

Image Encryption based on Chaotic Blocks Shuffling and RC4

 *Donia Fadil Chalob*¹ , *Rusul Hussein Hasan*^{*2} , *Farah Neamah Abbas*

¹ Department of Computer Science, College of Education, Al-Mustansiriya University, Baghdad, Iraq.

² College of Law, University of Baghdad, Baghdad, Iraq.

*Corresponding Author.

Received 30/09/2023, Revised 05/02/2024, Accepted 07/02/2024, Published Online First 20/12/2024



© 2022 The Author(s). Published by College of Science for Women, University of Baghdad.

This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

The necessity for image encryption has grown significantly, especially the rapid development of the Internet of Things (IoT) fast development and the ease with which images can be taken and transferred, including those related to travel, health care, the agricultural sector, the military and autos. Additionally, since every image has significant characteristics like size, high correlation, and massive redundant positions, encrypting it with a conventional key via IoT communication technology exposes it to numerous threats. Chaotic image cryptography is considered the most suitable method for image application due to its sensitivity to the initial conditions and control parameters. This research contributes in encrypted image devoid of statistical information to make cryptanalysis impossible. Thus, this research offered a new algorithm based on confusion and diffusion to strengthen the algorithm security. In essence, the confusion method creates random numbers for the block shuffling approach using Lorenz and Rossler system. Nonetheless, RC4 cipher and XOR operation are utilized in the diffusion approach. A very low value ($\times 10^{-3}$) of the correlation between neighboring pixels was achieved. Moreover, to prevent brute force attacks, the key space was expanded to a relatively large 2594 and key sensitivity. The resultant encrypted image is free of statistical features in terms of histogram and entropy since a histogram was idealized to be completely equal in all instances and the entropy produced was almost equal to the ideal value(8).

Keywords: Chaotic Blocks, Image Encryption, Lorenz System, RC4, Rossler System.

Introduction

At the beginning of major civilizations, there has always been an issue regarding transmitting confidential information. With the globalization of exchanges (messages, Internet, electronic commerce), based on a variety of sound, image, and video mediums, cryptography is an efficient means to safeguard secret data and maintain secrecy in the face of attackers¹⁻³. The two fundamental types of cryptography are symmetric key, where the key used to cipher and decipher is the same, and asymmetric key, where the key used to cipher and decipher is different^{4,5}.

Current developments in the field of chaotic image encryption include studies like, Patel S, et al.⁶

proposed an encryption algorithm using three-dimensional chaotic maps and a DNA encoding. The x, y, and z parameters of the 3D logistic map are initialized using three keys: Chebyshev, prime, and ASCII. The obtained x and y sequencing is applied to create shuffles. Eight complementing standards are used to encode the resulting image using DNA. By normalizing the z-sequences and encoding DNA, a key image is produced. The key and encoded images are combined using bit XOR.

Yasin, and Saraçoğlu.⁷ introduced an image cipher using RC4 for Haar wavelet transform images. After converting data from the spatial domain to the frequency domain, a wavelet transformation saves

each segment with a coordinate determining scale. Such an image is represented in terms of a low-determination image and the configuration of the descriptive coefficient by implementing HWT. The algorithm's phases are: Select the data you wish to cipher as well as the chosen key. Create two string arrays. Introduce an array with numbers in it between 0 and 255. The other array should be loaded with the chosen key. Using the primary array as a base, randomize the original array. To create the final key-stream, randomize the initial array. To send ciphertext, XOR is the last keystream of the material to be encoded.

Essaid, et al.⁸ presented a new image encryption algorithm based on three enhanced one-dimensional chaotic maps and a secured Hill Cipher (HC) variant. The combination of a 1D matrix made up of the key pixel couple and a 2×2 Hill array, and the addition of a second pseudorandom translating vector, ensures the confusion. Besides, a powerful avalanche effect that joins every cipher pixel to the aforementioned neighbor ensuring diffusion.

S Tunçer, et al.⁹ improved the RC4 algorithm based on chaotic systems with the aid of 2D Cat Map, Tent Map, and Lorenz system. Using Cat Map, image shuffle is accomplished. Tent Map is used to generate randomized values once RC4 has been applied.

Kumari, and Gupta.¹⁰ presents an image cipher technique that encrypts/decrypts the images using RC4 cipher and intertwined chaotic map. The RC4 cipher generates random sequences using this key to perform diffusion. The diffusion method is carried out in both forward and reverse directions, row and column-wise.

Susanto, and Setiadi,¹¹ provided a method for encrypting image that consists of three levels of encryption: stream, bit-shift, and chaos-based cryptography. Arnold's chaotic map is the chaos algorithm, while RC4 is the stream cipher algorithm. The first layer of the scheme is bit-shifting. Based on the key, circular -shifting is performed on the original image.

Mehdi, and Kadhim.¹² created a new chaotic scheme based on Sudoku matrix, in which a new 5D chaos system is constructed to produce the random key. The chaotic sequence is utilized to create a scrambled image, followed by XOR operation between Sudoku Matrix and the scrambled image, another scrambling operation, and finally an XOR operation between the original image and chaotic key.

Chen E, et al.¹³ provided nine discrete chaotic

systems by one line equilibria (DCSLE) in 4D made up of a few basic sine functions. A DCSLE is used to build an 8D DCSLE GCS system based on the general chaos synchronization (GCS) concept to develop a chaotic pseudorandom number generator (CPRNG). A RGB image is encrypted using the CPRNG and an avalanche effect encryption method. Pourjabbar, et al.¹⁴ based on double chaotic systems, presented a new image encryption algorithm. A hybrid strategy that parallels and mixes the chaotic maps. It is based on a combination of the discrete wavelet transform (DWT), which divides the original image into sub bands. The DWT separates the image down into sub bands using high-pass and low-pass filtering. The image is presented as four sub bands for a single plane deconstruction. The positions of the four sub band pixels are shuffled using four proposed maps. To diffuse the overall shuffled image, the created recommended chaotic sequence is utilized.

Hamza, and Dahar.¹⁵ utilized RC4 and rossler system to cipher a plain image. Rossler system's initial conditions are produced by implemented the identical key. Rossler system is used to generate a 2D array of random numbers. To acquire the final cipher text image, the resultant array is XORed with the ciphered image. Gaffar et al.¹⁶ utilized a Gingerbread man map to shuffle picture pixels during the transposition stage, and the RC4A (Rivest Cipher 4A) cipher technique was utilized to bit-wise XOR the key stream and the image pixels during the replacement step.

Malik, et al.¹⁷ proposed an approach employing an image bit plane cryptographic algorithm that combines logistic map and RC4 using CBC (Cipher Block Chaining) mode. In the diffusion phase, CBC mode is employed. The YCbCr color model is shaped like the RGB image because it consumes less bandwidth in transmission. The S-box byte-substitution is produced using RC4. The confusion phase uses channel transforming to accomplish randomization. Inter bit shuffling is based on zigzag XORing of pixels between inter bit planes.

Hanchinamani, and Kulkarni.¹⁸ suggested an image decipherment method based on RC4 and chaotic Peter De Jong map. The preliminary keys of RC4 producer and the shuffle stage are chosen using a Peter De Jong map. The pseudorandom numbers of the pixel rotation and diffusion maneuvers are produced using the RC4 generator. The shuffle is based on rotating the rows and columns in opposite directions while randomly rearranging the rows and

columns. Using $M \times N$ pseudorandom numbers, the second step rotates every pixel in a circular motion. The diffusion is repeated twice in the last stage by scanning the image twice.

In¹⁹, this paper developed a new approach for image encryption based on three chaotic systems — Chen system, logistic map, and 2D Arnold cat map. The image is first subjected to a shuffling algorithm; the shuffled image is divided into blocks. The Chen system is utilized for each block to create confusion. The logistic map is applied to create Substitution-boxes to replace image blocks. The S-box is dynamic and is scrambled for each image block to shuffle it. Following by the employment of 2D Arnold cat map for diffusion. The encrypted image is achieved by XORing the outcome with the keys of Chen system. The problem statement is that digital image cryptographic can be done using conventional, unconventional, and hybrid methods. The conventional algorithm has problems of pattern

appearance and slowness.

The contributions of the research include: using the unconventional encryption techniques are used to encrypt digital media in recent research to accelerate and enhance encryption necessities. This research suggests a new image cryptographic algorithm that combines the chaotic systems and RC4 stream algorithm. By employing chaotic XOR operations and RC4, high diffusion is obtained. The block shuffle method, Lorenz system, and Rossler system are employed to obtain high confusion.

The remaining sections have been ordered as following order. In 2nd section, the techniques employed in the suggested algorithm will be described. The 3rd Section provides a comprehensive explanation of the proposed system. The security evaluation metrics is shown in 4th section. The 5th Section is where the findings are made.

Methods

RC4 Algorithm

The term "Rivest Cipher 4" is often abbreviated as "RC4". Ron Rivest created this method in 1987^{20,21}. The technique can be utilized successfully in both software and hardware because of its simplicity, speed, and convenience of creating PRNG sequence. Wep, Skype, WPA, SSL/TLS, and other internet protocols all utilize RC4 in encrypting data, secrecy, and communication security. While this algorithm is in its initial stage, the 256- byte array is initialized using a variable key length that ranges between 0 and 255 bytes. Key, which is longer than 128 bytes, should be used in RC4. Key Scheduling Algorithm (KSA) is utilized to initialize the RC4 Key. Algorithm 1 describes RC4 stream cipher.

Algorithm 1. RC4 Algorithm

Input: $K [k_1, k_2, \dots, k_L]$

Output: K_{seq}

1. Initialize:
2. for $i = 0 : 255$
3. $S[i] = i$
4. KSA Scrambling
5. $j = 0$
6. for $i = 0 : 255$
7. $j = (j + S[i] + K[i \bmod L]) \bmod 255$
8. Swap ($S[i]$, $S[j]$)
9. End for

10. PRNG for RC4

11. $j = 0$

12. $i = 0$

13. While not end of seq Do

14. $i = (i + 1) \bmod 256$

15. $j = (j + S[i]) \bmod 256$

16. Swap $S[i]$ with $S[j]$

17. $K_{seq} = S[S[i] + S[j] \bmod 256]$

18. End While

19. Return K_{seq}

Lorenz System

A significant advance in the field of dynamical systems is the concept of defining chaotic dynamics with the use of chaotic maps. E. Lorenz was the first to present a mathematical model of air flow in the atmosphere²²⁻²⁴ in Fig. 1. The system of chaotic differential equation is given as Eq. 1, Eq. 2 and Eq. 3:

$$\frac{dx}{dt} = a(y - x) \quad 1$$

$$\frac{dy}{dt} = bx - y - xz \quad 2$$

$$\frac{dz}{dt} = xy - cz \quad 3$$

Where the specified intervals for the variables x , y , and z : $-60 \leq x \leq 60$, $-60 \leq y \leq 60$, $-60 \leq z \leq 60$. The parameters a , b , and c have the following values to achieve chaotic behavior: $a = 10$, $b = 28$ and $c = 8/3$.

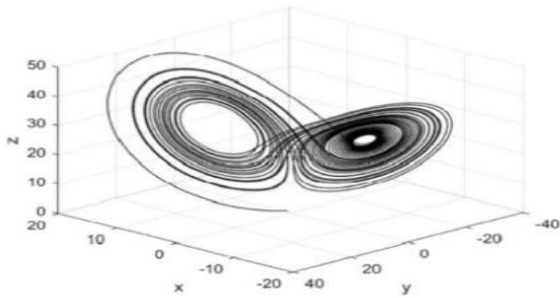


Figure.1. Plot of Lorenz System in x–y–z Plane

Rosler System

In 1976, Rosler¹⁵ provided a set of three differential equations, one of which contains a non-linear term with a chaotic dynamic behavior. The Rosler system is described as Eq. 4, Eq. 5 and Eq. 6:

$$\begin{aligned} dx/dt &= -y - z & 4 \\ dy/dt &= x + ay & 5 \\ dz/dt &= b + z(x - c) & 6 \end{aligned}$$

Where t is a time, $(x, y, z) \in \mathbb{R}^3$ are the dynamic variables that described the phase space, and $(a, b, c) \in \mathbb{R}^3$ are the Rosler system parameters, $(x_0, y_0, z_0) \in \mathbb{R}^3$ are initial conditions of Rosler system. At $(a=0.2, b=0.2$ and $c=5.7)$, the chaotic system reaches the Rosler attractor. The Rosler attractor is shown in Fig. 2 with the initial conditions $(x_0=1.9895, y_0=0.6788$ and $z_0=0.3741)$.

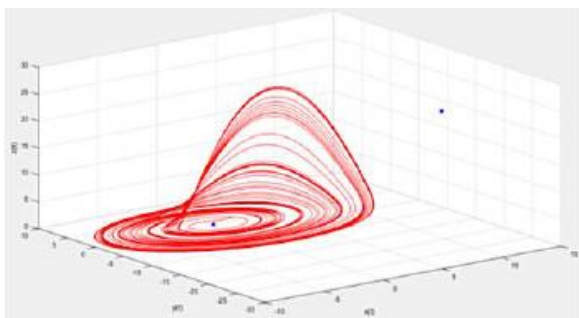


Figure.2. Rosler Attractor

Proposed Methods

General Proposed Algorithm

The suggested algorithm contains multiple phases of confusion and diffusion, including:

a. Confusion phase, implemented twice: in the first, a suggested chaotic block shuffling approach, explained in next subsection, based on Lorenz system scrambles the plain image. In the second, the same proposed block shuffling mechanism, but based on Rosler system shuffles the image.

b. Diffusion phase will be implemented three times in three different ways which are, implementing RC4 algorithm, XOR between Lorenz key and the resultant image, XORing the obtained image and Rosler keys to produce the cipher image. The diagram of the suggested model is demonstrated in Fig. 3 and Fig. 4 shows shuffled House image, ciphered image by proposed algorithm and decipher image.

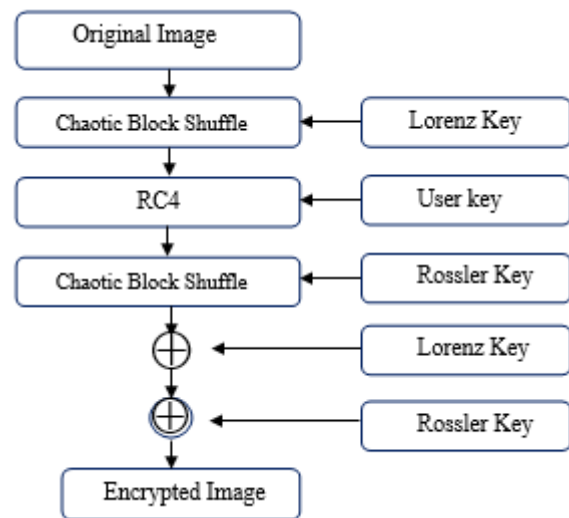


Figure.3. General Diagram of Proposed Algorithm

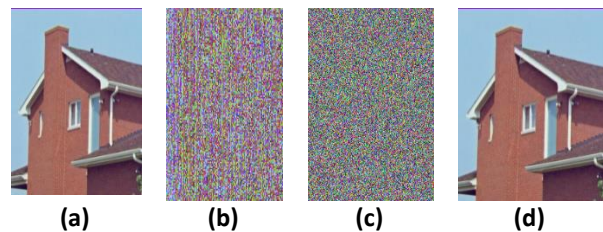


Figure.4. Test Image: (a) Original House Image, (b) Shuffled House Image, (c) Ciphered House Image, (d) Decipher House Image

Block Shuffling Method

The property of randomness in chaos can be utilized to implement scramble behavior in images. The pixel position is scrambled block by block in the order of the randomness of elements obtained from the chaotic system. In this proposed algorithm, block shuffling method is implemented twice, in the first one, Lorenz key is used and in the second one Rosler key is utilized. The key generated from chaotic system and the image are divided into many blocks of size 2×2 . The sum operation is performed for the values in the key block, thus if the sum result is odd, then a key block is saved in a new matrix (odd

key) and the image block in the corresponding location of the odd key block is saved in a new matrix (odd img), and if the sum values in the key block is even, then the key block is saved in (even key) matrix and the image block corresponding to it in the location is saved in (even img) matrix. In the result, have two key arrays, one for even block and the other for odd, and two image arrays, odd array for the image blocks corresponding to the position of the odd key blocks and the even array for image blocks corresponding to the position of the even key blocks. Each block in the odd and even key arrays is summed and then sorted employing the sort mathematical

function, which provides the matrix's element's index position after ascending order. Both of the new (odd and even) indexes obtained from odd and even key arrays after sorting will be pointing to the new position that an image block will be transposed to it depending on odd or even key. Note that the proposed block shuffling is applied for Red, Green and Blue level individually. Table 1 illustrates the proposed chaotic block shuffling of first 5x5 image blocks before and after image shuffling, the blocks will be replaced by new blocks and transposed in new different positions all over the image. Obviously, the blocks are not the same.

Table 1. Image Chaotic Block Shuffling

Original Blocks										Shuffled Blocks									
131	165	160	159	158	167	176	174	181	180	101	206	139	135	90	90	116	128	173	173
150	197	191	189	191	190	200	183	195	191	102	194	135	130	61	82	126	118	190	190
147	197	192	187	187	182	192	177	188	192	130	126	130	126	172	175	112	108	191	194
148	191	190	184	183	181	185	184	180	185	128	129	128	129	172	172	126	117	180	194
142	194	191	188	184	186	184	187	181	181	163	159	155	158	125	116	128	129	117	112
133	198	184	185	181	183	183	180	179	184	162	160	160	161	130	122	126	127	120	113
127	190	173	171	173	176	178	175	174	168	163	158	156	157	139	133	118	125	120	111
124	175	166	161	170	173	168	173	175	171	161	163	151	149	143	126	118	116	114	116
108	161	168	176	174	175	178	182	181	180	193	171	204	208	120	127	126	136	183	186
105	188	190	191	191	193	202	200	201	200	200	167	209	204	120	121	126	138	180	178

Algorithm 2. Chaotic Block Shuffling

Input: Original Image (OH×W), chaotic key
Output: Shuffled image (SH×W)
1. Iterate chaotic system to generate chaotic keys, {ki, i=1, ..., H×W}
2. key ← absolute (round (k))
3. keyblock ← divided key into blocks of size 2×2
imgblock ← divided O into blocks of size 2×2
4. For l ← 1: keyblock
For i ← 1: 2
For j ← 1: 2
keysum ← sum (key(i, j))
end
end
if keysum(l) modulare 2 ≠ 0
keyodd ← keysum(l)
imgodd ← imgblock(l)
else

keyeven ← keysum(l)
imgeven ← imgblock(l)
end
5. Indexodd ← sort (keyodd)
Indexeven ← sort (keyeven)
6. imgodd (Indexodd) ←transpose (imgodd)
Imgeven (Indexeven) ← transpose (imgeven)
7. S ← collect odd and even blocks.

Proposed Encryption Algorithm

This subsection offers a comprehensive explanation of the suggested encryption technique. Initially, Input the original image and intial conditions and parameters of Lorenz system, the intial conditions and parameters are utilized to solve Lorenz system using adaptive Runge-Kutta technique. Lorenz system iterates T times to generate three chaotic arrays, implement chaotic arrays to confuse the plaintext image as obtained in subsection (*Block*

Shuffling Method), each chaotic array is specified to confuse one level of RGB image. Next, the shuffled image is diffused by RC4 algorithm. The resultant image is confused using the same shuffling technique in subsection (*Block Shuffling Method*), but this time the chaotic array is generated by Rossler system. Finally, XORed the resulting image with Lorenz key and then XORed with Rossler system to provide extra diffusion process.

Key Generation

The Chaotic Key Generator is one of the main components of the suggested image cryptography. Any length of random number within the specified range can be produced by the generator method. The key generation steps are explained below:

Step 1. Three distinct chaotic maps are given state variables for Lorenz and Rossler systems, each with unique initial conditions and control parameter values that yield attributes related to unpredictability.

Step 2. The following equation is used to convert the bit values of these state variables:

$$\text{Key} = (\text{Absolute}(\text{bit values}) * 10^{14}) \text{ Mod } 256.$$

Step 3. Random bits are produced until a block with a length of 256 bits is achieved.

XOR in Encryption

The XOR operator is a very popular component in cryptography. Frequency analysis can easily solve a basic XOR encryption problem on its own with a constant repeating key. The main advantages of this approach are its ease of implementation and the low computing cost of the XOR operation. The XOR cipher is significantly more secure than key repetition within a message if the key is random and at least as lengthy as the message. A stream cipher is

produced when a pseudo-random number generator generates the keystream. The outcome is a one-time pad that is theoretically impenetrable when the key is truly random²⁵. This characteristic can be achieved using a chaos system for key generation.

Algorithm 3. Encryption Operation

Input: Original Image (OH×W), Lorenz_key, RC4_key, Rossler_key

Output: Encrypted Image (C)

1. Input image (OH×W)
2. For i ← 1: H
 For j ← 1:W
 P1 ← Chaotic Block Shuffle (OH×W, Lorenz_key)
 end
end
3. For i ← 1: H×W
 P2 ← RC4 (P1, RC4_key)
end
4. For i ← 1: H
 For j ← 1:W
 P3 ← Chaotic Block Shuffle (OH×W, Rossler_key)
 end
end
5. For i ← 1: H×W
 P4 ← XORed (P3, Lorenz_key)
end
6. For i ← 1: H×W
 C ← XORed (P4, Rossler_key)
end.

The receptor utilizes the same secret keys to generate key arrays based on the 3D Lorenz and Rossler system during the decryption operation. Then, the plain data from the cipher text image is successfully recovered using the inverse of the confusion-diffusion and block shuffling phases.

Results and Discussion

Several analysis metrics were applied, including key space, information entropy, NPCR and UACI, histogram analysis, to compare and evaluate the encryption performance. The size of the test images is 256×256.

Key Space Analysis


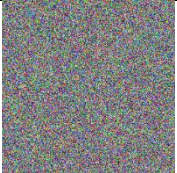
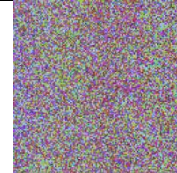
The key space is one of the most crucial components of any encryption algorithm. A large key space offers protection from the brute force threat. Together, Lorenz and Rossler systems have six initial values, six parameters. Furthermore, the computer precision

is set at 10^{-15} . This therefore serves $(10^{15})^{12} = 10^{180} = 2^{594}$ to the key space. Besides, the key is provided by RC4 algorithm. Thus, this score exceeds the minimum threshold of 2^{100} , making it sufficient to counter the threat of brute force²⁶. The large key space enables us to deal with encrypting the huge amount of image pixels, since each pixel in the image encrypts using a unique key that is not duplicated with another pixel, and this will help to eliminate the problem of pattern appearance issues when encrypting images using small key.

Sensitivity of Key Analysis

The value of initial condition of Lorenz system is slightly altered from $y(0) = 1.6$ to $y(0) = 1.60000000000001$ in decryption. Table 2 shows that even with a minor variation of 10^{-14} , the decrypted image with the tiny altered key is entirely different from the original image. It implies that the proposed algorithm is extremely sensitive to any potential changes to the key ²⁶.

Table 2. Key Sensitivity Test

Plain Image	Encrypted Image with $y(0)= 6.1$	Decrypted Image with $y(0)= 1.60000000000001$
		

Information Entropy Analysis

Entropy is used to calculate the probability of a decrypted image opportunity, which can be calculated by (7), $p(i)$ is chance of probability. The good and safe entropy value of the attack is close to eight ^{27, 28}. Table 3 displays the entropy values of different plain images and respective cipher image, showing that the suggested scheme has high randomization. The findings demonstrate that the suggested algorithm's entropy is closer to the theoretical value of 8, indicating greater security.

$$E = -\sum_{i=0}^{255} p(i) \log_2(p(i)) \quad 7$$

Table 3. Information Entropy of Original and Cipher Images

Images	Entropy	
	Plain image	Cipher image
Sun	5.8168	7.9993
House	7.0686	7.9991
Boat	7.7757	7.9990
Flower	7.5832	7.9991
Pepper	7.7272	7.9991
Clock	6.3320	7.9989
Mountain	7.7931	7.9991
Green	2.1851	7.9990
Splash	7.3649	7.9990
Tree	7.5370	7.9991

Correlation Analysis

In this analysis, 5,000 pairs of neighboring pixels

were utilized. Table 3 lists the outcomes of the associations found. The correlation coefficients of tested images are obtained using Eq. 8, Eq. 9 and Eq. 10:

$$d_{xy} = (cov(x, y)) / (\sqrt{D_x} \sqrt{D_y}) \quad 8$$

$$cov(x, y) = E[(x - E(x))(y - E(y))] \quad 9$$

$$E(x) = \frac{1}{L} \sum_{i=1}^L x_i; D(x) = \frac{1}{L} \sum_{i=1}^L (x_i - E(x))^2 \quad 10$$

Where L is the number of samples, x and y stand for adjacent pixels. The range of d_{xy} is between -1 and 1. If it is near to 0, the image is uncorrelated and the cipher process is strong enough to withstand statistical attack ²³. After implementing the correlation test using the plain and cipher image obtained from the proposed algorithm, noticed that the plain image is close to (+1), which indicates that the correlation between the pixels is high, and the ciphertext image is near to (0), indicating that there is low association between the pixels. The correlation results using several plain and cipher images are displayed in Table 3, and Fig. 5 displays the plain and cipher House image's diagonal, vertical, and horizontal correlation coefficients. The correlation coefficients of the cipherimage using the proposed algorithm are closer to zero than the original, as can be seen from Table 4 and Fig. 5. This indicates that the cipherimage pixels using the proposed algorithm are highly uncorrelated and cannot predict one another, indicating that the proposed algorithm is highly secure.

Table 4. Correlation of Encrypted and Original Images

Images	Original Images			Cipher Images		
	H	V	D	H	V	D
Sun	0.9921	0.9919	0.9890	0.0005	0.0026	-0.0115
House	0.9671	0.9352	0.9126	-0.0016	-0.0029	-0.0058
Boat	0.8773	0.8654	0.8188	0.0013	-0.0050	-0.0042
Flower	0.9564	0.9717	0.9413	0.0048	0.0029	-0.0020
Pepper	0.9408	0.9457	0.9043	0.0034	0.0060	-0.0049
Clock	0.9295	0.9525	0.9209	0.0011	0.0003	-0.0033
Mountain	0.9322	0.9317	0.9134	0.0026	0.0016	-0.0070
Green	0.7222	0.2712	-0.3028	0.0045	0.0043	-0.0126
Splash	0.9758	0.9889	0.9695	0.0076	0.0009	-0.0084
Tree	0.9590	0.9361	0.9160	0.0049	-0.0011	-0.0030

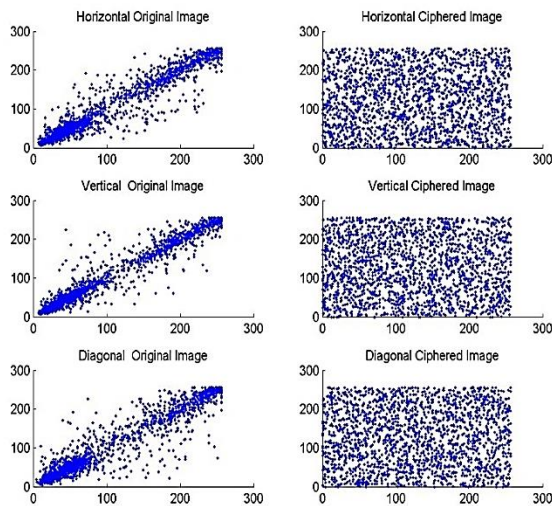


Figure 5. Correlation of Adjacent Pixels in Original and Cipher House Image

Study of Differential Attack

Shannon's diffusion primitive theory states that small differences in the plaintext should eventually affect the entire cipher text. For defending against a differential attack, Chen suggested using NPCR and UACI to quantitatively measure this spreading potential for image ciphers. NPCR and UACI can be calculated via (11), where P1 and P2 are two images with a combined size of M×N. For 256 grey-level image encryption, the typical NPCR and UACI values are 99.6094 and 33.4635%, respectively²⁹. Table 4 demonstrates UACI and NPCR Indications. The values of the proposed algorithm are nearer the theoretical value, according to the results of the NPCR and UACI tests in Table 5. Thus, the algorithm has a strong defense against differential attacks.

$$\left\{ \begin{aligned}
 D(i, j) &= \begin{cases} 0 & \text{if } P_1(i, j) = P_2(i, j) \\ 1 & \text{if } P_1(i, j) \neq P_2(i, j) \end{cases} \\
 NPCR &= \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\%, \\
 UACI &= \frac{1}{M \times N} \left[\sum_{i=1}^M \sum_{j=1}^N \frac{|P_1(i, j) - P_2(i, j)|}{L-1} \right] \times 100\%
 \end{aligned} \right. \quad (11)$$

Table 5. UACI and NPCR Indications of Encrypted Image

Image	NPCR	UACI
Sun	99.6159	42.6824
House	99.6037	29.5329
Boat	99.6175	32.3326
Flower	99.6033	33.5487
Pepper	99.6028	32.0635
Clock	99.6124	35.4023
Mountain	99.6175	32.5433
Green	99.6226	33.7779
Splash	99.6251	33.9564
Tree	99.6002	31.9826

Histogram Indicator

A histogram shows how brightly the pixels in a digital image are distributed. In a statistical attack, an intruder exploits frequency distribution to find the key to encrypt or decipher image pixels. The original image histogram and the encryption image shouldn't be statistically similar to one another to thwart statistical assaults. The cipher image histogram should be statistically evenly distributed for this purpose³⁰. Fig. 6 highlights the House image histogram in both its plain and encrypted forms and clearly shows that the suggested algorithm's cipher image histogram differs from the original image's histogram and has a more uniform distribution. As a result, the suggested method offers no information that a statistical attack on the encrypted photos may exploit.

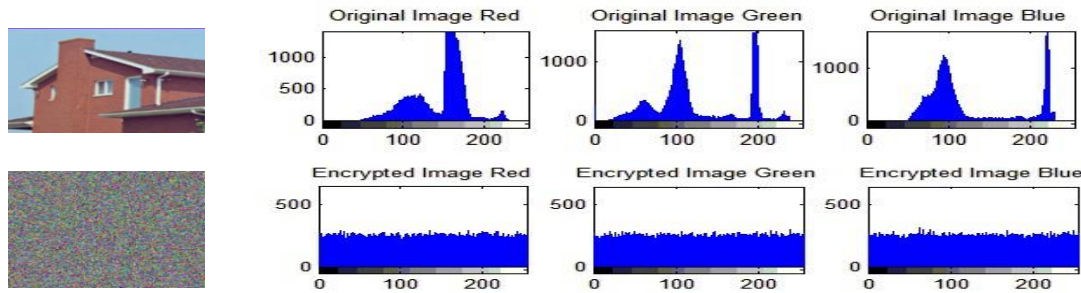


Figure. 6. Histogram Analysis of House Image

Comparison of Performance

In^{10,18}, the performance of the proposed technique is contrasted with that of the existing algorithms. Table 6 contrasts our techniques, keyspace, entropies,

NPCR, and UACI are superior to preceding methods. The suggested cryptographic technique is more effective and resistant to current attacks than earlier cryptosystems.

Table 6. Comparison of House Image by Different Algorithms

Schemes	Correlation			Info. Entropy	Key Space	NPCR%	UACI%
	H	V	D				
Proposed	-0.0016	-0.0029	-0.0058	7.9991	$>2^{594}$	99.6037	29.5329
[10]	0.01627	0.00380	0.01090	7.9991	2^{384}	99.5854	29.5764
[18]	-0.0029	0.00139	0.00796	7.99703	2^{384}	NA	NA

Conclusions

Shannon (1949) proposed that the ideal secrecy system for cryptography consists of two main processes which are confusion and diffusion. The proposed novel processes align with Shannon's concepts by designing a new image cryptographic algorithm that combines the chaotic systems and RC4 stream algorithm and designing a new chaotic block shuffling based on chaotic systems, high confusion and diffusion cryptography features are obtained. The formed sequence of 3D Lorenz system and 3D Rossler system is utilized to reduce the correlation between nearby pixels by shuffling them using new chaotic block shuffling method. The XORing of image pixels and chaotic keys generated from Lorenz and Rossler systems experienced a remarkable improvement. The breaking of strong correlations between nearby pixels is due to the proposed confusion mechanism. The proposed diffusion approach also eliminates the statistical characteristics of the encrypted image while

increasing resistance to differential attacks. According to these methods used to encrypt image, the proposed algorithm provides robust security since all security tests have been passed. The proposed implementation yields nearly optimal results for the cipher image's histogram and information entropy. Additionally, the remaining statistical features, such as the correlation. The proposed method enhances the key secrecy via increase key space by utilizing two strong chaotic systems (Lorenz and Rossler) since the key space is very large with maintain key sensitivity. Despite the differential analysis being a very interesting attack but the proposed framework resolves this issue. In general, the proposed framework consists of two processes (confusion and diffusion) with new methods instead of one process in conventional image encryption frameworks. For future work, the security of the proposed algorithm may be enhanced using a different encryption algorithm than RC4.

Authors' Declaration

- Conflicts of Interest: None.

- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore,

- any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No animal studies are present in the manuscript.

- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at Mustansiriyah University.

Author's Contribution Statement

D. F. C., R. H. H. and F. N. A. Contributed to the implementation and design of the research, to the

analysis of the results and to the writing of the manuscript

References

1. Kumar S, Kumar S, Ranjan N, Tiwari S, Kumar TR, Goyal D, et al. Digital watermarking-based cryptosystem for cloud resource provisioning. *Int J Cloud Appl Comput* . 2022; 12(1): 1–20. <http://dx.doi.org/10.4018/ijcac.311033>
2. S. Kumar N. Kumar. Conceptual service level agreement mechanism to minimize the SLA violation with SLA negotiation process in cloud computing environment. *Baghdad Sci. J.* 2021; vol. 18, no. 2: pp. 1020–1029. [http://dx.doi.org/10.21123/bsj.2021.18.2\(Suppl.\).1020](http://dx.doi.org/10.21123/bsj.2021.18.2(Suppl.).1020)
3. Kumar S, Samriya JK, Yadav AS, Kumar M. To improve scalability with Boolean matrix using efficient gossip failure detection and consensus algorithm for PeerSim simulator in IoT environment. *Int J Inf Technol* . 2022; 14(5): 2297–307. <http://dx.doi.org/10.1007/s41870-022-00989-8>
4. Kumar N, Kumar S. A salp swarm optimization for dynamic resource management to improve Quality of service in cloud computing and IoT environment. *Int J Sens Wirel Commun Control* . 2022; 12(1): 88–94. <http://dx.doi.org/10.2174/2210327911666210126122119>
5. Yadav AS, Kumar S, Karetla GR, Cotrina-Aliaga JC, Arias-González JL, Kumar V, et al. A feature extraction using probabilistic neural network and BTFSC-Net model with deep learning for brain tumor classification. *J Imaging*. 2022; 9(1): 10. <http://dx.doi.org/10.3390/jimaging9010010>
6. Patel S, Bharath K P, Rajesh Kumar M. Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique. *Multimed Tools Appl* . 2020; 79(43–44): 31739–57. <http://dx.doi.org/10.1007/s11042-020-09551-9>
7. Yasin E, Saraçoğlu R. Haar wavelet transformation and RC4 algorithm based Image Encryption. *Int J Appl Math Electron Comput*. 2020;8(3):45–9. <http://dx.doi.org/10.18100/ijamec.763283>
8. Essaid M, Akharraz I, Saaidi A, Mouhib et A. Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. *J Inf Secur Appl*. 2019; 47:173–87. <http://dx.doi.org/10.1016/j.jisa.2019.05.006>
9. S Tunçer, C Karakuzu, F Uçar. RC4 Stream Cipher Based Digital Color Image Encryption Using Chaotic Systems. *ICATCES'18*. 2018 pp. 302–305.
10. Kumari M, Gupta S. A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. *3D Res*. 2018; 9(1): 1–20. <http://dx.doi.org/10.1007/s13319-018-0162-2>
11. Susanto A, Setiadi DRIM, Rachmawanto EH, Wahyu Mulyono IU, Sari CA, Sarker MK, et al. Triple layer image security using bit-shift, chaos, and stream encryption. *Bull Electr Eng Inform*. 2020; 9(3): 980–987. <http://dx.doi.org/10.11591/eei.v9i3.2001>
12. Mehdi SA, Kadhim AA. Image encryption algorithm based on a new five dimensional hyperchaotic system and Sudoku matrix. In: 2019 International Engineering Conference (IEC). IEEE; 2019. <https://doi.org/10.1109/IEC47844.2019.8950560>
13. Chen E, Min L, Chen G. Discrete chaotic systems with one-line equilibria and their application to image encryption. *Int J Bifurcat Chaos*. 2017; 27(03): 1750046. <http://dx.doi.org/10.1142/s0218127417500468>
14. Pourjabbar Kari A, Habibizad Navin A, Bidgoli AM, Mirnia M. A new image encryption scheme based on hybrid chaotic maps. *Multimed Tools Appl*. 2021; 80(2): 2753–72. <http://dx.doi.org/10.1007/s11042-020-09648-1>
15. Hamza YA, Dahar Omer M. An Efficient Method of Image Encryption Using Rossler Chaotic System. *Acad J Nawroz Univ* . 2021 Apr.28 [cited 2024 Jan.21]; 10(2): 11–22.
16. Gaffar A, A Joshi, Kumar D. Image Encryption using Gingerbreadman Map And RC4A Stream Cipher. *AAM*. 2020 Dec 1 [cited 2024 Jan 21];15(2).
17. Malik A, Dhall S, Gupta S. An improved bit plane image encryption technique using RC4 and quantum chaotic demeanour. *Multimed Tools Appl* . 2021; 80(5): 7911–37. <http://dx.doi.org/10.1007/s11042-020-09973-5>
18. Hanchinamani G, Kulkarni L. An efficient image encryption scheme based on a Peter De Jong chaotic

- map and a RC4 stream cipher. 3D Res . 2015; 6(3):30.
<http://dx.doi.org/10.1007/s13319-015-0062-7>
19. Chalob DF, Maryoosh AA, Esa ZM, Abbud EN. A New Block Cipher For Image Encryption Based On Multi Chaotic Systems. *Telkomnika* . 2020; 18(6): 2983.
<http://dx.doi.org/10.12928/telkomnika.v18i6.13746>
20. Crainicu B. On invariance weakness in the KSAm algorithm. *Procedia Technol.* 2015; 19: 850–7.
<http://dx.doi.org/10.1016/j.protcy.2015.02.122>
21. Salih HM, Mahdawi RSA. The security of RC4 algorithm using keys generation depending on user's retina. *Indones J Electr Eng Comput Sci* . 2021; 24(1) :452-463.
<http://dx.doi.org/10.11591/ijeecs.v24.i1.pp452-463>
22. Satam IA, N. Shahab S, Kamel HA, Al-Hamadani MNA. Execution of a smart street lighting system for energy saving enhancement. *Bull Electr Eng Inform.* 2021; 10(4): 1884–92.
<http://dx.doi.org/10.11591/eei.v10i4.2924>
23. Al-Maadeed TA, Hussain I, Anees A, Mustafa MT. A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes. *Multimed Tools Appl.* 2021; 80(16): 24801–22.
<http://dx.doi.org/10.1007/s11042-021-10695-5>
24. Al-Bahrani AE, Kadhum NR. A New Cipher Based on Feistel Structure and Chaotic Maps. *Baghdad Sci J.* 2019 Mar. 17 [cited 2024 Feb. 5]; 16(1(Suppl.): 0270-0280.
[https://doi.org/10.21123/bsj.2019.16.1\(Suppl.\).0270](https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0270)
25. Overill RE. Codes and ciphers: Julius Caesar, the enigma, and the internet. *J Logic Comput* . 2002; 12(3): 543–543.
<http://dx.doi.org/10.1093/logcom/12.3.543>
26. Hanif M, Iqbal N, Ur Rahman F, Khan MA, Ghazal TM, Abbas S, et al. A novel grayscale image encryption scheme based on the block-level swapping of pixels and the chaotic system. *Sensors (Basel).* 2022; 22(16): 6243.
<http://dx.doi.org/10.3390/s22166243>
27. Irawan C, Moses Setiadi DRI, Rachmawanto EH, Sari CA, Doheir M. Hybrid encryption using confused and stream cipher to improved medical images security. *J Phys Conf Ser.* 2019; 1201(1): 012022.
<http://dx.doi.org/10.1088/1742-6596/1201/1/012022>
28. Ahmed WD, Jawad M., Jawad ML. An effective color image encryption scheme based on double piecewise linear chaotic map method and RC4 algorithm. *J Eng Sci Technol.* 2021 16(2): 1319–1341.
29. Abdullah HA, Abdullah HN. FPGA implementation of color image encryption using a new chaotic map. *Indonesian J Electr Comput Eng.* 2019 Jan 1; 13(1): 129-137.
<https://doi.org/10.11591/ijeecs.v13.i1.pp129-137>
30. Momeni Asl, A., Broumandnia, A., Mirabedini, S. J. Color image encryption using linear feedback shift registers by three dimensional permutation and substitution operations. *International Journal of Nonlinear Analysis and Applications*, 2021; 12 (Special Issue): 903-921.
<https://doi.org/10.22075/ijnaa.2021.5520>

تشفير الصورة بالاعتماد على بعثرة الكتل الفوضوية وخوارزمية RC4

دنيا فاضل جلوب¹ ، رسل حسين حسن² ، فرح نعمة عباس¹

¹ قسم علوم الحاسوب، كلية التربية، الجامعة المستنصرية، بغداد، العراق.

² كلية القانون، جامعة بغداد، بغداد، العراق.

الخلاصة

ملخص: تزايدت الحاجة إلى تشفير الصور بشكل كبير، خاصة في ضوء التطور السريع لإنترنت الأشياء (IoT) وسهولة التقاط الصور ونقلها، بما في ذلك تلك المرتبطة بالسفر والصحة والقطاع الزراعي والعسكري. بالإضافة إلى ذلك، نظرًا لأن كل صورة لها خصائص مهمة من حيث حجم البيانات الضخم والارتباط العالي بين بكسلات الصورة، فإن تشفيرها بمفتاح تقليدي عبر تقنية اتصالات إنترنت الأشياء يعرضها للعديد من الهجمات. يعتبر تشفير الصور الفوضوية أفضل طريقة لتشفير الصور نظرًا لحساسيتها للشروط الأولية ومعلمات التحكم. ينتج هذا البحث صورة مشفرة خالية من المعلومات الإحصائية لجعل تحليل الشفرات مستحيلًا. بناءً عليه، فإن البحث يقترح خوارزمية جديدة تعتمد على خاصية الخلط والانتشار لتعزيز الأمانية. في جوهرها، تقوم طريقة الخلط بإنشاء أرقام عشوائية لخلط كتل الصورة بالاعتماد على نظام Lorenz و Rossler. يتم استخدام خوارزمية RC4 وعملية XOR لتحقيق خاصية النشر. تم تحقيق قيمة منخفضة جدًا (10^{-3}) للارتباط بين وحدات البكسل المجاورة. علاوة على ذلك، لمنع هجمات القوة الغاشمة، تم توسيع حجم المفتاح بصورة كبيرة إلى 2^{594} وحساسية المفتاح. الصورة المشفرة الناتجة خالية من السمات الإحصائية من حيث الرسم البياني والإنتروبيا حيث تم جعل الرسم البياني متساويًا تمامًا في جميع الحالات وكان الإنتروبيا المنتجة مساوية تقريبًا للقيمة المثالية (8).

الكلمات المفتاحية: كتل فوضوية، تشفير الصورة، نظام Lorenz، خوارزمية RC4، نظام Rossler.