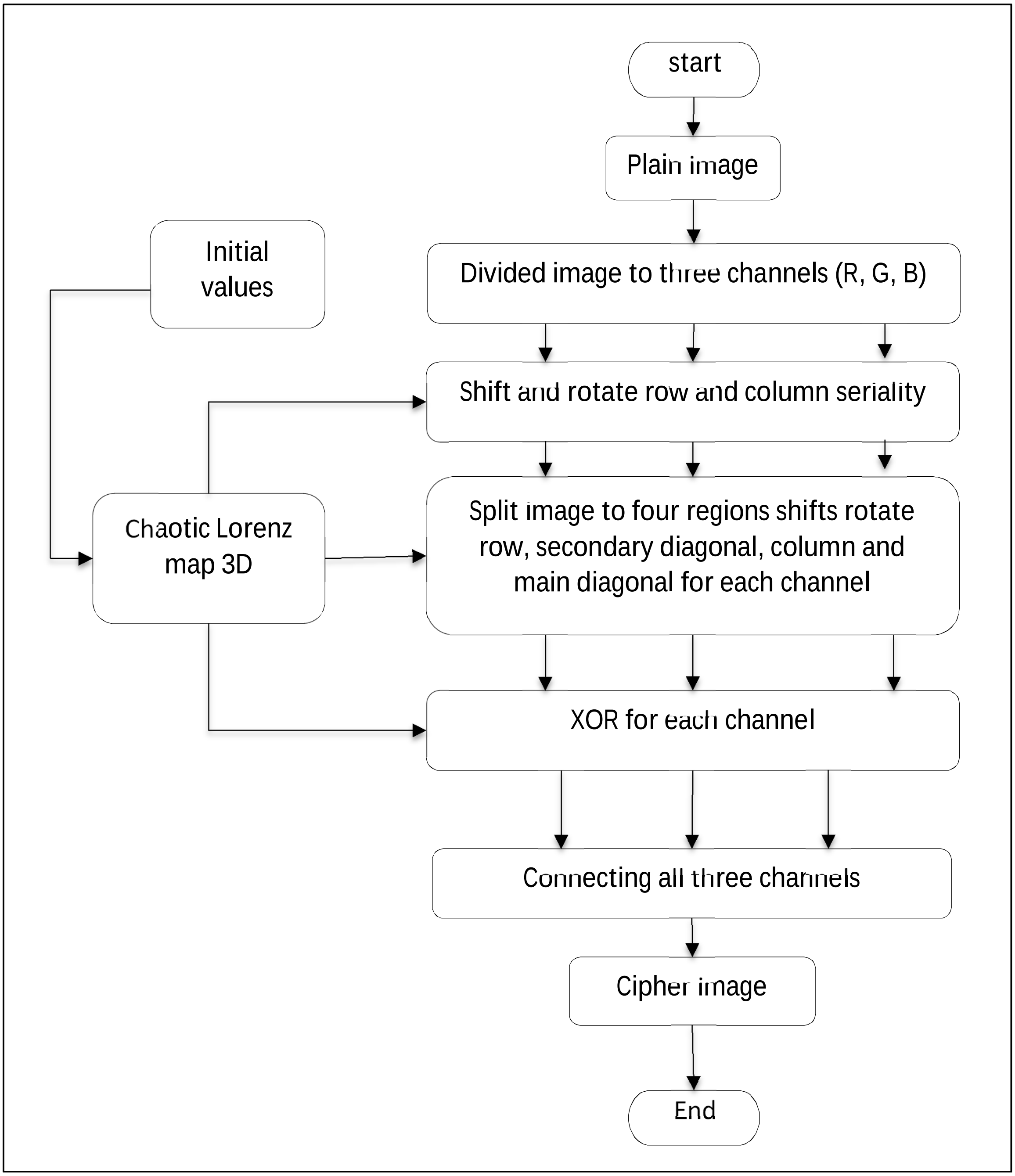

start
Plain image
Initial values
Divided image to three channels (R, G, B)
Shift and rotate row and column seriality
Chaotic Lorenz map 3D
Split image to four regions shifts rotate row, secondary diagonal, column and main diagonal for each channel
XOR for each channel
Connecting all three channels
Cipher image
End

Fig.1: Encryption system

Algorithm (1): Encryption System

```
Input: Plain Image.
Output: Cipher Image.
Begin
    Step1: Get image.
    Step2: Split image to three channels (R, G, B).
     Step2.1: Shift rotate row column
        1.Take X sequential from Lorenz chaotic 3D (each channel using
            different value).
        2. Shift rotate left first row by take first value from Lorenz map and shift
            rotate.
        3. Shift rotate up first column by take second value from Lorenz map
            and shift rotate (using the result from row shifting).
        4. Do these shift processing until end image from each channel.
    Step2.2: Shift rotate left the four regains
        1. Split image four areas for each channel.
        2. Take Y sequential from Lorenz chaotic 3D (each channel using
            different value).
        3. First area shift rotates left row by take values from Lorenz map and
            shift rotate.
        4. Second area shift rotates left second diagonal by take values from
          Lorenz map and shift rotate.
        5. Third area shift rotates up columns by take values from Lorenz map
            and shift rotate.
        6. Fourth area shift rotates left main diagonal by take values from Lorenz
            map and shift rotate.
        7. Do these shift processing for all areas and channels until ending size.
    Step2.2: XORed image
        1. Take Z sequential from Lorenz chaotic 3D (each channel using
            different value).
            2. With using XOR operation every pixel with Z map, to each channel
               using different Z map.
            3. the cipher image is final step now the cipher image is ready.
      Step3: Merge all three channels (R, G, B).
    Step4: Get cipher image.
End
```

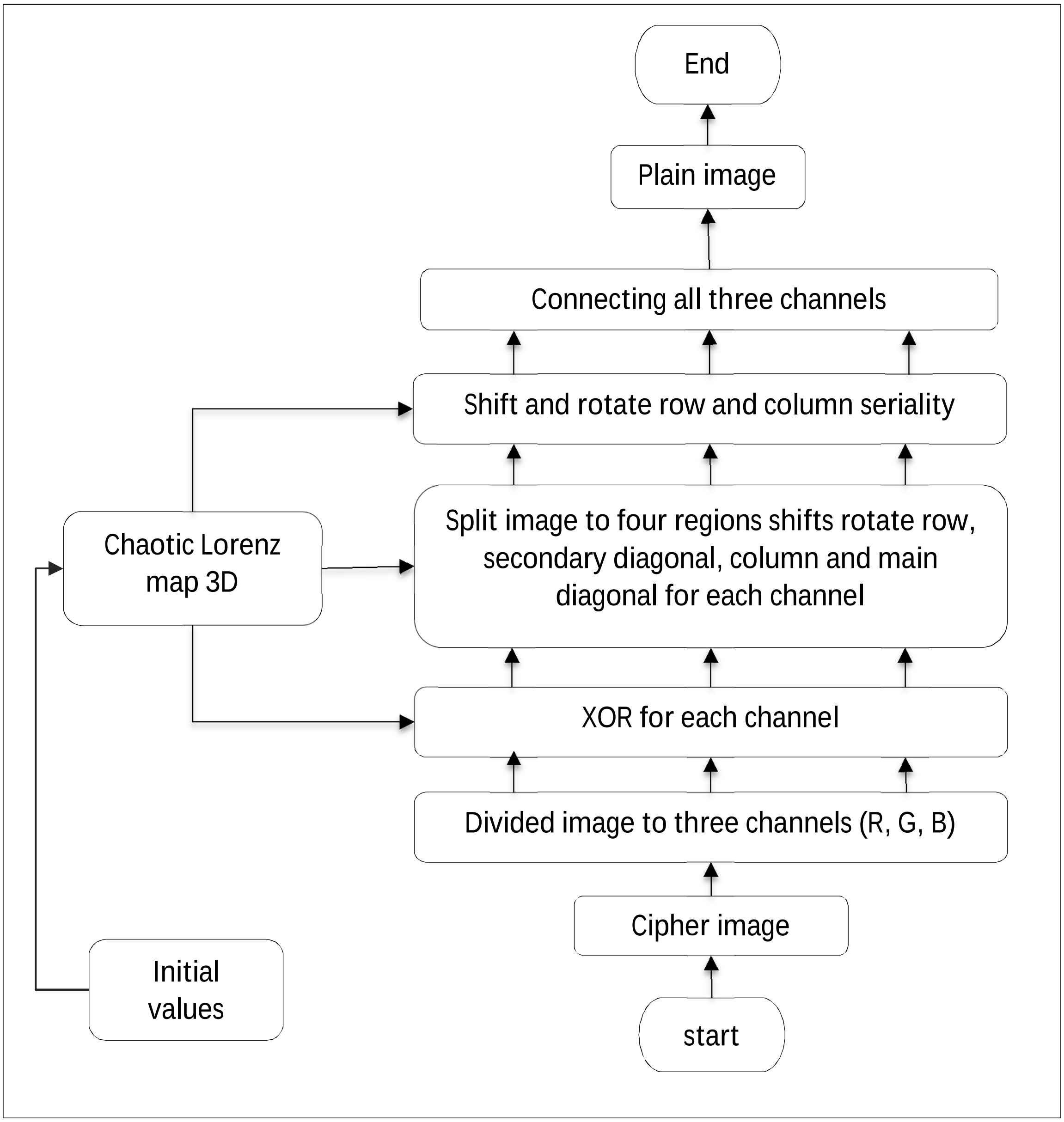

End
Plain image
Connecting all three channels
Shift and rotate row and column seriality
Chaotic Lorenz map 3D
Split image to four regions shifts rotate row, secondary diagonal, column and main diagonal for each channel
XOR for each channel
Divided image to three channels (R, G, B)
Cipher image
Initial values
start

Fig.2: Decryption System

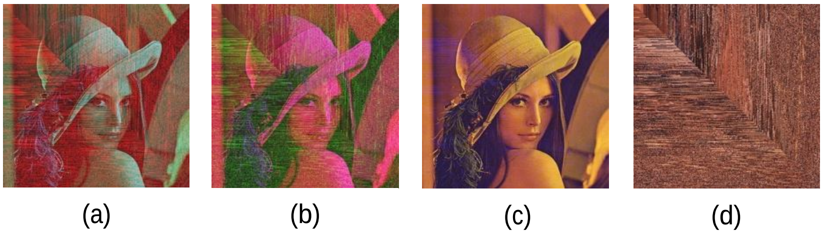
Algorithm (2): Decryption System

```
Input: cipher Image.
Output: plain Image.
Begin
    Step1: Get cipher image
    Step2: Split image to three channels (R, G, B).
        Step2.1: XORed image
            1.Take Z matrix from Lorenz chaotic 3D (each channel using different value) using same initial value with using in encryption processing.
            2. Using XOR operation every pixel with Z map, to each channel using different Z map.
        Step2.2: Shift rotate left the four regains
            1. Take Y sequential from Lorenz chaotic 3D (each channel using different value) same way that using in encryption.
            2. First area shift rotates right row by take values from Lorenz map and shift rotate.
            3. Second area shift rotates right second diagonal by take values from Lorenz map and shift rotate.
            4. Third area shift rotates down columns by take values from Lorenz map and shift rotate.
            5. Fourth area shift rotates right main diagonal by take values from Lorenz map and shift rotate.
            6. Do these shift processing for all areas and channels until ending size.
            7. Concatenation the four areas and send to next step.
        Step2.3: Shift rotate row column
            1. Take X sequential from Lorenz chaotic 3D (each channel using different
               value), same generate chaotic map way.
            2. Shift rotate right last column by take last value from Lorenz map and
               shift rotate.
            3. Shift rotate last row by take before last value from Lorenz map and
               shift rotate (using the result from column shifting).
            4. Do these shift processing until first column and row in image from each
               channel.
    Step3: Merge all three channels (R, G, B).
    Step4: Get plain image.
End
```

4. Experimental results

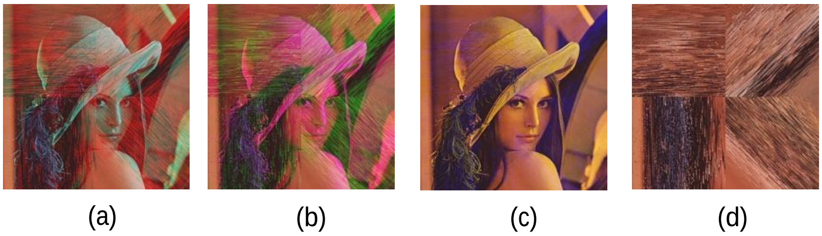
This segment discusses the effects of the systems suggested and analyzes the encryption pictures. Confusion is an important feature of the cryptographic block chip; any picture has blocks translated into cipher blocks of the message and is thus focused on the key. Each primary change indicates the output of each cipher. The diffusion is the block cryptographic cipher; by of digit of the plaintext and by hidden key digit, those ciphertext numbers can be calculated. The two models are very common and casual. Initial condition and controller parameters on Lorenz map α=10, r=28, and β=8/3.

As see in figure 3 use first encryption step and figure 4 and 5 show second and third step, all steps show and how each channel processing for each step, in figure 6 show all steps of Encryption Image



(a) (b) (c) (d)

Fig.3: Encryption Image (first step), **(a)** red channel, **(b)** green channel, **(c)** blue channel and **(d)** color image



(a) (b) (c) (d)

Fig.4: Encryption Image (second step), **(a)** red channel, **(b)** green channel, **(c)** blue channel and **(d)** color image

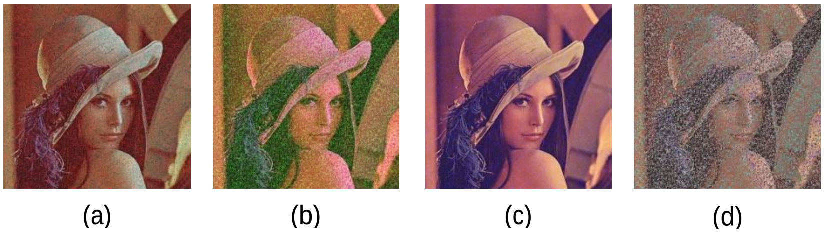


Fig.5: Encryption Image (third step), **(a)** red channel, **(b)** green channel, **(c)** blue channel and **(d)** color image

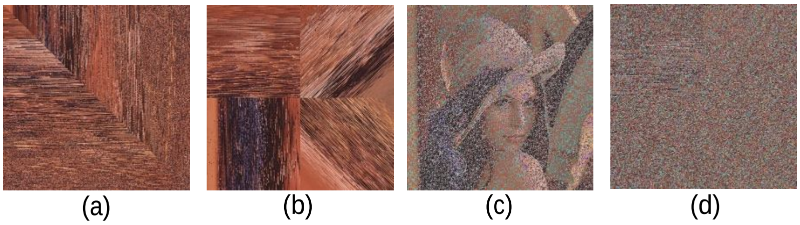


Fig.6: (a) first step, **(b)** second step, **(c)** third step and **(d)** encryption image

In figure 6, the encryption bitmap image has size 755*755 pixels and 1.7 Mb, consuming only 5,251 seconds to encrypt and 5,357 seconds in decrypt an image, because a big difference between plain and cipher image MSE between plain image (a) and decryption image (c) equal to 5498.22 that lead to PSNR equal to 10.72858, NC equal 1 because there is no deformation in the decoded image between plain image (a) and decryption (d), and entropy between plain image (a) and cipher image (c) equal to 7.9940, NPSR and UACI are 0.99309, 0.3310between plain image (a) and cipher image(c), other encryption and decryption result can see in figure 7, the size of a paper image is (256x256)pixel, Barbara image(512x512)pixel, Baboon image(560x560) pixel and finally monarch image(900x900) pixel.

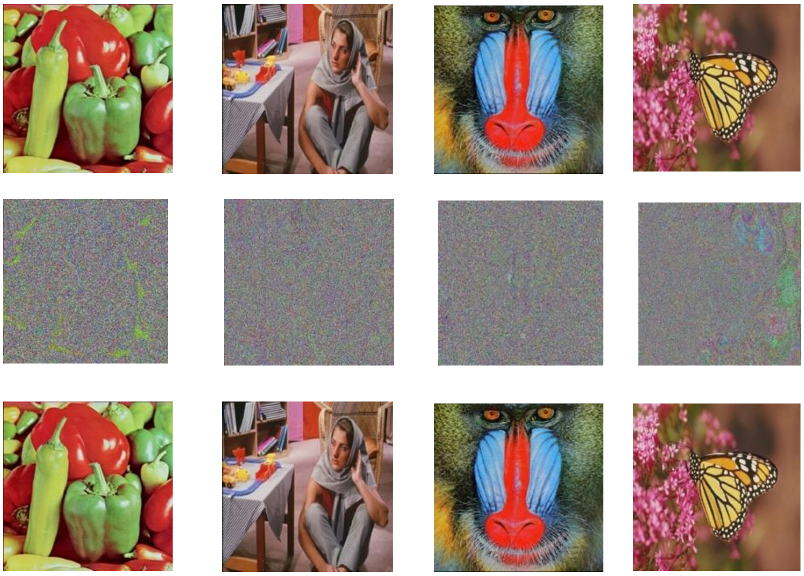


Fig.7: Encryption and decryption **(a)** Paper, **(b)** Barbara, **(c)** Baboon and **(d)** Monarch

Our proposed approach used different sizes and quality images tests for evaluated the efficiency and security of a proposed system. by Picture Quality Evaluation (PQE) [23], Histogram Analysis Randomness Tests and Evaluation of Image Quality by Entropy.

4.1. Picture Quality Evaluation (PQE) Metrics

For show experimental an encoded and decoded image quality measurement, The picture quality evaluation (PQE) must be used, as shown below with our images, these metrics implemented applied our proposal, table 1 show twelve measurements in MSE should be big number because it shows differently between plain image and cipher image with all images show big numbers, the reason PSNR results show with these numbers to calculate ratio max probable signal power and noise power, AD show the difference between plain and cipher image and divided by MSE, MD show maximum error between plain and cipher image convert both images to gray image with rang (0-255), NC must be shown in all images 1 between plain image and decryption image should be big number because it shows differences between plain image and cipher image, MAE show absolute same idea MSE instead of the square difference between plain and decryption image calculate absolute, NAE show 1 if plain and decryption have no deformation the but the result evaluation show less one, SNR Show all-electric signals between plain and encryption image, SIM show similar results between the original image and encoder image the same idea MSE, and EQ show encryption quality with all images show big results.

Table 1 - PQE Metrics

name	MSE	PSNR	AD	MD	NC	MAE	NAE	SC	NSR	SIM	CC	EQ
Paper	7217.26	9.54708	-2.24890	238	1	33.48825	0.562332	0.89321	-0.49811	1.35E+02	0.004093	1.77E+04
Barbara	7369.17	9.45661	-5.99177	241	1	31.954	0.59543	0.851694	-0.06994	1.30E+02	0.01467	7.16E+04
Baboon	4944.42	11.18965	-14.8767	188	1	20.89631	0.552606	0.73598	-1.3366	1.16E+02	0.000917	6.94E+04
Lena	5148.70	11.01382	-19.4692	231	1	19.264423	0.606295	0.693848	-1.58098	1.12E+02	0.002805	1.74E+05
Monarch	4351.23	11.74468	-14.3720	212	1	18.997913	0.495405	0.763527	-1.17439	1.17E+02	-.001486	1.66E+05

4.2. Running time of Encryption and Decryption Image

Table 2 and figure 8, shows time complexity with all images, time take few milliseconds for encryption and decryption.

Table 2 - time complexity milliseconds

name	diminution	size	Encryption time	Decryption time
Paper	256x256 pixel	201 KB	0.462	0.541
Barbara	512x512 pixel	786 KB	2.226	2.273
Baboon	560x560 pixel	941 KB	2.913	3.013
Lena	755x755 pixel	1.7 MB	5.251	5.357
Monarch	900x900 pixel	2.4 MB	7.725	7.853

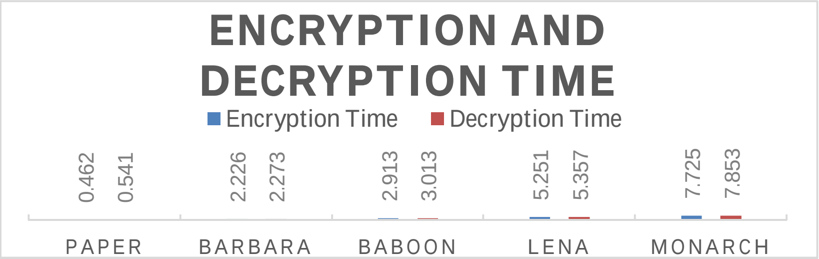


Fig.8: Encryption and decryption time

And in table 3 show the compare encryption speed in milliseconds with other proposed system, we see our proposed is faster than others for difference image sizes.

Table 3 - time complexity milliseconds among different algorithms

Image size	paper (256x256)	Barbara (512x512)
Our Proposed	0.462	2.226
Ref [6]	0.823	3.253
Ref [7]	1.256	4.828
Ref [9]	1.205	4.750

4.3. Differential Attacks Analysis

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) [19] are two farthest popular quantities used to estimate the strength of image encryption algorithms/ciphers with respect to differential attacks, can describe in table 4.

Table 4 - randomness tests

name	NPSR	UACI
Paper	0.992	0.333
Barbara	0.996	0.336
Baboon	0.996	0.336
Lena	0.997	0.337
Monarch	0.993	0.332

With table 5 show NPSR between our proposed and [12,32,18,19] proposals, and table 6 describe UACI between our proposed and [12,32,18,19] proposals.

Table 5 - NPSR comparisons among different algorithms

Image	Barbara	Baboon	Lenna
Our Proposed	0.996	0.996	0.997
Ref [27]	non	0.996	0.994
Ref [32]	non	0.996	0.996
Ref [12]	non	non	0.990
Ref [26]	0.996	0.996	0.996

Table 6 - UACI comparisons among different algorithms

Image	Barbara	Baboon	Lenna
Our Proposed	0.996	0.996	0.336
Ref [27]	non	0.996	0.336
Ref [32]	non	0.996	0.334
Ref [12]	non	non	0.335
Ref [26]	0.996	0.996	0.335

4.4. Uniformity Analysis of Image Pixel

The pixel strength diffusion measurements for a picture are represented in a histogram from a picture. A secure encryption system should provide identical histograms to survive statistical attacks. The histogram in Figure 9(a, b, c, d) depicts Lena, Pepper, Barbara, Baboon and Pepper's regular and encrypted pictures. We evaluated from Figure 9(a, b, c, d) that the histograms of regular images are not accurate, while the histograms of the digital images that have been encrypted are reliable. The uniformity of the pixel heights of the histograms of the encrypted image makes it hard to find an insight into the maximum information region for attackers.

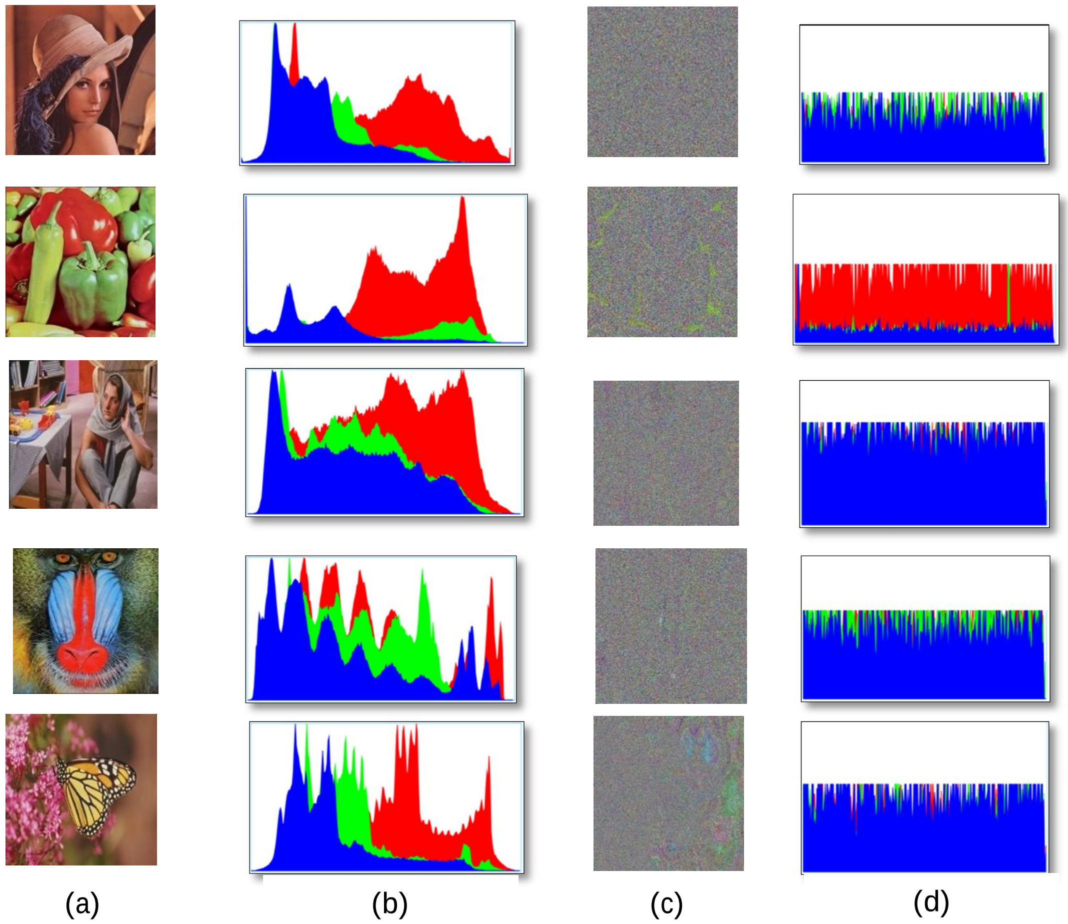


Fig.9: histogram of Lena, Pepper, Barbara, Baboon and Pepper (a) plain image, (b) histogram of plain image, (c) cipher image, (d)histogram of cipher image

4.5. Pixels Correlation Analysis

Adjacent pixels have a rather strong correlation in the images. The existence of neighboring pixels in an image will be removed by a high-security encryption algorithm. The formula for calculating the association of neighboring pixels is the correlation coefficient. The smaller the absolute value, the lower the correlation across adjacent pixels, in table 7 show calculate correlation coefficients between an original image and an encoded image and its corresponding encoded image the result for Lena image is listed in table 7.

Table 7- CC comparisons among different algorithms

Image	Our proposed	Ref [20]	Ref [11]	Ref [8]	Ref [28]	Ref [1]
Lena	0.009426	0.531	0.000249	0.005497	-0.00114	0.000329

4.6. Information Entropy

The entropy of information also is one of the most significant characteristics for calculating the randomness of the cipher file. The H(s) entropy in a source is given by:

$$H(s) = -\sum_{i=0}^{2^n-1} p(s_i)\ \log_2 p(s_i)$$

where p(si) corresponds to the probability of the s. Entropy would preferably be H(s) = 8 for a 2 –1 gray cipher-8 picture displaying random knowledge, table 8.

Table 8- information entropy

Paper	Barbara	Baboon	Lena	Monarch
7.993	7.994	7.995	7.997	7.994

The entropy in table 9 close to the ideal value 8. We thus assume that the algorithm suggested is strongly random.

Table 9 - information entropy for cipher image among different algorithms

Image	Our proposed	Ref [19]	Ref [22]	Ref [10]
Lena	7.997	7.997	7.997	7.997

5. *Conclusion*

This paper implemented a high performance and efficient image security encryption method that based on a chaotic system and shuffling scheme, It consists of three steps for dispersion principle to disengage the color points, the color point divided to three colors (red, green, and blue) and scrambled all color channel with all directions, this process depended on Lorenz chaotic map three-dimensional, first step shifting and rotate (row and column in series) each pixel in each channel, the second step split to four regions shift rotate each region with different directions. final step xored operation. the security analysis performs was sensitive with initial value speed in encryption processing, compared with some other encryption schemes the NPSR and UACI show high efficiency, also the entropy analysis, and the histograms of the encrypted image makes it hard to find an insight into the maximum information region for attackers. Because of the high efficacy of our suggested encryption method, we will explore its implementations in more methods like using high dimensional chaotic maps and using with videos.

References

[1] Ahmad, M.; Al Solami, E.; Wang, X.Y.; Doja, M.; Beg, M.; Alzaidi, A. ‘Cryptanalysis of an Image Encryption Algorithm Based on Combined Chaos for a Ban System, and Improved Scheme using SHA-512 and Hyperchaos’. *Symmetry*, Vol. 10, PP. 266, Jul.2018.

[2] Ahmed T., E.M.E.Mostafa, Yasser F. ,Ahmed B. ‘Using Chaotic Maps to Enhance RSA Public Key Cryptography’, *Sci.Int.(Lahore),* Vol. 30, PP. 711-715, Sep.2018.

[3] Alaa K Farhan, MAAJ Ali. ‘Database protection system depend on modified hash function’. *2nd International Conference of Cihan University-Erbil on Communication Engineering and Computer Science*, Mar.2017.

[4] Alaa Kadhim F,Hakeem Emad M. ‘Mouse Movement with 3D Chaotic Logistic Maps to Generate Random Numbers’ *Diyala Journal For Pure Science*, Vol. 13, PP. 24-39, Apr.2017.

[5] Alaa Kadhim, F., Abdul-Majeed, G. H., & Ali, R. S. ‘Enhancement CAST block algorithm to encrypt big data’. *Annual Conference on New Trends in Information & Communications Technology Applications (NTICT),* Mar.2017.

[6] Amjad H. Muhammad J. ‘An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping’, *Symmetry*, Vol. 11, PP. 437, Mar.2019.

[7] Balajee M., J. M. Gnanasekar, ‘Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output’, *TEM J.*, Vol. 5, PP. 67–75, Mar.2016.

[8] Bashir, Z.; Watrobski, J.; Rashid, T.; Zafar, S.; Salabun, W. ‘Chaotic dynamical state variables selection procedure based image encryption scheme’. Symmetry, Vol. 9, PP. 312, Dec.2017.

[9] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. ‘Secure image encryption algorithm design using a novel chaos based S-Box’. *Chaos, Solitons & Fractals*, Vol. 95, PP. 92–101, Dec.2017.

[10] Chai, X. ‘An image encryption algorithm based on bit level Brownian motion and new chaotic systems’. *Multimedia Tools and Applications*, Vol. 76, PP. 1159-1175, Nov.2015.

[11] Congxu Z., Guojun W., Kehui S. ‘Cryptanalysis and Improvement on an Image Encryption Algorithm Design Using a Novel Chaos Based S-Box”, *Symmetry*, Vol. 10, PP. 399, Sep.2018.

[12] Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. ‘A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map’, *Procedia Computer Science*, Vol. 127, PP. 539–548, Mar.2018.

[13] F. Alaa K., Hakeem Imad M.’Quantum Random Bits Generator based on Phase Noise of Laser’. *Journal of Engineering and Applied Sciences*. Vol. 13, PP. 629-633, 2018.

[14] Farhan, A. K., Al-Saidi, N. M. G., Maolood, A. T., Nazarimehr, F., & Hussain, I. ‘Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder’. *Entropy*, Vol. 21, PP. 958, Sep.2019.

[15] Fatema, M., Maheshkar, V., Maheshkar, S., & Agarwal, G. ‘Tamper Detection Using Fragile Image Watermarking Based on Chaotic System’, *Lecture Notes on Data Engineering and Communications Technologies*, PP. 1–11, Apr.2018.

[16] Hua, Z., & Zhou, Y. ‘Image encryption using 2D Logistic-adjusted-Sine map’, *Information Sciences*, Vol. 339, PP. 237–253, Jan.2016.

[17] Hua, Z., Jin, F., Xu, B., & Huang, H. ‘2D Logistic-Sine-coupling map for image encryption’, *Signal Processing*, Vol.149, PP. 148–161, Mar.2018.

[18] Hua, Z., Zhou, Y., & Huang, H. ‘Cosine-transform-based chaotic system for image encryption’. *Information Sciences*, Vol. 480, PP. 403–419, Dec.2019.

[19] Hui L,Bo Z.,Linquan H. ‘Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling’, *Entropy 2019*, Vol. 21, PP. 343, Mar.2019.

[20] Kadhim, A., & Mohamed, R. M. ‘Visual cryptography for image depend on RSA & AlGamal algorithms’. *2016,9-10 May Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, May. 2016.

[21] Kadhim, F. A., Majeed, G. H. A., & Ali, R. S. ‘Proposal new s-box depending on DNA computing and mathematical operations’. *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, May.2016.

[22] Liu, H., & Jin, C. ‘A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence’, *3D Research*, Vol. 8, Jan.2017.

[23] Mrak, M., Grgic, S., & Grgic, M. ‘Picture quality measures in image compression systems’. The IEEE Region 8 EUROCON. *Computer as a Tool*, PP. 233-237, Sep.2003.

[24] Obaida M., Mohammad F., Nouh A., Abedalkareem O. ‘Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys’, *Neural Computing and Applications*, Aug.2017.

[25] Pak, C., & Huang, L. ‘A new color image encryption using combination of the 1D chaotic map’. *Signal Processing*, Vol. 138, PP. 129–137, Sep.2017.

[26] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., & Blažauskas, T. ‘An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map’, *Entropy*, Vol.21, Jul.2019.

[27] Shokouh Saljoughi, A., & Mirvaziri, H. ‘A new method for image encryption by 3D chaotic map’, *Pattern Analysis and Applications*, Vol. 22, PP. 243–257, Nov.2018.

[28] Wang, W.; Si, M.; Pang, Y.; Ran, P.; Wang, H.; Jiang, X.; Liu, Y.; Wu, J.; Wu, W.; Chilamkurti, N.; et al. ‘An encryption algorithm based on combined chaos in body area networks’. *Computers & Electrical Engineering*, Vol. 65, PP. 282–291, Jan.2018.

[29] Xiaoqiang Z., Xuesong W. ‘Multiple-Image Encryption Algorithm Based on the 3D Permutation Model and Chaotic System’, *Symmetry*, Vol. 10, PP. 660, Nov.2018.

[30] Y. Wu, J.P. Noonan, S. Agaian. ‘NPCR and UACI Randomness Tests for Image Encryption’, *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun.* Vol. 2, PP. 31–38, Apr.2011.

[31] Yadav, G. S., & Ojha, A. ‘Chaotic system-based secure data hiding scheme with high embedding capacity’. *Computers & Electrical Engineering*, Vol. 69, PP. 447–460, Feb.2018.

[32] Yong Z. ‘The unified image encryption algorithm based on chaos and cubic S-Box’, *Information Sciences*, Vol. 450, PP. 361–377, Mar.2018.

[33] Zhou, N., Pan, S., Cheng, S., & Zhou, Z. ‘Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing’, *Optics & Laser Technology*, Vol. 82, PP. 121–133, Feb.2016.