IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 November 2023, accepted 5 December 2023, date of publication 8 December 2023, date of current version 1 February 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3341103

RESEARCH ARTICLE

A New Image Encryption Scheme Based on the Hybridization of Lorenz Chaotic Map and Fibonacci Q-Matrix

HALA I. MOHAMED[1], SARAH M. ALHAMMAD[2], DOAA SAMI KHAFAGA[2], OSAMA EL KOMY[1], AND KHALID M. HOSNY[1], (Member, IEEE)

[1]Department of Information Technology, Zagazig University, Zagazig 44519, Egypt
[2]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Corresponding author: Sarah M. Alhammad (smalhammad@pnu.edu)

This project is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R442), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT In various image-processing applications, the fractional-order functions outperform their equivalent integer-order functions. In this study, we proposed a novel technique to encrypt color images with fractional-order chaotic systems, where the fractional-order simple Loranz is integrated with the FQM. Our novel part is hybridizing two maps (Lorenz & Fibonacci). The new algorithm benefits from the strengths of the fractional-order simple Lorenz chaotic system and the FQM to get a good performance technique. We confirm that our suggested encryption algorithms are effective and robust against attacks. Our suggested technique comprises numerous sequences: The primary color channels of the input image were separated into R-, G, and B-channel. The processes of confusion and diffusion are independent for each channel. The simple Loranz generates random integers using fractional ordering to enable pixel placements. We utilized the Fibonacci Q-matrix to dilute every 2*2 block comprising the permitted image.

INDEX TERMS Encryption, security, encrypted image, fractional-order, chaotic system, simple_Loranz, Fibonacci Q-matrix.

I. INTRODUCTION

Everyone started sharing digital stuff on the Internet as it became a part of our daily lives. However, it is also possible for unauthorized parties to easily obtain the photographs, posing a serious threat to the exchange of image information [1]. Therefore, these factors have made protecting the information in photos a crucial concern. Security of the actual images is also in danger from unauthorized cryptanalysis. More importantly, certain photos might breach people's privacy rights and deal with national security matters. For instance, this category includes biometric identification and satellite monitoring. As a result, academics and business executives worldwide have expressed great interest in how to transmit digital photos [2] securely. Digital image security is crucial for protecting image content during transmission and hiding image data from hackers. Image pixels strongly correlate with one another, and image encryption differs from standard text encryption. On a computer or a mobile device over the Internet, the chaotic system's sensitivity and dependence on certain values are significantly influenced by the initial conditions in terms of constant values and distinguishing parameters. As a result, many distinct chaos-based picture security techniques have been created successively [3]. A powerful encryption system is required to maintain high levels of image security. Additionally, photographs have a significant degree of pixel redundancy and bulk capacity, which makes them susceptible to cryptanalysis techniques., to strengthen the security of the Internet. Due to its many advantages in cryptography, such as ergodicity, unpredictable nature, pseudo-randomness, and extreme sensitivity to variables and beginning conditions, chaos-based picture encryption has grown in popularity in recent years. Using a scrambling diffusion structure is based on the idea of chaos. The DNA rule, block scrambling, bit_level scrambling, matrix manipulation, and tensor theory are more ways

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

than chaos [4], [5], [6], [7]. Using dual scrambling at the bit level and double scrambling for images to offer more security throughout the permutation process created the semi-tensor product matrix method [6]. In picture encryption techniques, predicting or understanding the key that transforms a color image into an image with noises is impossible. No one can recover the image after encryption without using the key. One approach to image security is data hiding. A cover image is used to hide a hidden message so that it cannot be seen [7], watermarking [8], [9], [10], [11] and encryption [12], [13], [14], [15], [16]. On the other hand, lately, researchers used chaotic systems to encrypt images that have high security [12], [13], [14], [15]. Chaotic systems are the best choice for picture encryption because it is random, sensitive, and unpredictable [6]. Two kinds of chaotic systems exist: 1D and HD [16]. Some researchers used 1D chaotic systems to encrypt images because it is simple [20], [21]. Most image encryption methods rely on the two phases of scrambling (also known as confusion) and diffusion. When pixels are scrambled, their values remain unchanged, but their arrangement is altered. As a result, the scrambling step decreases the correlation coefficient between neighboring pixels. The diffusion procedure achieves greater security when used on the scrambled picture. In diffusion, we use mathematical operations to change pixels' values. This process conceals the connection between the image and its encryption one [19], [20]. Our suggested technique for picture encryption will overcome the above methods' restrictions, where the suggested method uses FO and the FQM for encryption. The suggested method overcame the abovementioned restrictions and flaws, successfully securing and effectively safeguarding the color image. Chaotic systems are well-liked for picture encryption, such as Lorenz systems and their variations [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]. FOHCL system exhibits strong, intricate, and non-static. Studies have shown that it is effective for picture encryption. In this study, we look at the cryptanalytic security of the picture encryption scheme. The investigation reveals security weaknesses in the encryption process that the selected plaintext attack could exploit. So, we suggest an encryption scheme to improve the security and robustness of real-world cryptographic applications.

This paper's main contributions are:

1. simple Lorenz is used to generate a secret key that scrambles the image, this image serving as an initial step.

2. FQM is the foundation for the diffusion step [32], [33], [34], [35], [36], [37], [38], [39].

3. The simple Lorenz system and FQM are integrated to ensure high security and the ability to withstand various attack types.

II. PRELIMINARIES

A. FRACTIONAL-ORDER SIMPLE LORENZ SYSTEM

Edward Lorenz offered a chaotic map. To better understand environmental convection, the Lorenz chaotic model was developed. The differential equation system can describe the model.

$$\begin{aligned} \boldsymbol{D}^{\alpha}(\boldsymbol{x_1}) &= \boldsymbol{A_w} * (\boldsymbol{x_1} - \boldsymbol{B_w} * \boldsymbol{x_2}) \\ \boldsymbol{D}^{\alpha}(\boldsymbol{x_2}) &= (24 - 4\boldsymbol{c_w}) * \boldsymbol{x_1} + \boldsymbol{C_w}\boldsymbol{x_2} - \boldsymbol{D_w}\boldsymbol{x_1}\boldsymbol{x_3} \\ \boldsymbol{D}^{\alpha}(\boldsymbol{x_3}) &= \boldsymbol{E_w}\boldsymbol{x_1}\boldsymbol{x_2} - \boldsymbol{F_w}\boldsymbol{x_3} \end{aligned} \tag{1}$$

where $\boldsymbol{A_w}$ as $1, \boldsymbol{B_w}$ as $2, \boldsymbol{C_w}$ as $3, \boldsymbol{D_w}$ as $4, \boldsymbol{E_w}$ as $5, \boldsymbol{F_w}$ as $8/3, \alpha$ as 0.98

These values are based on an optimization process known as Particle Swarm Optimisation (PSO), which gives us optimal results to initial it in our algorithm [40], which takes inspiration from nature Various prior studies have shown the effectiveness of Lorenz systems and their derivatives in picture encryption. The optimal key settings to maximize PSNR were obtained using this method.

A, B, C, and D demonstrate the system's chaotic behavior concerning some initial values for the 'x,' 'y', and 'z' axes.

B. FQM

Mathematically, the Fibonacci sequence is a sequence in which every number after the first two is the sum of the previous two. It contains a list of numbers closely related to the golden ratio.

The Fibonacci recurrence relation

$$f_n = f_{n-1} + f_{n-2}; \text{n} > 2 \tag{2}$$

where f_n = Fibonacci number, $f_1 = f_2 = 1$.

FQM can be expressed in matrix form:

$$\text{Q} = \begin{bmatrix} f_2 & f_1 \\ f_1 & f_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \tag{3}$$

where f_n is a Fibonacci number. Then

$$Q^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} \tag{4}$$

where f_n is the Fibonacci number, and the determinant of the FQM is defined as follows:

$$(Q)^n = f_{n+1}f_{n-1} - f_n^2 = (-1)^n \tag{5}$$

Q^{-n} is the inverse of the Q^n matrix can be expressed in matrix form:

$$Q^{-n} = \begin{bmatrix} f_{n-1} & -f_n \\ -f_n & f_{n+1} \end{bmatrix} \tag{6}$$

C. INSERT AND ROTATE

Insert random pixels in the original image; we add a random integer value in the first and last columns. The following equation defines it:

$$\text{I(i,j)} = \begin{cases} Rand\,(i) & if\ j = 1 \\ Q\,(i, j-1) & otherwise \end{cases} \tag{7}$$

where Q is the processed image $M \times N$; $I(i, j)$ is the processed image $M \times (N + 1)$, $1 \leq i \leq M, 1 \leq j \leq (N + 1)$; $Rand(i)$ is a function that generates random numbers. The following equation defines picture rotation as rotating a 2D image matrix 90 degrees anticlockwise:

$$E(i, j) = C(j, N - i + 1) \tag{8}$$

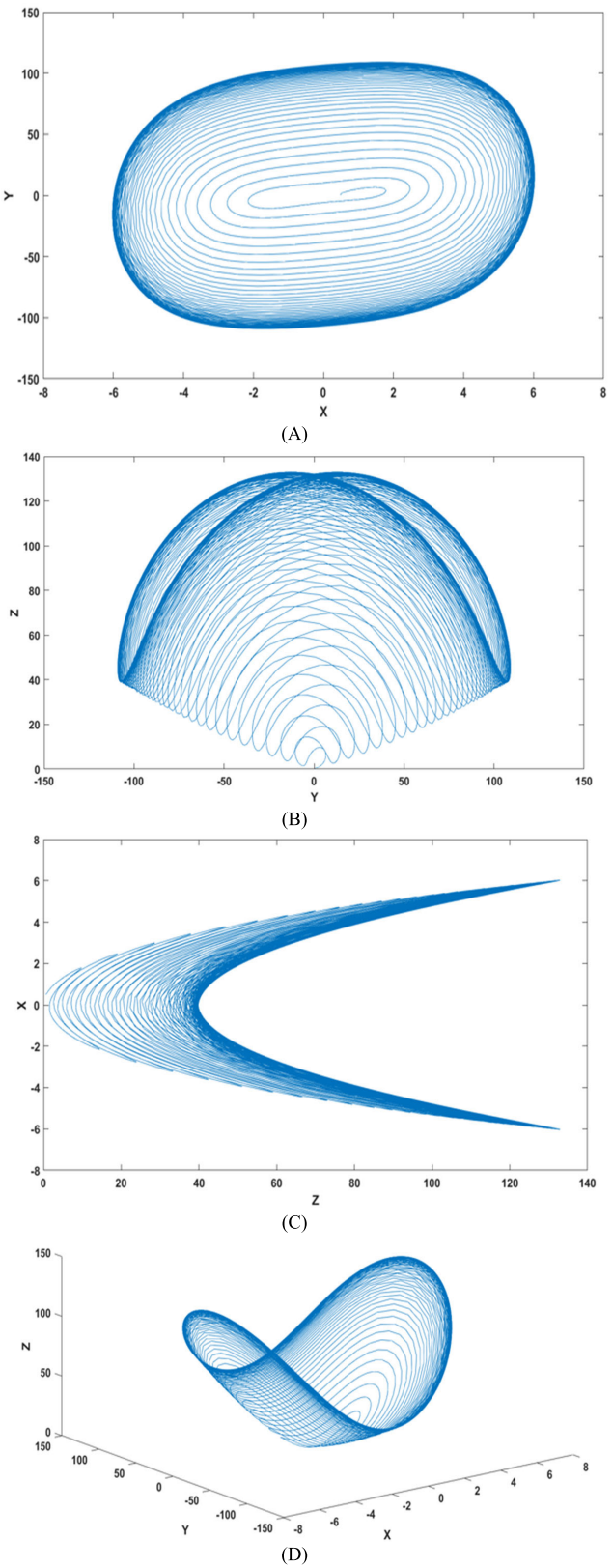

FIGURE 1. Lorenz's chaotic system behavior.

III. PROPOSED METHOD

We suggest a new algorithm to encrypt the color images. Our algorithm uses addition, rotation data, Lorenz, and Fibonacci Q-matrix. Simple Lorenz exhibits highly dynamic, complicated behaviors. Utilizing it raises the security level and enhances encryption performance. FQM is quick and simple to use, mainly for scrambling the images. Figure 2 displays a flowchart that illustrates the encryption method, and decryption is the inverse step of the encryption process. The main steps in our strategy are confusion and diffusion. Color images with size M × N × 3 divided into three channels, R-, G-, and B-; we individually encrypt each channel to get the encrypted image.

IV. ENCRYPTION

Confusion and diffusion are the two primary processes that determine the encryption method. Firstly, we insert random numbers in each row, then rotate the image. The Lorenz system is then solved using FDE. We first determine the system's initial status. The FDE is then iterated to produce a new vector, from which three sequences(x_1, x_2, and x_3) are chosen. This vector's order of sorted numbers is employed to mislead the unsorted image. The diffusion process is carried out to obtain the encrypted image after confounding the plain image. The FQM serves as the foundation for the diffusion in our algorithm. Each block of the chaotic image is diffused using the FQM, and each block is separated into 2 × 2 squares.

V. DECRYPTION

we input keys (SS, type: Cell) and encrypted image (Ienc, type: uint8) by reversing the encryption code from down to up as we first apply the reverse Fibonacci matrix. We sort the pixels as the sorting keys, and lastly, we rotate the image and remove unnecessary data.

We do this same as an encrypting process, and we extract the original image (Idec, type: uint8)

VI. EXPERIMENTAL ANALYSIS

The importance of our new algorithm is turning color images into noisy images that no one can understand its details and it become not meaningful. We evaluate this encrypted image by two methods, including information entropy and correlation analysis will discuss:

This method encrypts many types of images: (a) show the initial picture, (b) initial picture' histogram, (c) encrypted picture, and (d) encrypted picture' histogram.

A. IE

IE is a theory used to measure image unpredictability. Good image encryption technique gives encrypted images with high randomness. The entropy is calculated in every channel R-, G-, and B-. It should be close to 8 to give high randomness. Entropy can be expressed mathematically using the following formula:

$$\mathrm{IE(r)} = \sum_{i=1}^{2^q-1} p\,(r_i)\, log2 \frac{1}{p(r_i)} \tag{9}$$

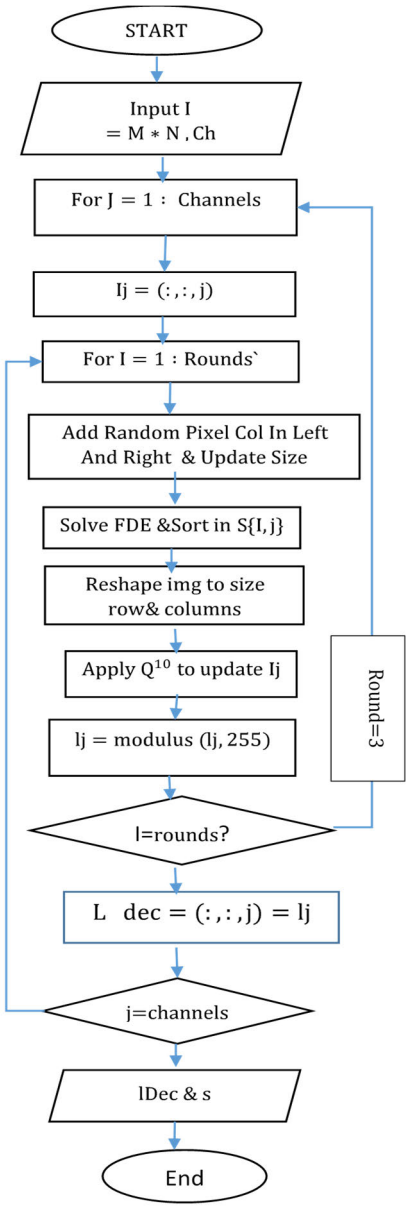

FIGURE 2. Flowchart of the proposed algorithm encryption process.

(r_i) : source of the image, q: total number of pixels, p(r_i): probability of (r_i)

2^q: total number of (r_i), we test our proposed algorithm on many images as shown below in Table 2, all results near 8. We also make a comparison with other previous methods. We show the best results in Table 3

B. LOCAL ENTROPY

The global entropy can occasionally be deceiving about the true randomness of an image. The global Shannon method's assessment of extremely high entropy levels close to their maximum may not necessarily reflect true randomness between two images. For example, a random image and an image that can be seen and recognized may have the same global entropy value to solve the global entropy.

Algorithm 1 Pseudo Code of the Proposed Method for Encryption

Input: image=>I, number of rounds => rounds
Output: Encrypted Image => Ienc, Encryption Keys => SS
Algorithm:
[row, col, number of color channels]=size(I)
if row/2 is not an integer
row=row+1
resize I with the new size
end if
if col/2 is not an integer
col=col+1
resize I with a new size
end if
save I as I_Temp
For NC = 1 to the number of color channels
I = I_Temp [:,:, NC]
For R=1 to rounds
r1,r2 => Integer random from 0 to 255 with size row∗1
add r1 as the first column of I and r2 as the last column
[row, col, number of color channels]=size(I)
MNc=row∗col∗ number of color channels
change I from *uint8* to *double*, and collect it to 1 column in P
x=(sum(P)+MNc)/(MNc+(2^23));
for i=2 to 6
x[i]=mod(x[i-1]∗1e6,1);
end for
define our Fractional Differential Function *FDE* and solve it, the results will be sorted and take its old location as S
SS{R,NC}=S
sort P location with respect to S
resize P with the same size as I
define A=[89 55;55 34]
C=zero Matrix [row∗col]
for i = 1 to row with increment 2
for j = 1 to the col with increment 2
BLK=I[i to i+1;j to j+1]
F=BLK∗A
C[i:i+1,j:j+1]=F
end for
end for
I=mod(C,255)
end for
I_enc[:,:,NC]=I
end for

C. CORRELATION ANALYSIS

The statistical method measures how pixels are related. In the original image, neighboring pixels have a high correlation. If the encryption algorithm is good, the correlation between adjacent pixels should be zero in the encrypted images. For

Algorithm 2 Decrypt Algorithm

Inputs : Encrypted image=>Ienc , Sorted Keys=>SS
Output: Decrypted Image=>Idec
Algorithm :
Convert I_enc to double in C
$A=\begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix}$
rounds = length(SS)
for round_iter starts from 1 to rounds :
[rows, cols, colors]=size(C)
D=zeros(rows,cols,colors)
For k, starts from 1 to colors :
For i, starts from 1 to rows with step=2:
For j, starts from 1 to cols with step=2:
$Cx=\begin{bmatrix} C_{i,j,k} & C_{i,j+1,k} \\ C_{i+1,j,k} & C_{i+1,j+1,k} \end{bmatrix}$
F=Cx*A
$\begin{bmatrix} D_{i,j,k} & D_{i,j+1,k} \\ D_{i+1,j,k} & D_{i+1,j+1,k} \end{bmatrix}= \begin{bmatrix} F_{i,j,k} & F_{i,j+1,k} \\ F_{i+1,j,k} & F_{i+1,j+1,k} \end{bmatrix}$
end for
end for
end for
Keys=SS{round_iter}
W=D(:)
Sort W in the sorting order of Keys
C = reshape(W,[rows,cols,colors])
C=mod(C,256)
C=rotate(C)
delete the first and last columns of C
end for
Idec=C

example, the Table below shows a relation between two pixels, x and y, for different images.

Wu and Zhou [41] proposed using the local Shannon entropy, which is determined by averaging the local entropy values of a random sample of non-overlapping image blocks. In mathematics, it is written as;

$$H_{n.T_g}(S) = \sum_{i=1}^{n} \frac{H(S_i)}{n} \tag{10}$$

T_g: local block size, n: number of blocks represented by S_i The (n, T_g). Local entropy results for different encrypted images are shown in the table below.

IE entropy should be 8 in any image layer. Our result is near eight, which proves high randomness.

We Compared the proposed algorithm IE with another method IE, and we show this algorithm have higher randomness than all method we listed.

This Table shows the relation between two pixels x y in Lena's image. All results near zero this value show a good algorithm.

TABLE 1. Colored images we will use in this paper.

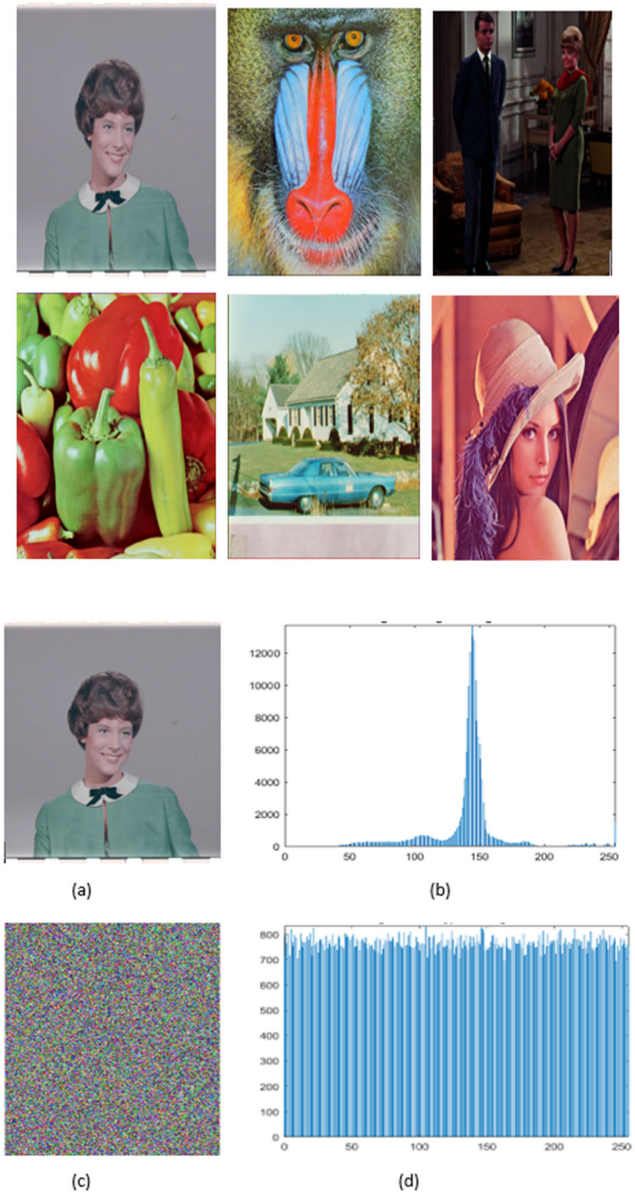

FIGURE 3. Female histogram, and it's encrypted.

D. DATA LOSS AND NOISE ATTACKS

Images in practical applications suffer from transmission noise and data loss. Any picture encryption technique should resist noise attacks and data loss. We display in the below figure the outcomes of these two attacks. Our suggested technique encrypts an image first. Then, individually, decrypt these two images by applying A data cut 64 × 64 and 1% Salt & Pepper noise. We observe a few data losses and noise when we reconstruct the images. These show the proposed algorithm's resistance to data loss and noise attacks.

Salt and pepper noise (0.002) in the encrypted image. Salt and pepper noise (0.005) in the encrypted image. Data cut attack: size 128 ×128 and 64 × 64.

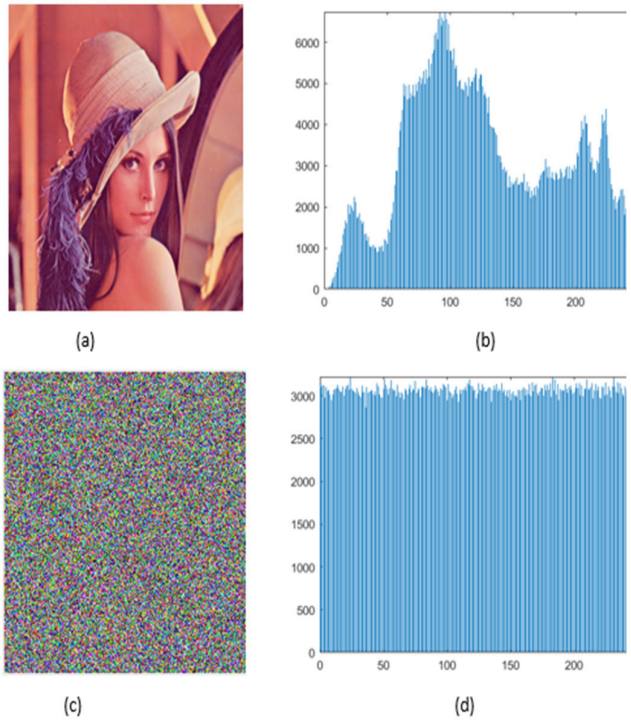

FIGURE 4. Lena e histogram, and it's encrypted.

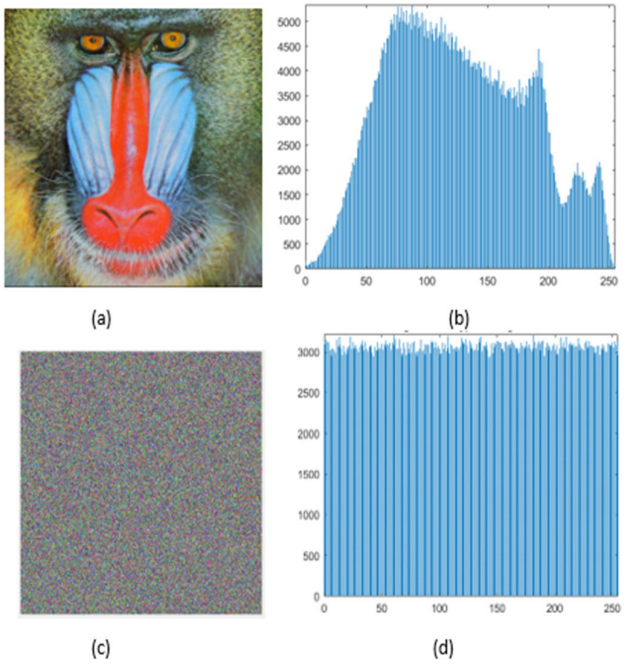

FIGURE 5. Baboon histogram, and it's encrypted.

Images that have been encrypted may experience data loss or noise during network transmission. An encryption method is successful when the encrypted image can be restored following noise and data cut attacks. This capability

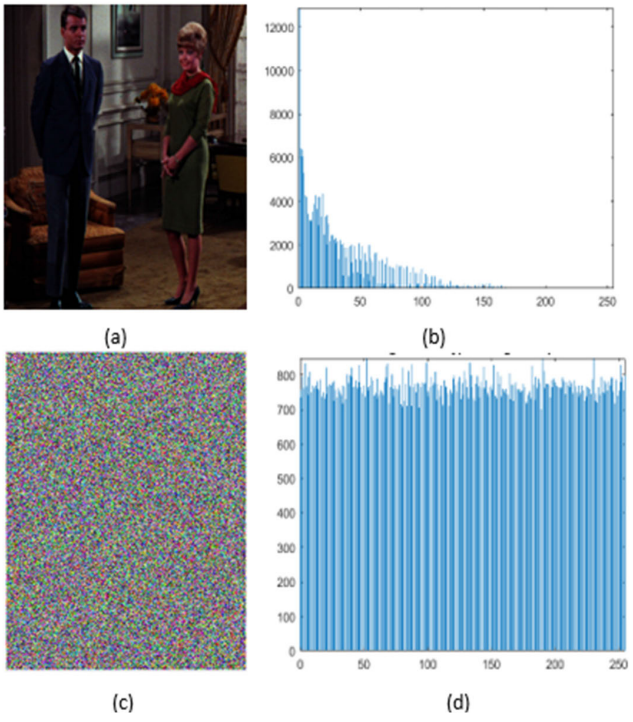

FIGURE 6. Couples histogram and its corresponding encrypted.

TABLE 2. IE and local entropy analysis.

Image	Information entropy	Local entropy
Babon	7.9993	7.1051
Couple	7.9993	7.1018
Female	7.9972	7.0848
Lena	7.9994	7.1167

is responsible for the (PSNR), determined by:

$$\text{PSNR} == 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{11}$$

The MSE is defned by:

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{n}|I_0(\text{i},\text{j}) - I_d(\text{i},\text{j})|^2 \tag{12}$$

The terms I_0"original" and I_d"encrypted" photos are used. High PSNR values indicate a high degree of similarity between the decrypted and the original image and are directly correlated to image quality. It isn't easy to discern between the original and decrypted images when the PSNR value is higher than 35. We perform the following tests on the encrypted image to see how well the suggested technique can resist various attacks:

- salt & pepper (SPN) with densities of 0.002 and 0.005
- Data cut with sizes 64 × 64 and 128 × 128. In the left-top

TABLE 3. Comparison of entropy values with our algorithm and other algorithms.

Method	Lena	Pepper	Baboon
[26]	7.9992	7.9993	7.9994
[1]	7.9993	7.9993	7.9994
[31]	7.9974	7.9994	7.9972
[19]	7.9975	7.9970	7.9972
Proposed	7.9994	7.9997	7.9992

Our algorithm improves the robustness against noise and data cut attacks because we can recognize the image. In the below Table PSNR for color image Lena in the three channels. With a 64-bit data cut size, we added noise with densities of 0.002 and 0.005. The experimental findings show that our technique restores encrypted images successfully after attacks.

We evaluate the resistance of our suggested algorithm to noise attacks. First, Lena's encrypted image is accompanied by salt and pepper noise of varied densities. Then, we employ our suggested approach to decrypt the obtained photos. The effectiveness of the suggested approach in decrypting the attacked image is shown in Fig. 9. All content of the decrypted photos is still identifiable. Table 5 lists the PSNR values between the plain and decrypted images after noise addition. When adding SPN with densities of 0.002 and 005, the PSNR values are around 25 and 21, respectively. The PSNR value increases with the similarity between the original and decrypted images. Finally, it is shown that the proposed algorithm is a noise-resistant

E. ROTATION WITH DIFFERENT ANGLES ATTACKS

VII. KEY SENSITIVITY AND KEYSPACE

The sensitivity of a good cryptographic algorithm to the secret keys must be quite great. A decent encryption (decryption) technique produces two entirely different encrypted (decrypted) images for two keys that differ only slightly. The color image is used in the key sensitivity test for the proposed image encryption scheme.

In contrast, slightly different sets of keys from the original keys are used during the decryption procedure. The images that have been decoded are displayed in Fig.12 to show how sensitive the proposed cryptographic procedure is to the secret keys, which provides a limited guarantee of the proposed picture encryption algorithm's security against brute-force attacks.

keyspace used in cryptography to describe the number of bits in a key that a cryptographic technique; for efficient encryption techniques to withstand brute-force attacks,

TABLE 4. Correlation analysis Lena in three directions.

Image	Color Channel	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Baboon	R	0.0157786	-0.007024	0.031825
	G	-0.022881	-0.001657	-0.006499
	B	0.026992	-0.00255	0.068920
Couple	R	-0.014722	-0.058260	-0.018614
	G	0.035149	0.015446	0.030473
	B	-0.016964	-0.002881	-0.037193
Female	R	-0.041620	0.019118	0.041024
	G	-0.001892	0.050320	0.048694
	B	-0.00616	0.00273	-0.000381
Lena	R	-0.001112	-0.027695	0.041276
	G	-0.033311	0.049580	0.003869
	B	0.011987	-0.017521	-0.047993

TABLE 5. Correlation coefficients in three directions: Horizontal (H), Vertical (V), and Diagonal (D) for baboon image.

method	direction	Correlation coefficient
[26]	H	0.9734
	V	0.9802
	D	0.9853
[31]	H	−0.0080
	V	−0.0116
	D	0.0291
[19]	H	0.0065
	V	0.0337
	D	0.0244
Proposed	H	0.0157786
	V	-0.007024
	D	0.031825

keyspaces must be sufficiently large than 2^{100}, our proposed method has key including eight parameters its values carried on the secure channel between sender and receiver, A_w, B_w, C_w, D_w, E_w, F_w. α. N: number of rounds. If the precision is 10^{16} for each parameter, And this leads to that key space very large and exceed 2^{100}, $8\times10^{16} = 10^{128} \approx 2^{425}$, The keyspace of the proposed algorithm is sufficiently large to resist brute-force attacks.

VIII. DIFFERENTIAL ATTACK ANALYSIS

Attackers attempt to link the original image to the encrypted image by relying on a slight modification to both the original and encrypted image that uses the same encryption technique.

An effective encryption algorithm must be more sensitive to any slight change in the original image to fight against this

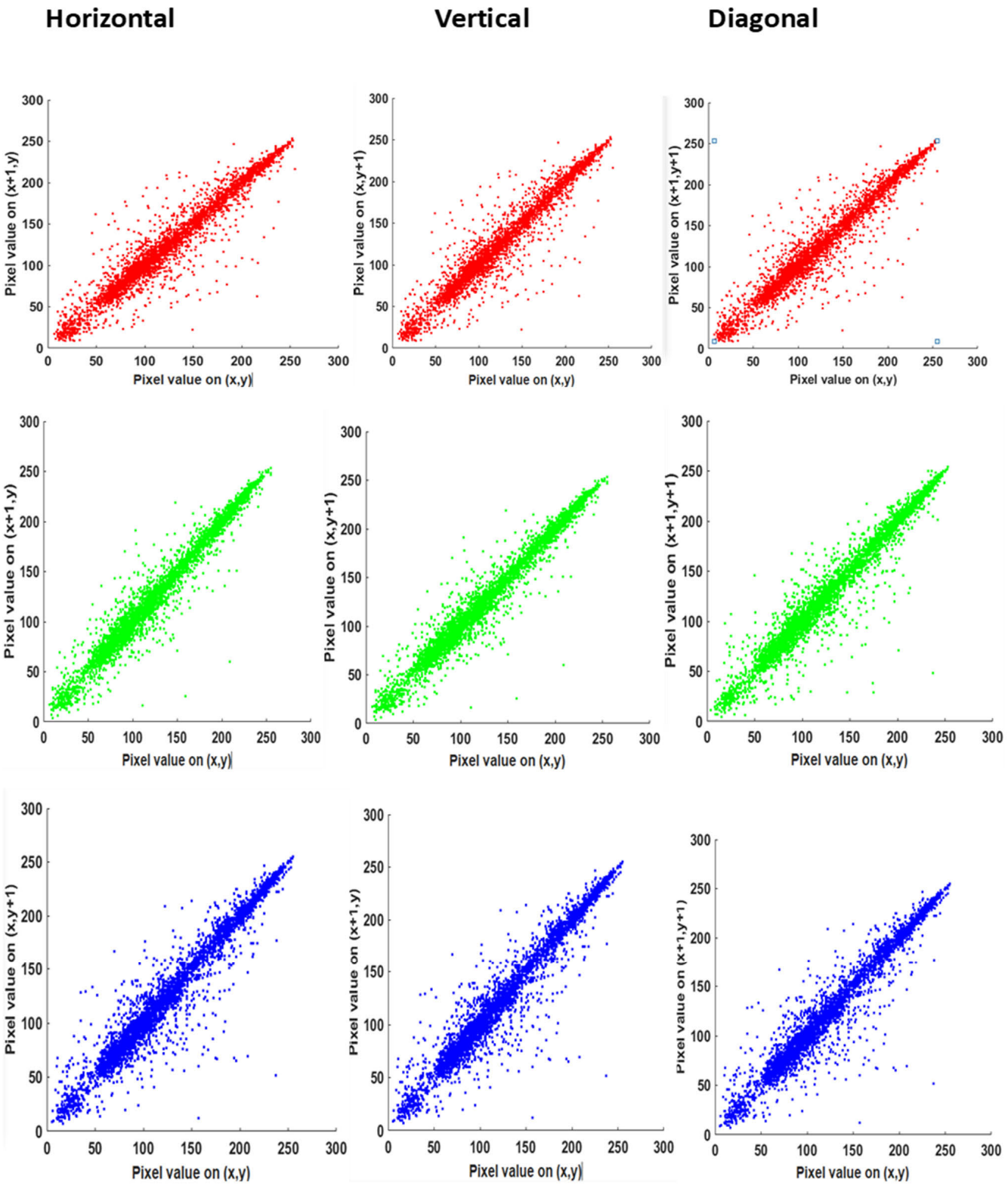

FIGURE 7. Lena's correlation in each of the three channels' three-way directions.

attack. To evaluate the sensitivity of our proposed algorithm to the original image, we estimate two differential attacks: (NPCR) and (UACI), two methods employed to carry out a differential attack analysis.

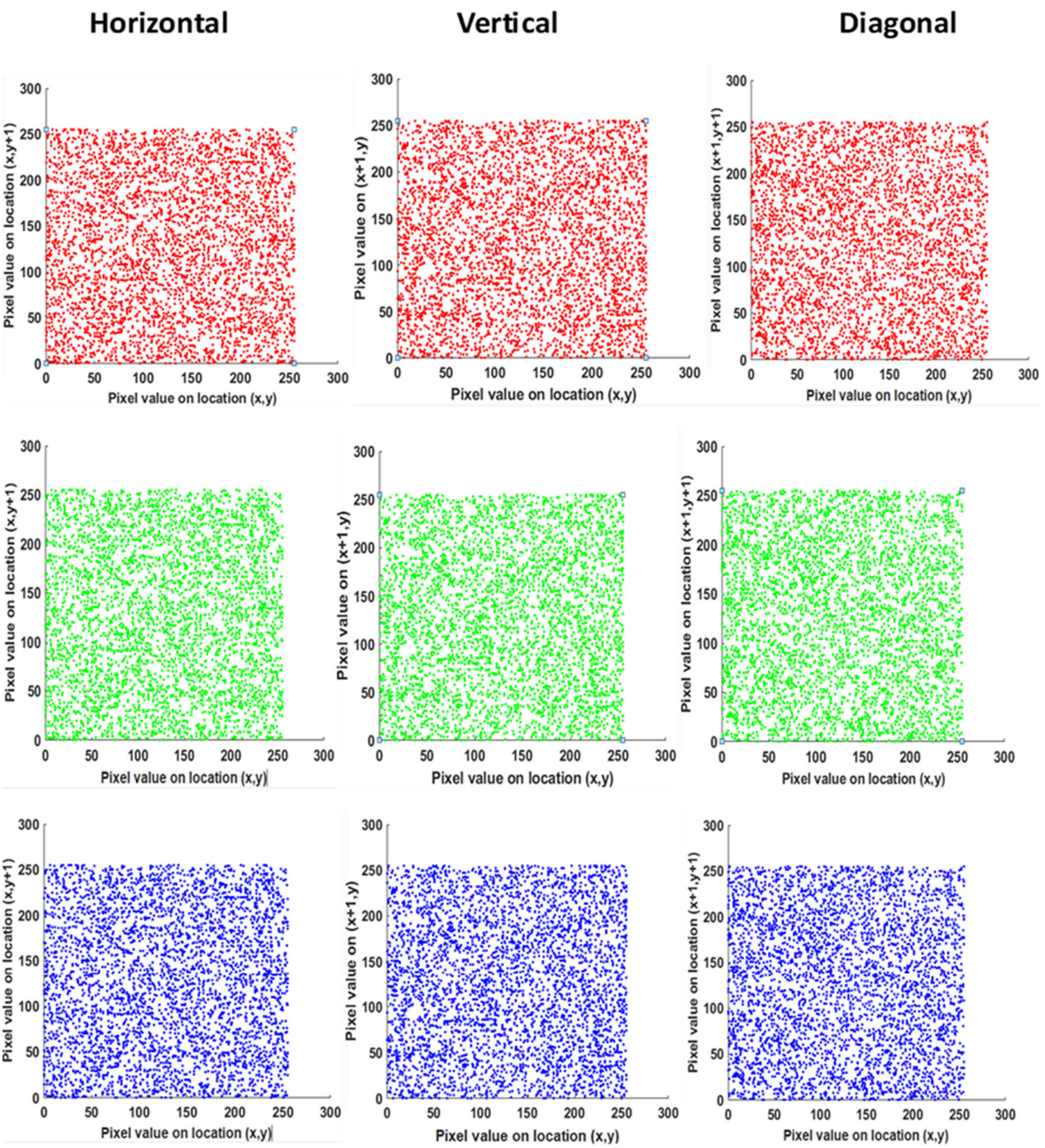

FIGURE 8. Lena's encrypted picture correlation for the three channels.

A. THE NUMBER OF PIXEL CHANGING RATE

The NPCR measures the number of pixels which are different between two images. It is mathematically expressed as:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D_{i,\mathrm{j}}}{M \times N} \times 100 \tag{13}$$

$$D_{i,j} == \begin{cases} 0, \mathbf{C1}_{(i,j)} = \mathbf{C2}_{(i,j)} \\ 1, \mathbf{C1}_{(i,j)} \neq \mathbf{C2}_{(i,j)} \end{cases} \tag{14}$$

B. THE UNIFIED AVERAGE CHANGE INTENSITY

The UACI measures the difference in the average intensity between the encrypted and plain images. It is mathematically

TABLE 6. Len Data's noise-adding and cutting attacks.

	PSNR_1	PSNR_2	PSNR_3
SNP D=0.002	25.585928	26.459722	27.484027
SNP D=0.005	21.883345	22.328344	23.744992
Data Cut 128*128	14.300155	14.993263	16.07020
Data Cut 64*64	19.992347	20.698952	21.681527

TABLE 7. Rotarion attack with different angles.

	Peak_ SNR_1	Peak_ SNR_2	Peak_ SNR_3	SSIM_ Value_1	SSIM_ Value_2	SSIM_ Value_3
90°	7.8499	8.5694	9.6192	0.01005	0.00911	0.01026
180°	7.8690	8.5572	9.6160	0.01010	0.00919	0.01051
270°	7.8649	8.5600	9.6237	0.0101	0.00924	0.0099

TABLE 8. NPCR and UACI attacks analysis.

Test type	Image	Result
NPCR (%)	Lena	99.6278
	Pepper	99.6242
	Babon	99.6127
UACI (%)	Lena	33.3466
	Pepper	33.4752
	Babon	33.5434

expressed.

$$\text{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255} \qquad (15)$$

where M & N refer to two dimensions of the image, C_1 & C_2 are encrypted images and modified image

We change the random pixel in the original image, encrypt it, and encrypt the original image, and repeat this step in the three layers more times. We take the average, and we get a result that is near the expected value, which leads to how sensitivity of our proposed algorithm to any change, and it can resist differential attacks.

(a) initial picture,(b) encrypted picture before the attack, and (c) encrypted picture after the rotation attack

Here we make acomparison between the proposed method and other methods,In comparison to other approaches, our suggested algorithm gets the highest pass rate, demonstrating the superior robustness of the differential attack.

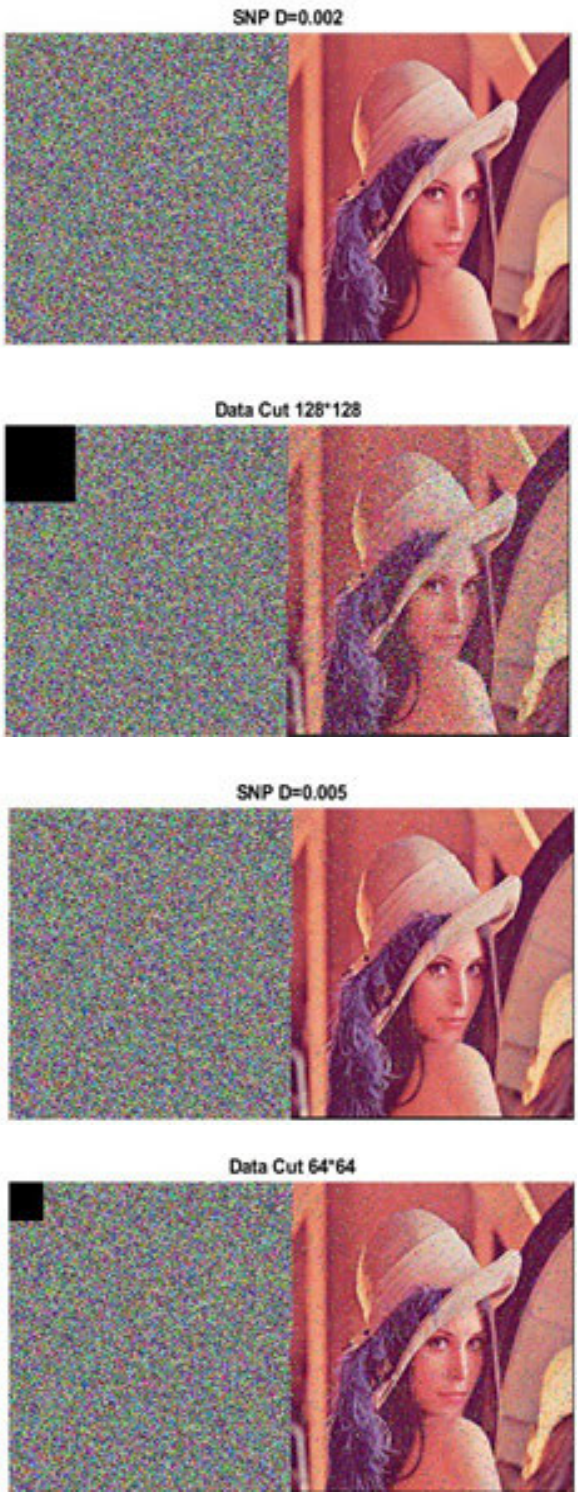

FIGURE 9. Data loss and noise attacks.

IX. COMOLEXITY

The execution times for encryption and decryption are within a few seconds and fractions of a second. The time required to convert plain text into cipher text is known as the encryption time of a cryptography algorithm. The encryption time, determined as the total encrypted plaintext (in bytes) divided

TABLE 9. Comparsion of average values of NPCR and UACI. for Lena image.

Method	NPCR	UACI
[1]	99.60	28.62
[19]	99.61	33.43
[31]	99.65	33.42
Proposed	99.62	33.34

TABLE 10. TIme analysis of encryption and decryption process.

Image Size	T_{ENC} (S)	T_{DEC} (S)
128× 128	0,90579	0,25963
256× 256	3.3978	1,1169
512× 512	11,274	4.2117

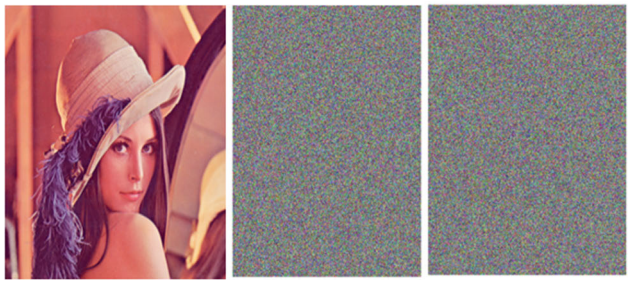

FIGURE 10. Lena with a 90° rotation attack.

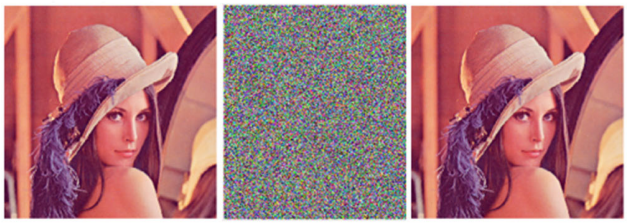

FIGURE 11. Key sensitivity analysis with the correct key: (a) Original image (b) encrypted image using correct key (c) decrypted image.

by the encryption time (in ms), determines the throughput of any encryption process.

X. CONCLUSION

A new technique to encrypt any color image was proposed in this paper. The FQM is combined with a simple Loranz in this system. This combination is very useful because we use the strengths of the two maps. Hence, we get more accurate results and high security and high-performance encryption algorithms very secure than we use every map alone. We create random sequences by changing the pixel location using a Loranz fraction system. For this image, then for each subblock (size(2 × 2)), FQM modifies the pixels' value. To increase safety, double confusion/diffusion techniques use the secret key, which can be used to decrypt a different image, and minor changes in pixel distribution are sensitive to the new method. The differential attack is thus successfully repelled by the proposed technique. This method brute-force attacks because of the large keyspace size and effective security. Data cut attack, histogram, noise, correlation coefficients, and IE are used with high-security settings.

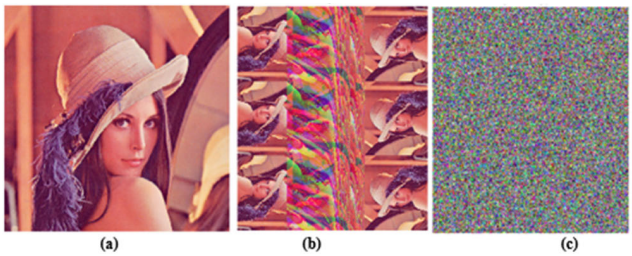

FIGURE 12. Key sensitivity analysis with a slight change in key: (a) Original image (b) encrypted image using key σ =, 35 (c) decrypted image.

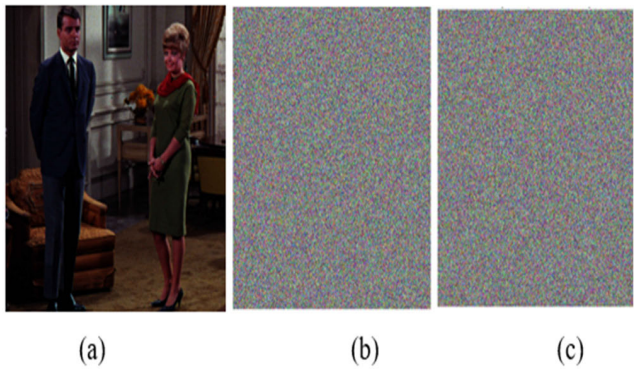

FIGURE 13. The couple image with 180° rotation attack 2.

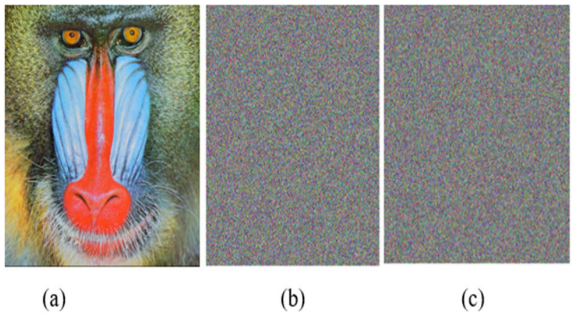

FIGURE 14. Baboon image with 270° rotation attack.

ABBREVIATION

F.Q.M:	Fibonacci Q-matrix
F.O:	Fractional Order
F.O.H.C.L	**:** Fractional Order Hyperchaotic Loranz
IE:	Information Entropy
1D:	One dimension
2D:	Two Dimension
P.S.N.R:	Peak signal-to-noise ratio

ACKNOWLEDGMENT

This project is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number

(PNURSP2023R442), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] R. Lin and S. Li, "An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm," *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, Apr. 2021.

[2] J. Ferdush, M. Begum, and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Adv. Multimedia*, vol. 2021, pp. 1–16, May 2021.

[3] S.Wang and Q. Peng, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Opt. Laser Technol.*, vol. 148, Apr. 2022, Art. no. 107753, doi: 10.1016/j.optlastec.2021.107753.

[4] K. Shahna and A. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," *Signal Process., Image Commun.*, vol. 99, Nov. 2021, Art. no. 116495.

[5] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," *Multimedia Tools Appl.*, vol. 81, no. 1, pp. 505–525, Jan. 2022.

[6] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[7] K. M. Hosny and M. Abdel-Aziz, "Improved data hiding method for securing color image," *Multimedia Tools Appl.*, vol. 80, pp. 12641–12670, Mar. 2021.

[8] D. Mata-Mendoza, M. Cedillo-Hernandez, F. Garcia-Ugalde, A. Cedillo-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Secured telemedicine of medical imaging based on dual robust watermarking," *Vis. Comput.*, vol. 38, no. 6, pp. 2073–2090, Aug. 2021, doi: 10.1007/s00371-021-02267-3.

[9] K. M. Hosny and M. M. Darwish, "New geometrically invariant multiple zero-watermarking algorithm for color medical images," *Biomed. Signal Process. Control*, vol. 70, Sep. 2021, Art. no. 103007.

[10] K. M. Hosny, M. M. Darwish, and M. M. Fouda, "Robust color images watermarking using new fractional-order exponent moments," *IEEE Access*, vol. 9, pp. 47425–47435, 2021.

[11] K. M. Hosny and M. M. Darwish, "Resilient color image watermarking using accurate quaternion radial substituted Chebyshev moments," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 2, pp. 1–25, May 2019.

[12] Y. Li, H. Yu, B. Song, and J. Chen, "Image encryption based on a single-round dictionary and chaotic sequences in cloud computing," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 7, p. 1, Apr. 2021.

[13] J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, "Image encryption using block cipher and chaotic sequences," *Signal Process., Image Commun.*, vol. 79, pp. 24–31, Nov. 2019.

[14] S. Yan, L. Li, B. Gu, Y. Cui, J. Wang, and J. Song, "Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image," *Integration*, vol. 88, pp. 203–221, Jan. 2023.

[15] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Syst. Signal Process.*, vol. 32, no. 1, pp. 281–301, Jan. 2021.

[16] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map," *Vis. Comput.*, vol. 39, no. 3, pp. 1027–1044, Mar. 2023.

[17] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi, and I. Hussain, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map," *Math. Comput. Simul.*, vol. 190, pp. 826–836, Dec. 2021.

[18] S. GaoImage and X. Wang, "Encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[19] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix," *Electronics*, vol. 10, no. 9, p. 1066, Apr. 2021.

[20] M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. M. Al-Jubari, "Designing 1D chaotic maps for fast chaotic image encryption," *Electronics*, vol. 10, no. 17, p. 2116, Aug. 2021.

[21] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, pp. 1–18, Feb. 2021.

[22] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyperchaotic system," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 2, pp. 973–988, Feb. 2022.

[23] M. Tang, G. Zeng, Y. Yang, and J. Chen, "A hyperchaotic image encryption scheme based on the triple dislocation of the liu and Lorenz system," *Optik*, vol. 261, Jul. 2022, Art. no. 169133.

[24] W. Alexan and M. ElBeltagy, "Lightweight image encryption: Cellular automata and the Lorenz system," in *Proc. Int. Conf. Microelectron. (ICM)*, Dec. 2021, pp. 34–39, doi: 10.1109/ICM52667.9664961.2021.

[25] W. S. Sayed, A. G. Radwan, H. A. H. Fahmy, and A. Elsedeek, "Trajectory control and image encryption using affine transformation of Lorenz system," *Egyptian Informat. J.*, vol. 22, no. 2, pp. 155–166, Jul. 2021.

[26] M. Khan and A. Rasheed, "A fast quantum image encryption algorithm based on affine transform and fractional-order lorenz-like chaotic dynamical system," *Quantum Inf. Process.*, vol. 21, no. 4, p. 134, Apr. 2022.

[27] V. M. Silva-García, R. Flores-Carapia, M. A. Cardona-López, and M. G. Villarreal-Cervantes, "Generation of boxes and permutations using a bijective function and the Lorenz equations: An application to color image encryption," *Mathematics*, vol. 11, no. 3, p. 599, Jan. 2023.

[28] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, S-Box and the Lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, Feb. 2022, doi: 10.3390/sym14030443.

[29] S. Moon, J.-J. Baik, and J. M. Seo, "Chaos synchronization in generalized Lorenz systems and an application to image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 96, May 2021, Art. no. 105708.

[30] V. Kumar and A. Girdhar, "A 2D logistic map and lorenz-rossler chaotic system based RGB image encryption approach," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 3749–3773, Jan. 2021.

[31] B. Ahuja, R. Doriya, S. Salunke, M. F. Hashmi, A. Gupta, and N. D. Bokde, "HDIEA: High dimensional color image encryption architecture using five-dimensional gauss-logistic and Lorenz system," *Connection Sci.*, vol. 35, no. 1, Dec. 2023, Art. no. 2175792.

[32] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023, doi: 10.1109/ACCESS.2023.3242311.

[33] C. Maiti, B. C. Dhara, S. Umer, and V. Asari, "An efficient and secure method of plaintext-based image encryption using Fibonacci and tribonacci transformations," *IEEE Access*, vol. 11, pp. 48421–48440, 2023, doi: 10.1109/ACCESS.2023.3276723.

[34] Y. Naseer, T. Shah, and D. Shah, "A novel hybrid permutation substitution base colored image encryption scheme for multimedia data," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102829.

[35] X. Zhang, M. Liu, and J. Tian, "Multiple-image encryption algorithm based on sarrus rule and 3D Fibonacci matrix," *Phys. Scripta*, vol. 98, no. 5, May 2023, Art. no. 055208, doi: 10.1088/1402-4896/acc905.

[36] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Comput. Appl.*, vol. 34, no. 21, pp. 19313–19341, Nov. 2022.

[37] Y. Ma and N.-R. Zhou, "Quantum color image compression and encryption algorithm based on Fibonacci transform," *Quantum Inf. Process.*, vol. 22, no. 1, p. 39, Jan. 2023.

[38] G. Biban, R. Chugh, and A. Panwar, "Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix," *Chaos, Solitons Fractals*, vol. 170, May 2023, Art. no. 113396.

[39] R. Anandkumar and R. Kalpana, "A Fibonacci p-code traversing and unified chaotic map-based image encryption algorithm," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 8, pp. 3713–3727, Aug. 2022.

[40] X. Yang, *Nature-Inspired Optimization Algorithms*. Amsterdam, The Netherlands: Elsevier, 2014.

[41] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.