3D chaos graph deep learning method to encrypt and decrypt digital image

Daniah Abdul Qahar Shakir, Ali Jbaeer Dawood
University of Anbar, College of Computer Science and Information Technology, Ramadi, Iraq

Article Info

Article history:

Received Aug 8, 2021
Revised Dec 1, 2021
Accepted Dec 15, 2021

Keywords:

3D chaos map
Decryption
Deep learning
Digital images
Encryption
Multimedia

ABSTRACT

We live in technological age development's where many important data transmitted electronically from one device to another and in every place. Deep learning algorithms have facilitated the process of encoding and decoding digital images. Chaotic graph systems, on the other hand, are one of the most recent techniques utilized to encode image data based on the methods of cryptography. The chaos maps are divided into two main aspects, first one deals with the 1D map which requires fewer features and can be developed easily, the second one is the high dimensional map which is more complex than the 1D graph and it requires more features, more parameters, and it is relatively hard to develop. In this paper, we present a method for image encoding and decoding electronically using deep learning, the proposed algorithm was developed by using the hybrid technique of 3D chaos map generation, the best case of the proposed technique gave the following results: The average entropy calculation was (7.4838) before image encryption and (7.9896) after image encryption with average number of pixels change rate (NPCR) of (99.7085%) and the unified average changing intensity (UACI) of (33.2030%) which are the best outcomes when compared to other similar works.

Corresponding Author:

Daniah Abdul Qahar Shakir
Department of Computer Science, University of Anbar
Anbar, Iraq
Email: dan14c1001@uoanbar.edu.iq

1. INTRODUCTION

Securing data communication became a must in the digital era, cryptography is the perfect method to remain the safety of the transmitted data over the communication channels, this field must ensure the four principles of cryptography namely: data confidentiality, integrity, authentication, and data non-repudiation [1]. Various algorithms have been taken into the place of date encryption and decryption specially to protect the multimedia data since these data are the most usable data across the internet [2]. Digital image encoding/decoding methods are widely examined rather than the traditional digital data cryptography methods such as the traditional data encryption standard (DES) algorithms which may not be able to suit the large-scale, highly complex digital images [3].

Machine learning algorithms vary depending on the type and features of the data along with the situation where how the research problem and aim were designed [4]. Data mining and deep learning tools have been given a promising outcome in both classification and clustering learning techniques especially when it comes to large-scale, complex, high dimensional data such as the image encryption and decryption method [5]. The aspect of image security thrives with artificial neural networks that confirm the data confidentiality and accuracy, but it is an expensive tool to implement with complex and sensitive data such as the image [6]. Images carry out huge information which makes it challenging to perform the encoding/decoding algorithms as the original text-based dataset. On the other hand, the image resolution and quality after the decoding process must be unchangeable which a quite challenging task [7], [8].

This paper proposes a modern digital image cryptography method with a chaotic map based on deep learning for an advanced, highly secure, and robust technique. This method ensures that images can be sent safely without worrying about information leakage. Recent works have examined digital image security and proposed different methods to protect the data of the images [9].

- Chen *et al*. [10] implemented artificial neural nets with impulse synchronization technique with nonlinear pulse controller, then developed this modern method to a digital image which showed a highly secure outcome.
- Dridi *et al*. [11] designed a new artificial neural network (ANN) approach that lessens the complexity of the digital medical image cryptography, pixel summation, and exclusive or (XOR) operation was used to ensure the performance of the method which confirms the effectiveness and the robustness of the neural networks.
- Fakhr [12] developed modern compression of key sensing technology with machine learning, it computes the square of the Euclidean distance long with the dot product then test the results using COREL image.
- Daolin *et al*. [13] utilized CryptoNets which are the cryptography with ANN was utilized cloud computing to ensure the safety of the transmitted image, this technique showed a divine result when tested using the modified national institute of standards and technology (MNEST) dataset.
- Hu *et al*. [14] implanted a network called the stack automatic encoder (SAE) to shuffle the coordinates of the pixels into the image which enhanced the encryption process and it showed that this method is robust against brute force attack, differential attack, and statistical attack.
- Hu *et al*. [15] steganography method was produced to enhance the image encoding, carrier image was developed using ANN to ensure that the data remains the same with no update or alter to its information with highly accurate and robust information extraction.
- Lu *et al*. [16] the equations of the second order were switched to the first order with Lyapunov-Krasovskii functional and Jensen's inequality functions along with chaotic ANN method was developed for reliable and efficient image transformation.
- Shifa *et al*. [17] produced advanced encryption standard (AES) technology with the 3 channel images i.e., the colored images rather than changing the image to grayscale first, this contribution has shown ideal information hiding with accurate performance.
- Liu *et al*. [18] chaotic S-Box, logistic-sine system (LSS) schema, and chaotic key were produced in this work which makes the method resistant against the certified public accounts (CPA) and it works perfectly with the real-time encoding of the images.
- Rungruanganukul and Siriborvornratanakul [19] proposed building and training a convolutional neural network from scratch using Google Colab's deep learning framework. The trained network is part of the core artificial intelligence of interactive software games, aimed at encouraging employees to exercise their hands and wrists frequently during the game. The network is trained on a self-collecting dataset of 12,000 images recorded against a static dark background, using simple gestures. The network focuses on classifying still images into one of six predefined gesture classes, handling small changes in size, skin color, position, and hand orientation. This network was designed to be easily calculated with real-time runtime even on the central processing unit (CPU). The network provides 99.68 accuracy in the validation set, with an average accuracy of 78% when tested with 50 different users.

2. METHODOLOGY

Explaining the proposed research methodology will be in detail in this section. Research design and research procedure (in the form Pseudocode) will be illustrated as presented in the following flowchart where the proposed work generated a 3D chaotic map from the concept that originated from the 2D chaotic map of image encryption. After that the original images will be fed one by one to the proposed system to encrypt and decrypt the results, along the process histogram equalization will be implemented which transforms the 3D Image channels to 2D (grey scale). Then applying the image rotation and XOR equations. Finally, hybrid image encryption-decryption technique will be produced. Figure 1 illustrates the entire process,

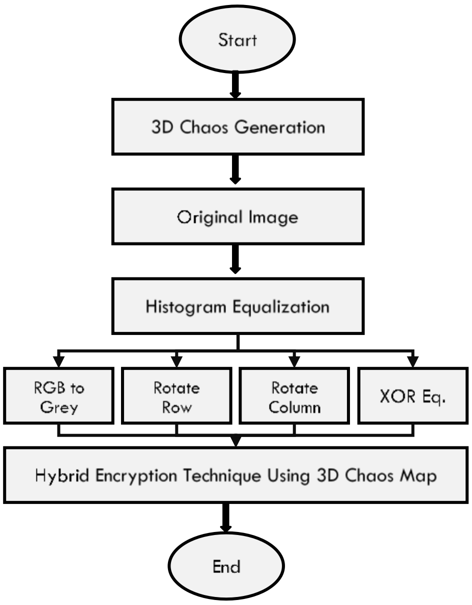


Figure 1. 3D chaotic map with image encryption implantation

2.1. Key generation

1. 3D logistic map is used to produce the behavior of the chaotic map, to reach a 3D chaotic map, 2D Map will be he start point, 2D map was proposed by Liu *et al*. as a 2D logistic map given by the following equations [20],

$$X_{i+1} = \mu_1 X_i (1 - x_i) + y_1^1 y_i^2 \quad (1)$$

$$Y_{i+1} = \mu_2 Y_i (1- y_i) + y_2^1 (x_i^2 + x_i y_i) \quad (2)$$

in this work, 3D key generation consists of three main parameters of the key which are (x, y, and z) along with three symbols (μ, β, and γ) where the values of the mentioned symbols should be in a range from [0 to 1]. The values of each variable is given in Table 1.

The equations on which the chaotic actions were given to the proposed method is illustrated in (3), (4), and (5) [21],

$$X_{n+1} = \mu(1 - x_n) + \beta y_n^2 x_n + \gamma z_n^3 \quad (3)$$

$$Y_{n+1} = \mu(1 - y_n) + \beta z_n^2 x_n + \gamma x_n^3 \quad (4)$$

$$Z_{n+1} = \mu(1 - z_n) + \beta x_n^2 x_n + \gamma y_n^3 \quad (5)$$

Table 1. Variables range values

Symbol	>	<
μ	3.35	3.81
Β	0	0.022
Γ	0	0.015

2. To produce the histogram of the key, an equalization process is given to the grayscale of the original image, where the image has the row and column with A*B dimension only the histogram equalization is given to the variables of the key (x), (y), and (z) as shown in questions (6), (7), and (8),

X=(integer (x*i)) mod A (6)

Y=(integer (y*i)) mod B (7)

Z=(integer (x*i)) mod 256 (8)

where integer values are always set to be greater than 10000, where A and B are equal to 256.

3. Column and Row Rotation: to change the position of the image pixels, it is known that the image is transformed to the grayscale e level and the dimensionality is limited to 2D only with A and B symbols each presents the row and the column. A random number (i) was generated when i1=1000 rotate the row according to (7), and when the random number i3=1000 rotate the column according to (8) with both respect the values of (x') and (y'). In both cases, rotate to the right when chaos is even, otherwise rotating to the left.
4. XOR operation is implanted to the values of the pixels sequence, where the values remain hidden to the attacker unless he/she has the chaotic key, the XOR starts from i5 values after that the image dimension (A*B) shuffled to produce the encrypted image.

2.2. Pseducode

Pseudocode is proposed to implement the work of this paper. It consists of 18 steps. The pseudocode of the overall work is illustrated in the following points:

Start:
Step 1: Set the initial values: key, chaotic behavior symbols.
Step 2: Define the output: encrypted image.
Step 3: Define the input images.
Step 4: Change the 3D image input to 2D image input.
Step 5: Design the image height.
Step 6: Set the encryption phase.
Step 7: Prepare the equations of the initial key conditions.
Step 8: Set the 3D chaotic values to the variables and the symbolic values.
Step 9: Start a for loop to all the random number (i) values.
Step 10: Develop the histogram equalization phase.
Step 11: Set of conditions for row and column rotation.
Step 12: Reshape the image with XOR operation implantation.
Step 13: Start the decryption phase.
Step 14: Set of conditions for row and column rotation.
Step 15: Calculate the entropy.
Step 16: Calculate the coefficient correlation.
Step 17: Calculate number of pixels change rate (NPCR) and unified averaged changed intensity (UACI).
Step 18: Print the outputs.
End

3. Experimantal Results

In this section six main experemntial results will be given in the following tables, in is noted that three different images were utilized during the statistical analysis of these images, matrix laboratory (MATLAB) software was utilized to run the results, the outcomes will be shown in the following sections:

1. Image pixels diffusion results: three images where given (owl, birds, and buterfliy) the original 3D channels of these images are switched to 2D greyscale then their pixels are diffused, as shown Table 2.
2. Histogram Visulazation: from the visulzation of the encrypted image histogram it is visula that the values are distributed over the resultd image evenly which indicates that there is no useful information that can be extracted from the encrypted image, as shown in Tables 3, 4, and 5.
3. The calculation of the entropy: the besst case of the entroy calculation theroitcally is 8 values, the higher the inforamtion entropy embedded into the image the higher uneven values distribution of the results, the entropy was applied to the three images and the entropy of both the original and the encoded image were reistered as mentioned in Table 6.
4. The calculation of the correlation coffiecent: the correlation coefficients between vertically adjacent pixels and horizontally adjacent pixels of an encrypted image are given in Tables 7, 8, and 9.
5. The calculation of NPCR and UACI: the former means that it is the number of changing pixel rate. (NPSCR) That gives tha avarage changed pixels in the encoded image, while the latter indicates that it is the averaged changed intensity (UACI) that gives the avarage different of the encrypted image with respect to its dimentions A*B, the results were examined with the owl image only and it is mentioned in Table 10.
6. Comparision with previous works: this comparision was made with respect to both encryption and sensitiveity analysis with owl image which is the proosed image with our work and with different images from other similr works in the field of image encryption, Tables 11 and 12 show the analysis results.

Table 2. Pixels diffusion results

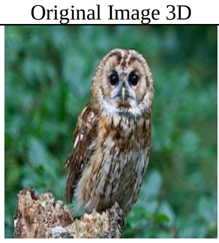
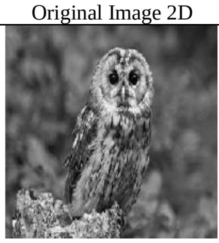
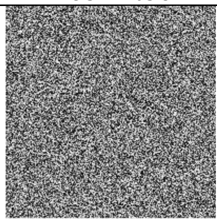
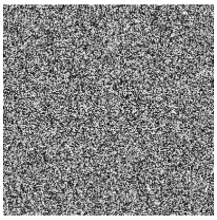
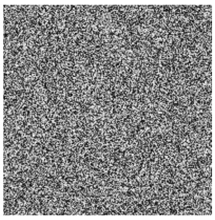
Original Image 3D	Original Image 2D	Pixels Diffusion
		
		
		

Table 3. Histogram visualization of the 1st image

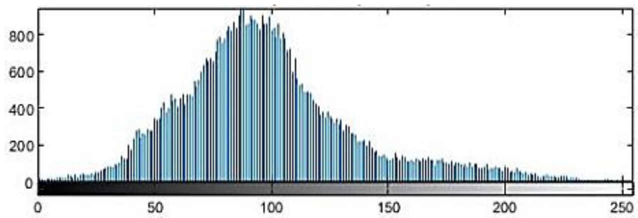
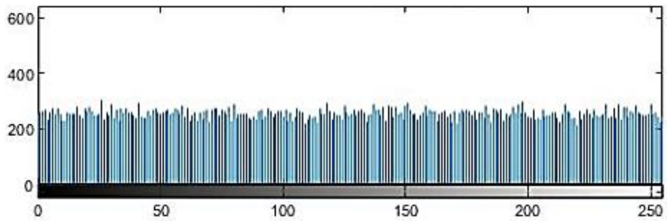
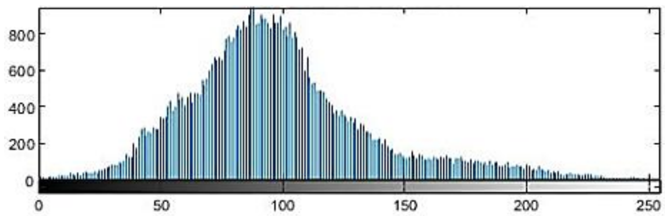
Source	Visualization
Original Image	
Original's Image Histogram	
Encrypted Image Histogram	
Decrypted Image Histogram	

Table 4. Histogram visualization of the 2nd image

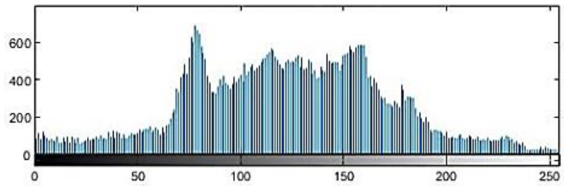
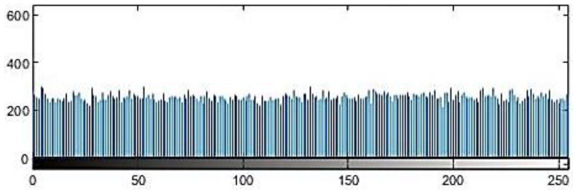
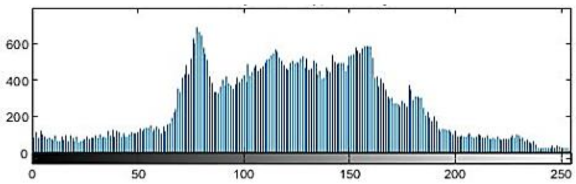
Source	Visualization
Original Image	
Original's Image Histogram	
Encrypted Image Histogram	
Decrypted Image Histogram	

Table 5. Histogram visualization of the 3rd image

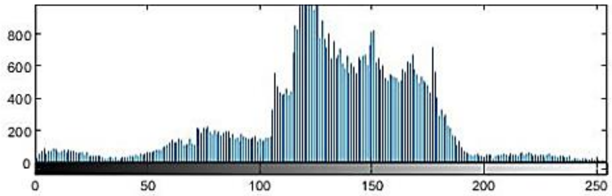
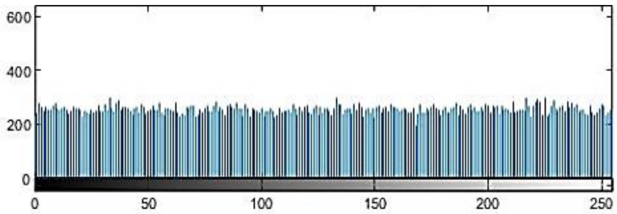
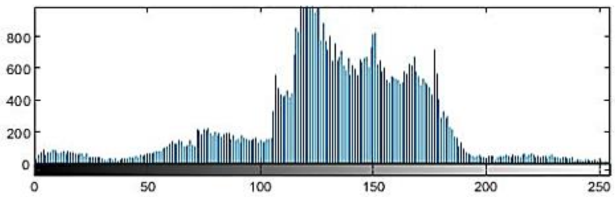
Source	Visualization
Original Image	
Original's Image Histogram	
Encrypted Image Histogram	
Decrypted Image Histogram	

Table 6. Entropy calculation of the implented imges

	Original Entropy	Encrypted Entropy
OW1 Image	7.4838	7.9896
Birds Image	7.2543	7.9887
Butterflies Image	7.6333	7.9894

Table 7. Correlation coefficient calculation of owl image

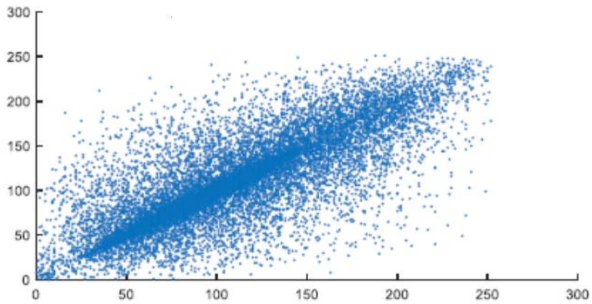
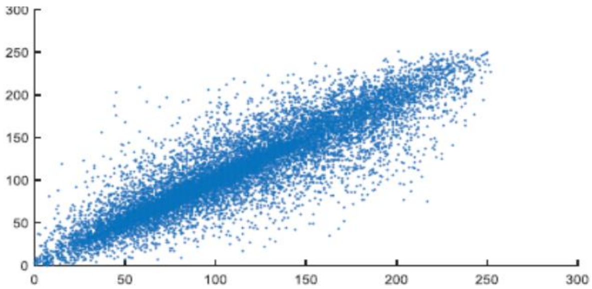
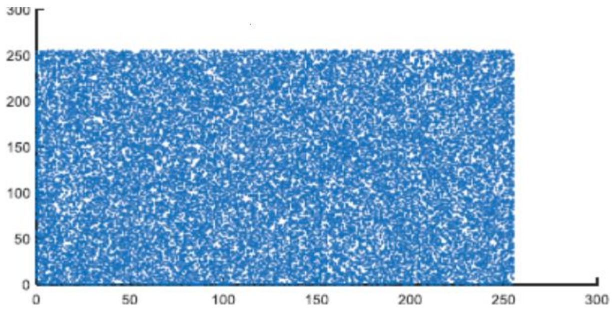
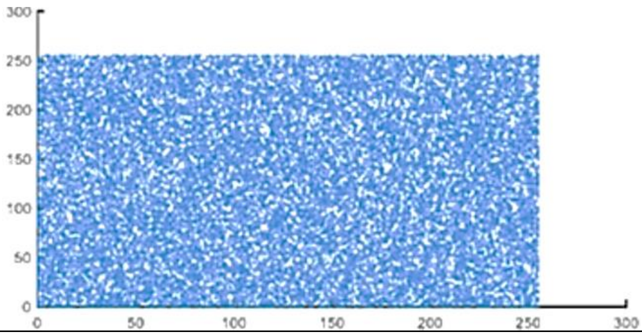
Source	Visualization
Original Image	
Vertical Correlation of Original Image	
Horizontal Correlation of Original Image	
Vertical Correlation of Encrypted Image	
Horizontal Correlation of Encrypted Image	

Table 8. Correlation coefficient calculation of birds image

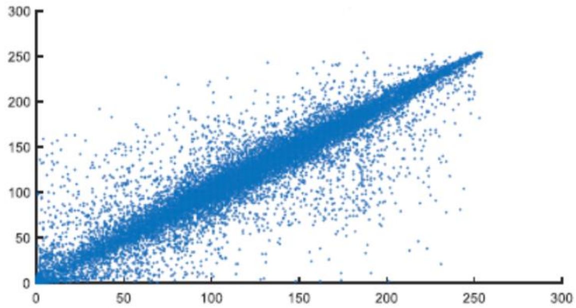
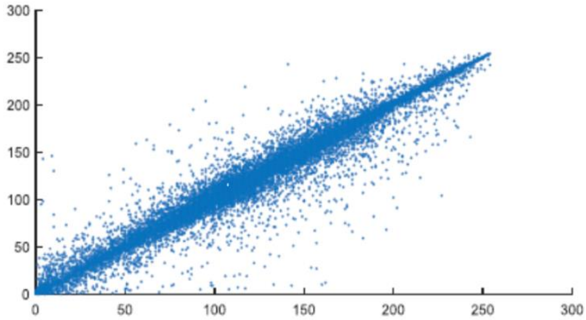
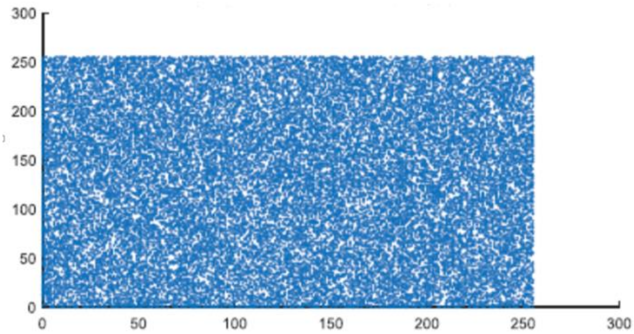
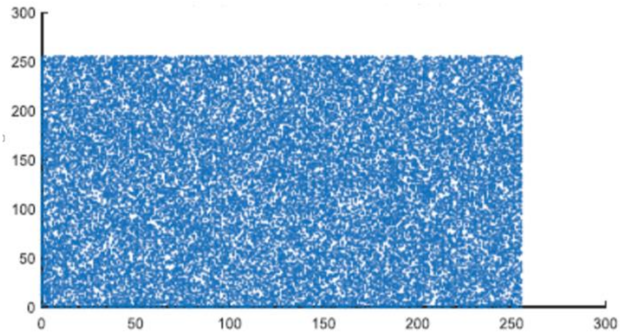
Source	Visualization
Original Image	
Vertical Correlation of Original Image	
Horizontal Correlation of Original Image	
Vertical Correlation of Encrypted Image	
Horizontal Correlation of Encrypted Image	

Table 9. Correlation coefficient calculation of butterflies image

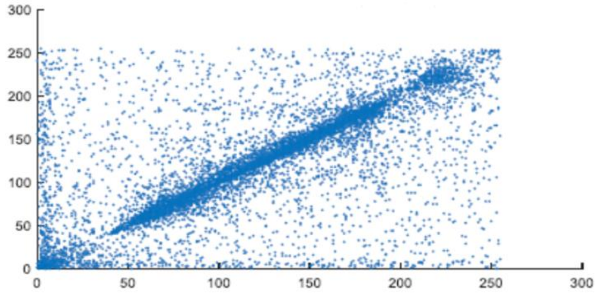
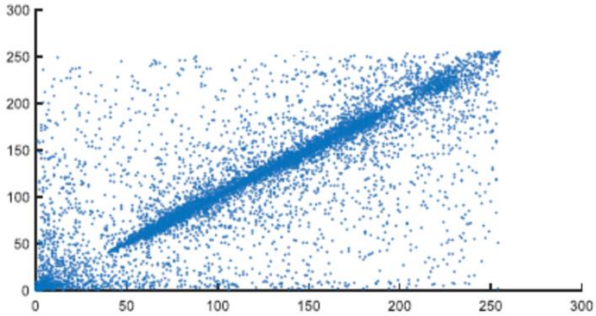
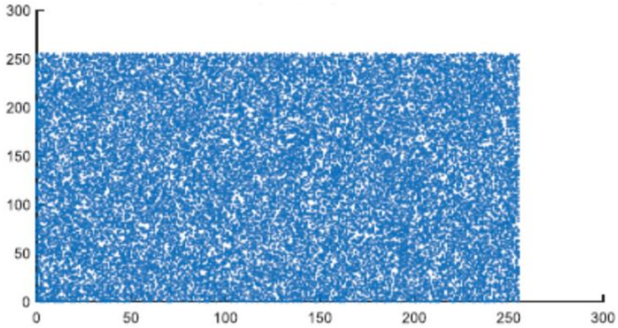
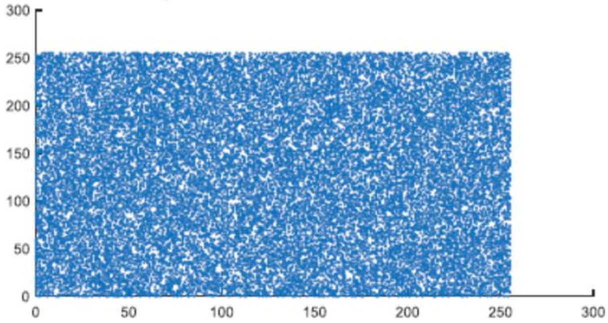
Source	Visualization
Original Image	
Vertical Correlation of Original Image	
Horizontal Correlation of Original Image	
Vertical Correlation of Encrypted Image	
Horizontal Correlation of Encrypted Image	

Table 10. The NPCR and UACI of owl image

The NPCR and UACI Calculation		
Measurements	Image	Calculation
NPCR	OWL	99.7085
UACI	OWL	33.2030

Table 11. Entropy analysis comparison

Method	Entropy (Encryption Image)
The Proposed Method 3D Chaos Map 3DCM	7.9889
Nested Piece Wise Linear Chaotic Map (NPWLCM) [22]	7.9975
Multiple Maps Combinations (MMC) [23]	7.9997
Linear Independence Scheme and the Logistic Map (LIS) and (LM) [24]	7.9912
Chaotic Encryption Algorithm (CEA) [25]	7.9993
Chaotic Coupled (CM) [26]	7.9891
mixture of chaotic maps (MCM) [27]	7.9968
Enhance 3D Chaotic MAP [28]	7.9890

Table 12. NPCR and UACI comparison

Method	NPCR (%)	UACI (%)
The proposed method	99.7085	33.2030
NPWLCZ [22]	99.6292	28.5050
MMC [23]	99.5100	33.4500
CM and CF [29]	99.6000	33.5400
LIS and LM [24]	99.5956	33.6035
CEA [25]	99.6128	33.4420
CCML [30]	25.0000	19.0000
MCM [27]	41.9620	33.2500
3D Cat [31] (6 Round)	50.3000	25.2000
3D CBM [32] (5 Round)	99.6000	33.4000
Enhance 3D Chaotic MAP [28]	99.6048	33.5044

4. CONCLUSION

From the above results, the proposed method gave promising outcomes with the 3D chaotic graph for image encryption and decryption with perfect usages in real-time image cryptography. Three different images were implemented in this work and all gave robust results with the statistical analysis. The pixel diffusion method was implemented to change the position of the pixels of each image, then the entropy analysis was calculated. It is known that the coding and the visualization of the results were taken with MATLAB environment, so the entropy outcomes showed optimal results near to 7.89% with the encrypted owl image which is considered the ideal image in this work. All the proposed images were transformed from the 3D colored image to the 2D greyscale images before the operations were taken, the average calculation of the NPCR was (99.7085%) and UACI was (33.2030%). Finally, the keyspace gives higher space with 10^124 which made the proposed work powerful against different kinds of attacks.

REFERENCES

[1] D. R. Patel, "*Information security: theory and practice*," PHI Learning Pvt. Ltd., Apr.2008.

[2] C. P. Wu and C. C. J. Kuo, "Fast encryption methods for audiovisual data confidentiality," *Multimedia Systems and Applications III, International Society for Optics and Photonics*, vol. 4209, pp. 284-295, Mar. 2001, doi: 10.1117/12.420829.

[3] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors and Microsystems*, vol. 77, pp. 103134, Sep. 2020, doi: 10.1016/j.micpro.2020.103134.

[4] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255-260, Jul. 2015, doi: 10.1126/science.aaa8415.

[5] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access* vol. 24, no. 7, pp.13960-88, Jan. 2019, doi: 10.1109/ACCESS.2019.2894819.

[6] M. T. Gaata and F. F. Hantoosh, "An efficient image encryption technique using chaotic logistic map and rc4 stream cipher," *International Journal of Modern Trends in Engineering and Research*, vol. 3, no. 9, pp. 213-218, 2016, doi: 10.21884/IJMTER.2016.3068.YIAPY.

[7] G. R. Sinha and V. Bajaj, "Data deduplication applications in cognitive science and computer vision research", *Data Deduplication Approaches: Concepts, Strategies, and Challenges*, vol. 25, pp. 357, Nov. 2020, doi: 10.1016/B978-0-12-823395-5.00001-X.

[8] S. Ahadpour, Y. Sadra, and Z. A. Arasteh Fard, "A Novel Chaotic Encryption Scheme based on Pseudorandom Bit Padding," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 2, Jan. 2012.

[9] M. I. Haider, A. Ali, D. Shah, and T. Shah, "Block cipher's nonlinear component design by elliptic curves: an image encryption application," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4693-718, Jan. 2021, doi: 10.1007/s11042-020-09892-5.

[10] W. H. Chen, S. Luo, and W. X. Zheng, "Impulsive Synchronization of Reaction– Diffusion Neural Networks with Mixed Delays and Its Application to Image Encryption," in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 12, pp. 2696-2710, 2016, doi: 10.1109/TNNLS.2015.2512849.

[11] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," in *IET Image Processing*, vol. 10, no. 11, pp. 830-839, 2016, doi: 10.1049/iet-ipr.2015.0868.

[12] M. W. Fakhr, "A multi-key compressed sensing and machine learning privacy preserving computing scheme," *5th International Symposium on Computational and Business Intelligence (ISCBI)*, pp. 75-80, 2017, doi: 10.1109/ISCBI.2017.8053548.

[13] R. G.-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," In *International Conference on Machine Learning*, pp. 201-210, 2016.

[14] F. Hu, J. Wang, X. Xu, C. Pu, and T. Peng. "Batch Image Encryption Using Generated Deep Features Based on Stacked Autoencoder Network," *Mathematical Problems in Engineering*, 2017, doi: 10.1155/2017/3675459.

[15] D. Hu, L. Wang, W. Jiang, S. Zheng and B. Li," A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 38303-38314, 2018, doi: 10.1109/ACCESS.2018.2852771.

[16] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664-25678, 2020, doi: 10.1109/ACCESS.2020.2970806.

[17] A. Shifa *et al*., "Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering," *IEEE Access*, vol. 6, pp. 16189-16206, 2018, doi: 10.1109/ACCESS.2018.2815037.

[18] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-Box based on chaotic map and backtracking," *Applied Mathematics and Computation*, vol. 376, pp. 125153, 2020, doi: 10.1016/j.amc.2020.125153.

[19] M. Rungruanganukul and T. Siriborvornratanakul, "Deep Learning Based Gesture Classification for Hand Physical Therapy Interactive Program, In: Duffy V. (eds) Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management," *Posture, Motion and Health*. HCII, Lecture Notes in Computer Science, vol 12198. Springer, Cham, 2020, doi: 10.1007/978-3-030-49904-4_26.

[20] P. N. Khade and M. Narnaware, "3D chaotic functions for image encryption," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 3, pp.323, 2012.

[21] Z. Zhe, Y. Haibing, Z. Yu, P. Wenjie, and Z. Yunpeng, "A block encryption scheme based on 3D chaotic Arnold maps," In *2009 International Asia Symposium on Intelligent Interaction and Affective Computing*, pp. 15-20, Dec. 2009, doi: 10.1109/ASIA.2009.47.

[22] H. H. Abdlrudha and Q. Nasir, "Low complexity high security image encryption based on nested PWLCM chaotic map," In *2011 International Conference for Internet Technology and Secured Transactions*, ISBN 978-1-4577-0884-8, pp. 220-225, Dec. 2011.

[23] K. Faraoun, "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption," *The International Arab Journal of Information Technology*, vol. 7, no. 3, pp. 231-240, Jul. 2011.

[24] H. M. Al-Najjar, "Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map," in *Proceedings of ACIT*, pp. 172-175, 2011.

[25] A. Awad and D. Awad, "Efficient Image Chaotic Encryption Algorithm with No Propagation Error," *ETRI Journal*, vol. 32, no. 5, pp 774-783, Oct. 2010, doi: 10.4218/etrij.10.1510.0063.

[26] M. Ahmad and M. S. Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping," *International Journal on Computer Science and Engineering*, vol. 2 no. 1, pp. 46-50, 2009.

[27] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaoticmaps," *ELSEVIER Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408-419, Jan. 2008, doi: 10.1016/j.chaos.2006.05.011.

[28] M. B. Hossain, M. T. Rahman, A. B. M. S. Rahman, and S. Islam, "A new approach of image encryption using 3D chaotic map to enhance security of multimedia component," *International Conference on Informatics, Electronics and Vision (ICIEV)*, 2014, doi: 10.1109/iciev.2014.6850856.

[29] A. Masmoudi, M. S. Bouhlel, and W. Puech, "A New Image Cryptosystem Based On Chaotic Map And Continued Fractions," *18th European Signal Processing Conference (EUSIPCO-2010)*, Aalborg, Denmark, pp. 1504-1508, Aug. 2010.

[30] S. Ahadpour and Y. Sadra, "A chaos-based image encryption scheme using chaotic coupled map lattices," *International Journal of Computer Applications*, vol. 49, no. 2, pp. 973-93-80869-31-6, 2012, doi: 10.5120/7599-0311.

[31] G. Y. Chen, Y. B. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749-761, 2004, doi: 10.1016/j.chaos.2003.12.022.

[32] Y. Maa, G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp 3613-3624, 2004, doi: 10.1142/S021812740401151X.

BIOGRAPHIES OF AUTHORS

Daniah Abdul Qahar Shakir works in Computer Science & Information Technology where she has been a college employee since 2006. From 2007-2019, he taught many laboratory materials and programming language. Now she studies MSc degree at the University of Anbar, College of Computer and his undergraduate studies at the same University. Her current research include Image Processing, Artificial Intelligence and security methods. She can be contacted at email: dan14c1001@uoanbar.edu.iq.

Ali Jbaeer Dawood has received Ph. D. in Computer science, Iraqi Commission for Computers and Informatics-Informatics Institute for Postgraduate Studies (2010). He joined in (2000-2003) to Computer Science Department College of Science-Baghdad University, Baghdad, Iraq as an external lecturer. He joined in (2001-2003) to Computer Science Department College of Computer, Anbar University, Anbar, Iraq as an external lecturer. He joined in (2002-2007) to Computer Science Department, AL-Mansour University College, Baghdad, Iraq as an external lecturer. He joined in (2005-2007) to Computer Science Department, College of Science. He can be contacted at email: co.dralijd@uoanbar.edu.iq.