2022 International Conference on Advances in Computing, Communication and Materials (ICACCM) | 978-1-6654-7439-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACCM56405.2022.10009076

A Novel Image Encryption using 3D Logistic Map and Improved Chirikov Map

Ch. Jnana Ramakrishna[1*], D. Bharath Kalyan Reddy[2], B. Vishaal Bharadwaj[3], Sonali Agrawal[4], Ganapathi Hegde[5]
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru
Amrita Vishwa Vidyapeetham, India
chjramakrishna25@gmail.com[1], dbkrbharath@gmail.com[2], vishbariki@gmail.com[3], a_sonali@blr.amrita.edu[4] ,
ganapathi_hegde@blr.amrita.edu[5]

***Abstract*—Images are one of the essential data being generated daily. Many images are taken in our day-to-day life. It is vital to keep those images secure. This paper proposes a new image encryption algorithm utilizing a 3D Logistic Map and an improved Chirikov Map. There have been several suggested image encryption techniques using chaotic maps. Some of these are time expensive and sophisticated, while others have limited key space. A non-linear 3D Logistic Map performs better in terms of randomization attributes and security measures. With the modification in the Chirikov Map from the standard map adds more robustness to the algorithm by producing a cipher image which is a more secure and random image compared with the plain-text image. This paper performed well-known cryptographic tests to assess the security and performance analysis of the proposed scheme. The proposed scheme is resistant to brute force attacks and differential cryptanalysis. The algorithm is susceptible, even to a slight change in the secret key.**

Keywords— Logistic Map, Chirikov Map, Image Encryption, Cryptanalysis, Chaotic Map.

I. Introduction

Communication networks have extended around the world and have drastically altered our lives. This digital information comprises pictures, audio, and text data, among other things. In today's world, the use of multimedia data is increasing. Image is multimedia data utilized in authentication, biology, military research, online commerce, medical, personal albums, and other applications. Because of huge data size, the high correlation of pixels, and high redundancy, conventional cryptosystems like RSA, DES, 3DES, AES, and others are not suitable for multimedia applications [1]. Due to its resemblance to the noise signals that cause randomness in image pixels for unauthorized individuals, chaos-based encryption has received much interest. Some characteristics are sensitivity to the initial parameters, diffusion, and confusion.

Regarding security, several studies advise that an encryption algorithm can be used directly on the image without compression [2]-[7]; however, this technique is rarely practical because the information to be conveyed demands a large amount of transmission capacity [8]. Pixel value transformation and pixel position scrambling are the two types of image encryption algorithms. Pixel value transformation is done using chaos equations, which were proposed in the 1970s by a group of researchers. Many chaotic algorithms were proposed in recent years [9], [10]. Pixel position scrambling is done using a modified chirikov map.

Several image encryption algorithms are proposed every year. Many algorithms are proposed by using text encryption cryptosystems like RSA, AES, and 3DES in [11]-[17], but they are not much useful for image encryption as they consume a lot of time and computation speed. In the past few years, image encryption based on chaotic maps had a potential increase in the usage of encryption due to its robustness, unpredictability, and security [1], [4]-[8], [11]. Researchers suggested algorithms combining two chaotic maps [18] for more robustness. Research using S-box with chaotic sequences [3],[19] proposed new schemes of encryption. In [1], researchers used Chen's hyper-chaotic system along with 2D compressive sensing, applying cyclic shift to the suggested scheme modifies the pixel values efficiently. M.A. Murillo-Escobar, C. Cruz-Hernández et.al., proposed a novel algorithm based on plaintext image characteristics 1D logistic map based on Murillo-Escobar's algorithm [2]. Akram Belazi et al. suggested a novel encryption algorithm using S-box for substitution and permutations followed by diffusion using a logistic map [3]. In [4], Yushu Zhang and Di Xiao used a discrete chirikov standard map to scramble image pixels, and chaos-based fractional random transform, double random phase encoding, is used to complete the process. In 2017, Xiaoling Huang and Guodong Ye proposed an encryption scheme based on an intertwining logistic map with many control parameters and more initial conditions that make the algorithm unpredictable to break in brute-force attacks [20]. Image encryption is also applied in the medical field to protect medical images [21]. Even biometrics are used as a key in encryption algorithms [22].

This paper proposes a novel image encryption scheme based on a 3D logistic map and an improved chirikov map. The 3D logistic map and improved chirikov map are utilized to modify pixel values and scramble pixel positions. The maps depend on the initial parameters and values, without which it is impossible to decrypt the cipher image due to the ample key space. The algorithm is susceptible to an acute change in the initial values and key parameters.

The rest of the paper is arranged as follows. A brief overview of the existing 3D Logistic Chaotic and improved Chirikov Map is elaborated in section II. Section III introduces the proposed scheme for the encryption and decryption of images. Section IV provides the results and analysis, and section V presents the comparison with state-of-the-art methods. Section VI presents the conclusion.

II. 3D Logistic Chaotic Map and Improved Chirikov Map

A. 3D Logistic Chaotic Map

The logistic map, which is one of the simplest chaos generations, is used and is given by an equation.

$$x_n = \mu x_n(1 - x_n) \tag{1}$$

For the equation to be chaotic, it must be considered the conditions $0<x<1$ and $\mu=4$. It is extended to 3D chaos to enhance security.

$$x_{n+1} = \alpha x_n(1 - x_n) + \beta y_n^2 x_n + \gamma z_n^3 \tag{2}$$

$$y_{n+1} = \alpha y_n(1 - y_n) + \beta z_n^2 y_n + \gamma x_n^3 \tag{3}$$

$$z_{n+1} = \alpha z_n(1 - z_n) + \beta x_n^2 z_n + \gamma y_n^3 \tag{4}$$

Where, α, β, γ are parameters. For the above equations to exhibit chaotic behavior, the values of parameters should be between 3.68<α<3.99, 0<β<0.022, 0<γ<0.015, and the initial conditions for x, y, z can be any value in a range from 0 to 1 [6], [23].

B. Improved Chirikov Map

The chirikov map is also used in chaos generation to scramble the pixel positions of the image. The standard mapping expression for the chirikov map is

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} (k \sin y_n + x_n) mod\ 2\pi \\ (x_{n+1} + y_{n)} mod\ 2\pi \end{pmatrix} \tag{5}$$

As the value of k (Control parameter) is increased, the mapping image reaches a certain threshold; the mapping will become chaotic and evenly fill up the spaces. The parameters (x_n, y_n) and (x_{n+1}, y_{n+1}) is the pixel position before and after the application of equations respectively. A new control parameter 'h' is added to the chirikov map to increase the arbitrariness of the input parameters and the security of the image [24].

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} (k \sin y_n + x_n)\ mod\ 2\pi \\ (x_{n+1} + h y_n)\ mod\ 2\pi \end{pmatrix} \tag{6}$$

The original pixel positions for the improved chirikov map can be computed as

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} (x_n - k \sin y_n)\ mod\ 2\pi \\ (\frac{y_{n+1} - x_{n+1}}{h})\ mod\ 2\pi \end{pmatrix} \tag{7}$$

III. Proposed Scheme

In this section, the proposed encryption and decryption algorithm to secure the images is discussed. The encryption scheme has two stages of encryption, initially by the 3D logistic map and later with an improved chirikov map for better image security. The algorithm is inputted with different-sized images to get encrypted images. The proposed methods and analyses of the encryption and decryption processes are listed below. The flowchart for the scheme is given in Fig. 1 and Fig. 2.

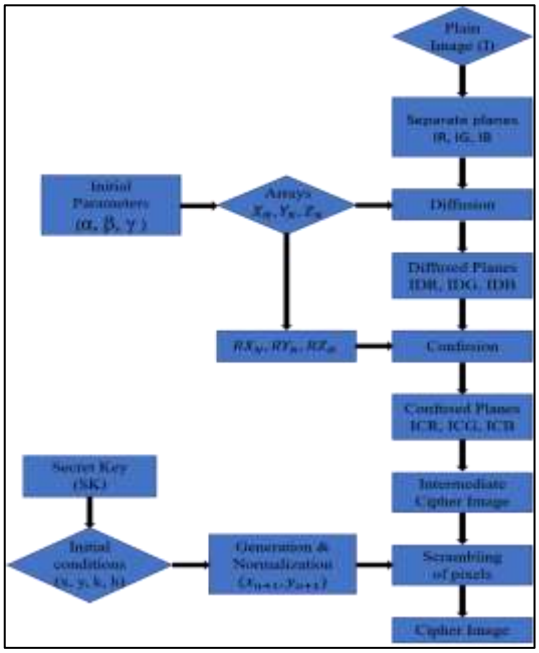
Plain Image (I)
Separate planes IR, IG, IB
Initial Parameters (α, β, γ)
Arrays X_N, Y_N, Z_N
Diffusion
Diffused Planes IDR, IDG, IDB
RX_N, RY_N, RZ_N
Confusion
Confused Planes ICR, ICG, ICB
Secret Key (SK)
Intermediate Cipher Image
Initial conditions (x, y, k, h)
Generation & Normalization (x_{n+1}, y_{n+1})
Scrambling of pixels
Cipher Image

Fig. 1. Encryption Flowchart

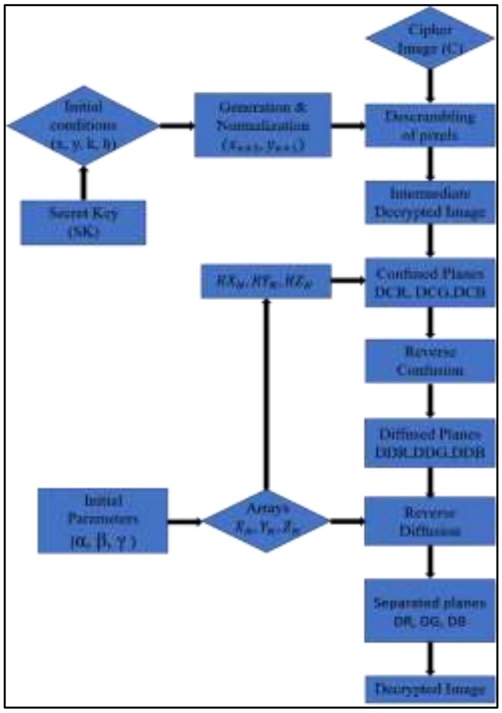
Cipher Image (C)
Initial conditions (x, y, k, h)
Generation & Normalization (x_{n+1}, y_{n+1})
Descrambling of pixels
Secret Key (SK)
Intermediate Decrypted Image
RX_N, RY_N, RZ_N
Confused Planes DCR, DCG,DCB
Reverse Confusion
Diffused Planes DDR,DDG,DDB
Initial Parameters (α, β, γ)
Arrays X_N, Y_N, Z_N
Reverse Diffusion
Separated planes DR, DG, DB
Decrypted Image

Fig. 2. Decryption Flowchart

A. Encryption Algorithm

A 3D logistic map coupled with the chirikov map is used for the encryption of the image. Eq. (2), (3), (4) along with the chirikov map's Eq. (7) are used to develop the encryption scheme for the image. The flowchart for the step-by-step process is shown in Fig. 1. The steps of encryption are-

1. Diffused plane image is generated as
2. $IDR_N = X_N * IR_N$, $IDG_N = Y_N * IG_N$, $IDB_N = Z_N * IB_N$.
3. Before confusion, convert X_N, Y_N, Z_N into the range from 0 to 255 and let them be RX_N, RY_N, RZ_N. For the generation of confused plane images,
4. $ICR_N = RX_N \oplus IDR_N$, $ICG_N = RY_N \oplus IDG_N$ and $ICB_N = RZ_N \oplus IDB_N$.
5. Before confusion, convert X_N, Y_N, Z_N into the range from 0 to 255 and let them be RX_N, RY_N, RZ_N. For the generation of confused plane images,
6. $ICR_N = RX_N \oplus IDR_N$, $ICG_N = RY_N \oplus IDG_N$ and $ICB_N = RZ_N \oplus IDB_N$.
7. Combine ICR_N, ICG_N, ICB_N to form the intermediate cipher image.
8. Consider a secret key SK = [SK_1, SK_2, SK_3, SK_4]. Calculate initial conditions for equation (6) by using $x' = SK_1$, $y' = SK_2$, $k' = SK_3$, $h' = SK_4$ as follows in Eq. (8).

$$\begin{cases} k = 2 + e^{(h' + 10\sin(k') + k')mod\ 2\pi} x \\ h = 2 + e^{(h' + 10\sin(k'))mod\ 2\pi} \\ x = (x' + h\sin(y') + ky')mod\ 2\pi \\ y = (x' + h\sin(y'))mod\ 2\pi \end{cases} \tag{8}$$

9. With x, y, k, has initial conditions, generate x_{n+1}, y_{n+1} for 2N values.
10. Normalize and round the generated (x_{n+1}, y_{n+1}) values using the below formula

$$\begin{cases} x_{n+1} = ceil\left(\frac{x_{n+1} * N}{2\pi}\right) \\ \\ y_{n+1} = ceil\left(\frac{y_{n+1} * N}{2\pi}\right) \end{cases} \tag{9}$$

11. Convert the intermediate cipher image into an 8-bit array and flatten it into a 1D array of size 1xN.
12. Scramble the 1D array using the sequence created in step 8 to alter the positions in the list.
13. Reshape the bit array and convert it back to an image. This is our cipher image(C).

B. Decryption algorithm

The decryption process of the algorithm is backtracing the encryption scheme. The flowchart of decryption is given in Fig. 2. The steps are as follows.

1. With the secret key (SK), generate initial conditions (x, y, k, h) for the improved chirikov map using Eq. (8).
2. Using the initial conditions, create an array of size 2N for both x_{n+1}, y_{n+1} with the help of Eq. (6).
3. Normalize and round the generated (x_{n+1}, y_{n+1}) using Eq. (9) and using Eq. (7), create the inverse values of (x_{n+1}, y_{n+1}).
4. Convert the cipher image into an 8-bit array and flatten it into a 1D array of size 1xN. Descramble the 1D array using the normalized sequence and reshape the bit array back to the image. It is our intermediate decrypted image.
5. Extract the RGB planes from the intermediate decrypted image ($D_{w \times h \times d}$) and save them as DCR for the Red plane, DCG for the Green plane, and DCB for the Blue plane. Calculate the size of image N = h*w. Use initial values of parameters as x(0) = 0.2487, y(0) = 0.35,
6. z(0) = 0.10001, α = 3.79, β = 0.017 and γ = 0.0012.
7. Generate the logistic map for N values and store the values in X_N, Y_N, Z_N arrays from Eq. (2), (3), and (4) respectively.
8. Convert X_N, Y_N, Z_N into a range from 0 to 255 and store them as RX_N, RY_N, RZ_N. Reverse confusion can be performed by $DDR_N = RX_N \oplus DCR_N$, $DDG_N = RY_N \oplus DCG_N$, and $DDB_N = RZ_N \oplus DCB_N$.
9.
10. Reverse diffusion is performed by $DR_N = DDR_N * X_N^{-1}$, $DG_N = DDG_N * Y_N^{-1}$, and $DB_N = DDB_N * Z_N^{-1}$.
11. Combine DR_N, DG_N, DB_N into $D_{w \times h \times d}$, which gives the decrypted image the same as the plain-text image.

IV. RESULTS AND ANALYSIS

In this section, the security analysis of the proposed method is measured against a certain set of parameters. The results of these metrics are evaluated for all the images shown in Fig. 3. The execution of the algorithm is performed on a Dell i7 laptop with 16GB RAM using MATLAB. Lena, Baboon, and Airplane are the plaintext images considered for simulation and their respective encrypted images are also given in Fig. 3. Histograms for the images are given in Fig. 4.

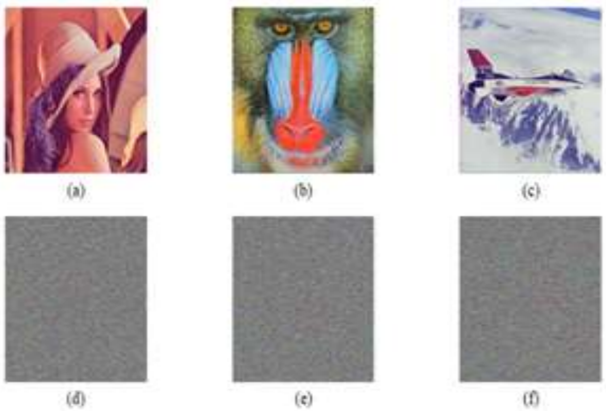

Fig. 3. (a) Lena (b) Baboon (c) Airplane (d) Cipher image of Lena (e) Cipher image of Baboon (f) Cipher image of Airplane

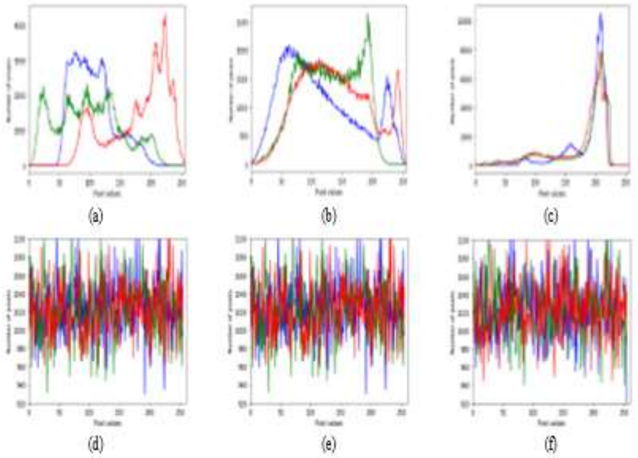

Fig. 4 Histogram of (a) Lena (b) Baboon (c) Airplane Histogram of Cipher image of (d) Lena (e) Baboon (f) Airplane

A. *Entropy*

Entropy is defined to express the level of uncertainty in the encrypted image. The entropy (H) of a symbol source(M) is given by Eq. 10

$$H(M) = -\sum_{i=0}^{255} P(M_i)\log_2 P(M_i) \qquad (10)$$

Where $P(M_i)$ denotes the probability of the symbol M_i, the ideal entropy value for an encrypted image is 8 [6]. It occurs when all the pixel values for an image have the same probability [6], [25]. The higher the entropy of the image, the more uniformity of distribution of pixel values of the image [6]. The entropy of images is shown in Table I.

TABLE I. ENTROPY ANALYSIS

Image	Plaintext image	Encrypted image
Lena	7.7502	7.9997
Baboon	7.7624	7.9998
Airplane	6.6639	7.9998

B. *Correlation Analysis*

Correlation analysis means finding the proportionality rate between adjoining pixels in vertical, horizontal, and diagonal directions. In general, a plaintext image may strongly correlate with its adjoint pixels, creating many security issues by disclosing such information. In contrast, the encrypted image will not have any relationship with its adjacent pixels. The given equation (Eq. 11) will calculate the correlation coefficient (CC).

$$CC(x,y) = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x\sigma_y} \qquad (11)$$

Where σ_x and σ_y denote the standard deviations of x and y, μ_x and μ_y represent the mean values of x and y, and E[x] is the representation of the mathematical expectation of x. The correlation distribution of pixels for Lena's image and the encrypted image of Lena in all directions are shown in Fig. 5, and correlation coefficients of all plaintext and encrypted images in all directions are accumulated in Table II.

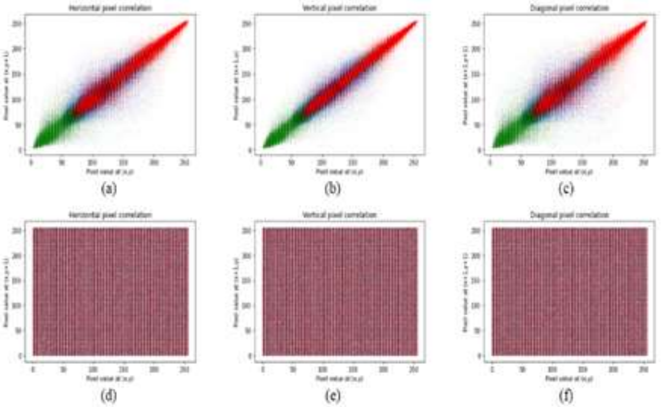

Fig. 5. Correlation of pixels of Lena (Fig. 3(a)) in (a) Horizontal (b) Vertical (c) Diagonal directions Correlation of pixels of Lena cipher image (Fig. 3(d)) in (d) Horizontal (e) Vertical (f) Diagonal directions

TABLE II. CORRELATION COEFFICIENTS

Image	Horizontal coefficient	Vertical coefficient	Diagonal coefficient
Fig. 3(a)	0.960527	0.976471	0.947842
Fig. 3(b)	0.898629	0.837285	0.809663
Fig. 3(c)	0.964799	0.953295	0.927166
Fig. 3(d)	-0.000252	-0.001740	0.000318
Fig. 3(e)	0.001598	-0.000244	0.000638
Fig. 3(f)	-0.000419	0.001608	0.001088

C. *Differential Attacks*

Nowadays, the differential attack has become the most effective method for cryptanalysis. An attacker tries to relate plaintext and encrypted image by tracing the difference between them and rebuilding the information of plain images without a key using this method. The capacity of obstructing differential attack is tested by two methods, Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). These show the strength of the proposed encryption scheme. The absolute number of pixel change rate is given by NPCR, and the change of colour intensities is given by UACI. NPCR is calculated by Eq. 12 and UACI by Eq. 13. The ideal value of NPCR is 99.61% and UACI is 33.46% [6]. Their values are shown in Table III.

$$N(C_1, C_2) = \sum_{ij} \frac{D(i,\ j)}{m\ x\ n}\ x\ 100\% \qquad (12)$$

$$U(C_1, C_2) = \frac{1}{m\ x\ n}\sum_{ij} \frac{C_1(i,\ j) - C_2(i,\ j)}{255}\ x\ 100\% \qquad (13)$$

$$\text{where D (i, j)} = \begin{cases} 0\ if\ C_1(i,\ j)\ \neq C_2(i,\ j) \\ 1\ if\ C_1(i,\ j)\ = C_2(i,\ j) \end{cases} \qquad (14)$$

Where C_1 and C_2 are two encrypted images acquired by implementing the proposed encryption algorithm on two plaintext images with the only difference of 1-bit and using the same key for both images, $m\ x\ n$ is the size of the image.

TABLE III. NPCR AND UACI VALUES

Parameter	Lena	Baboon	Airplane
NPCR	99.65%	99.63%	99.64%
UACI	33.43%	33.41%	32.42%

D. Key Space

The size of key space is an essential factor in security. It is given as the total number of various keys that can be produced for encryption. Key space must be huge enough to sustain brute-force attacks. In an ideal cryptosystem, the key space must be at least 2^{100} to provide high security [4]. The usage of a 3D chaotic map that is non-linear provides more security than others. Key space is given by a total number of initial parameters and values considered for encryption. The initial conditions used for the sequence generation in the 3D logistic map are $\alpha, \beta, \gamma, x_1, y_1, z_1$, and the improved chirikov map SK_1, SK_2, SK_3, SK_4 are the secret key values used for creating a sequence. Each parameter and secret key are considered with a precision of 10^{-14}, so the overall key space will be $(10^{14})^{10}$ i.e., 10^{140}, which is vast enough to resist any exhaustive attacks [6].

E. Key Sensitivity

Key sensitivity is an essential component of the security analysis of image encryption schemes. The decryption of the encrypted image is performed multiple times by making acute modifications to one of the keys used in the procedure each time to check the sensitivity [4]. Here in our test, the initial value of x is incremented in the improved chirikov map by 10^{-14}, decremented the initial value of β in the 3D logistic map by 10^{-14}, and kept the remaining parameters constant. After decryption with these wrong keys, the obtained decrypted images are shown below in Fig. 6. By this result, it can be seen that the scheme is highly sensitive to minor changes in initial values.

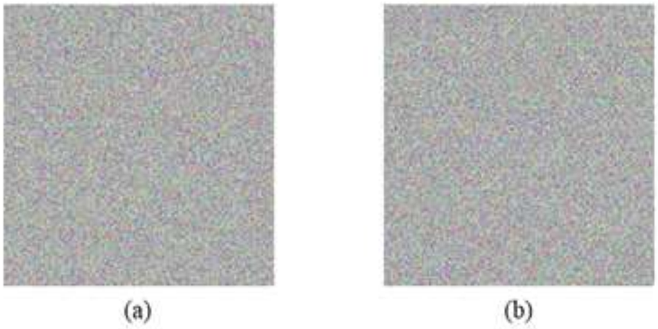

Fig. 6. Decrypted images of Lena with key (a)Logistic map $\beta = 0.017 - 10^{-14}$ (b) Chirikov map $x = x + 10^{-14}$

F. MSE and PSNR

The differentiation between the original image and cipher image can be measured by Mean Square Error (MSE) and Peak-Signal to Noise-Ratio (PSNR). MSE value between the two images considered should be high such that the images are completely distinct from each other and calculated by Eq. (15). The measure of the amount of distortion of the original image after the encryption scheme can be evaluated by PSNR [26], [27]. A PSNR value of less than ten will be framed as a good cryptosystem and calculated using Eq. (16). The values are shown in Table IV.

$$MSE = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|P1(i,j)-P2(i,j)|^2}{m\times n} \tag{15}$$

$$PSNR = 10 \times log_{10}(\frac{255^2}{MSE}) \tag{16}$$

TABLE IV. MSE AND PSNR VALUES

Parameter	Lena	Baboon	Airplane
MSE	8.9330e+03	8.6000e+03	1.0344e+04
PSNR (dB)	8.6208	8.7858	7.9839

G. Structural Similarity Index (SSIM)

The structural similarity (SSIM) index can show how similar are the two pictures. It lies in the range of [-1,1]. When the SSIM equals 1, both images are entirely identical. It is determined by the quality of the object structure in the reflection scene, which relies only on the picture's compositional angle and irrespective of brightness and contrast. Brightness, contrast, and the composition of the images make up the value of SSIM [28]. Mean values are used to gauge brightness, standard deviation is used to gauge contrast, and covariance is used to gauge structural similarity. For the evaluation purpose of SSIM, the relation is given by Eq. (17). SSIM values are shown in Table V.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_1)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \tag{17}$$

TABLE V. SSIM VALUES

Parameter	Lena	Baboon	Airplane
SSIM	0.0093	0.0090	0.0088

H. Robustness Analysis

1) Occlusion Attack

The robustness analysis of encrypted images against occlusion attack is performed with different percentages of an encrypted image being cropped (10%, 25%, 50% & 75%), and their respective decrypted images are displayed in Fig. 7. Occlusion may occur when the data gets lost while its transmission process happens. PSNR values evaluated between the original and decrypted images are shown below in Table VI. With the increase in cropped portion, PSNR value decreases. Even after some portion of the cipher image is cut out, the

The original image is roughly perceptible after recovering from the decryption procedure [29].

TABLE VI. OCCLUSION ATTACK PSNR VALUES

Parameter	**Fig. 7(f)**	**Fig. 7(g)**	**Fig. 7(h)**	**Fig. 7(i)**	**Fig. 7(j)**
PSNR (dB)	17.3593	14.0242	11.2582	9.7019	11.2491

2) Noise Attacks

On the other hand, this analysis is also successfully implemented against noise attacks like salt & pepper noise. In this attack, we check whether the recovered image is retrieved correctly or not after adding noise to cipher images in various proportions. The results are presented below in Fig. 8.

V. COMPARISON WITH STATE-OF-THE-ART METHODS

The performance of the proposed scheme is compared with state-of-the-art techniques. Lena image is considered (Fig. 3(a)) to compare correlation coefficients, entropy, NPCR, UACI, MSE, PSNR, and SSIM with relative methods. The values are listed in Table VII. From the results, one can say the proposed scheme is a compatible encryption method compared with various state-of-the-art methods.

VI. CONCLUSION

This paper demonstrates a novel image encryption scheme based on a 3D logistic map and an improved chirikov map. The encryption and decryption methods are clearly explained, and the security analysis has been performed. The 3D logistic map and improved chirikov map are utilized to modify pixel values and scramble pixel positions. The maps depend on the initial parameters and values, without which it is impossible to decrypt the cipher image due to the ample key space. The algorithm is susceptible to an acute change in the initial values and key parameters. Analysis results show that the proposed algorithm resists statistical attacks, brute-force attacks, noise attacks, and differential attacks. Comparison with the state-of-art methods shows that the scheme is highly secure and faster. The proposed work can be further extended to multidimensional chaotic maps, and other compression methods can be included in the process.

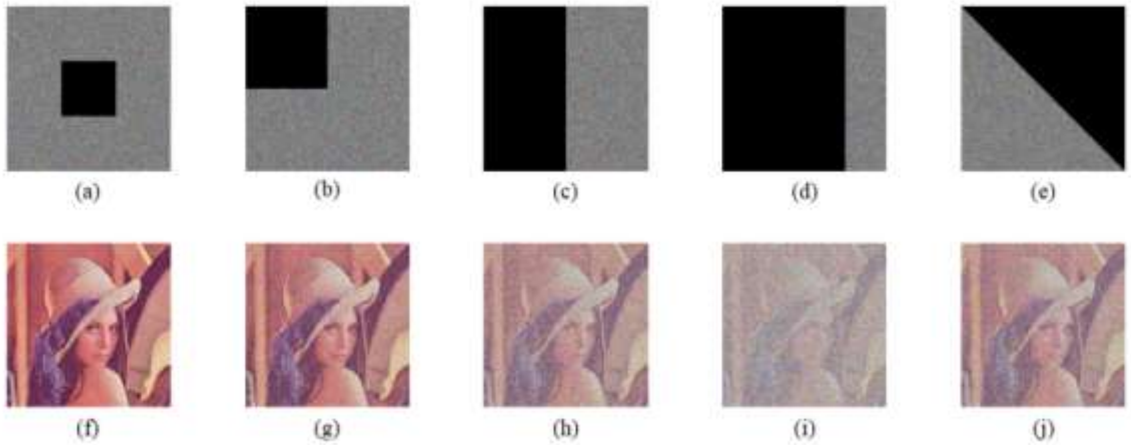

Fig. 7. Occlusion attack performed on cipher image of Lena (Fig. 3(d)) at different levels (a) 10% (b) 25% (c) 50% (d) 75% (e) 50% diagonally (f) Decrypted image of (a). (g) Decrypted image of (b). (h) Decrypted image of (c). (i) Decrypted image of (d). (j) Decrypted image of (e)

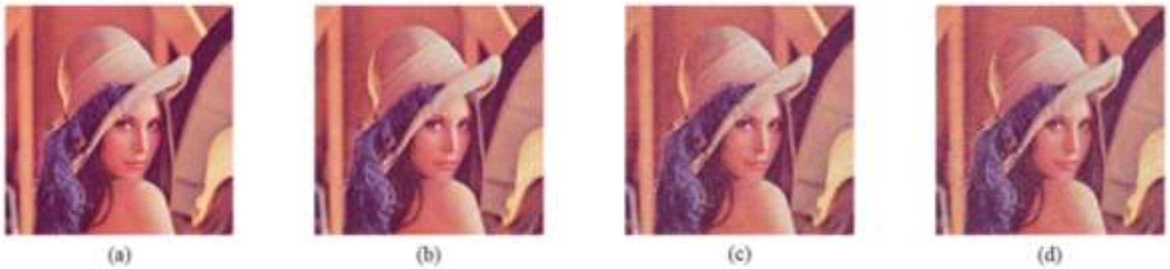

Fig. 8. Decrypted images of Lena with "Salt and pepper" noise with (a) 2% (b) 5% (c) 10% (d) 12%

TABLE VII. COMPARATIVE ANALYSIS

Scheme	**Correlation Coefficients**			**Entropy**	**NPCR (%)**	**UACI (%)**	**MSE**	**PSNR (dB)**	**SSIM**
	Horizontal	***Vertical***	***Diagonal***						
Ref. [25]	0.0005	0.0017	−0.0025	7.9981	99.60	33.43	-	-	-
Ref. [26]	0.001	−0.011	−0.006	7.9993	99.62	33.46	1.12934e+04	7.6030	-
Ref. [28]	−0.0012	−0.0027	−0.0033	7.9983	99.62	33.41	-	8.6767	0.009765
Proposed	-0.000252	-0.00174	0.000318	7.9997	99.65	33.43	8.9330e+03	8.6208	0.0093

REFERENCES

[1] N. Zhou, S. Pan, S. Cheng, Z. Zhou, “Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing”, Opt. Laser Technol. 82 (2016) 121–133.

[2] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gu-tiérrez, O.A. Del Campo, “A RGB image encryption algorithm based on total plain image characteristics and chaos”, Signal Process. 109 (2015) 119–131.

[3] A. Belazi, A.A.A. El-Latif, S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos”, Signal Process. 128 (2016) 155–170.

[4] Y. Zhang, D. Xiao, “Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform”, J. Opt. Lasers Eng. 51 (4) (2013) 472–480.

[5] C. Fu, J.J. Chen, H. Zou, W.H. Meng, Y.F. Zhan, Y.W. Yu, “A chaos-based digital image encryption scheme with an improved diffusion strategy”, Opt. Express 20 (3) (2012) 2363–2378.

[6] 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 the security of multimedia component”, 2014 International Conference on Informatics, Electronics & Vision (ICIEV), 2014, pp. 1-6, DOI: 10.1109/ICIEV.2014.6850856.

[7] P. Preethi and G. Prakash, “Secure Fusion of Crypto-Stegano Based Scheme for Satellite Image Application”, 2021 Asian Conference on Innovation in Technology (ASIANCON), 2021, pp. 1-6, DOI: 10.1109/ASIANCON51346.2021.9544752.

[8] Mimoun Hamdi, Rhouma Rhouma, Safya Belghith, “A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map”, Signal Processing, Volume 131, 2017, 514-526, ISSN 0165-1684

[9] Manikantha Vallabhaneni, Bhaswitha Maddula, Sarada Jayan, Subramani R (2020) “Chaotic Hooke-Jeeves Algorithm using Cubic map with MATLAB code”, 2020 IEEE International Conference for Innovation in Technology (INOCON), 1 – 4, DOI:10.1109/INOCON50539.2020.9298244.

[10] Bhaswitha Maddula, Manikantha Vallabhaneni, Sarada Jayan and Subramani R “Chaotic Evolutionary Algorithm”, 2020 IEEE International Conference for Innovation in Technology (INOCON), 1 – 4, DOI: 10.1109/INOCON50539.2020.9298233.

[11] Ye, Guodong, and Xiaoling Huang. “An efficient symmetric image encryption algorithm based on an intertwining logistic map”. Neurocomputing 251 (2017): 45-53.

[12] El-Deen, A., E. El-Badawy, and S. Gobran. “Digital image encryption based on RSA algorithm”. J. Electron. Communication. Engineering 9, no. 1 (2014): 69-73.

[13] Alsaffar, D.M., Almutiri, A.S., Alqahtani, B., Alamri, R.M., Alqahtani, H.F., Alqahtani, N.N. and Ali, A.A., 2020, March. “Image encryption based on AES and RSA algorithms”. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[14] Li L., Abd El-Latif, A.A. and Niu, X., 2012. “Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret image”. Signal Processing, 92(4), pp.1069-1078.

[15] Gupta, K., Silakari, S., Gupta, R. and Khan, S.A., 2009, July. “An ethical way of image encryption using ECC”. In 2009 First International Conference on Computational Intelligence, Communication Systems and Networks pp. 342-345. IEEE.

[16] Karthigaikumar, P. and Rasheed, S., 2011. “Simulation of image encryption using AES algorithm”. IJCA special issue on “computational science-new dimensions & perspectives” NCCSE, pp.166-172.

[17] Zeghid, M., Machhout, M., Khriji, L., Baganne, A. and Tourki, R., 2007. “A modified AES based algorithm for image encryption”. International Journal of Computer and Information Engineering, 1(3), pp.745-750.

[18] V. Sharma, H. C. Agnihotri, and C. H. Patil, “An Image Encryption and Decryption Techniques Using Two Chaotic Schemes”, vol. 2, no. 2, pp. 313–316, 2014.

[19] A. Belazi, M. Khan, AAA. El-Latif, S. Belghith, “Efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption”, Nonlinear Dynamics, (2016) 1-25.

[20] Ye, G. and Huang, X., 2017. “An efficient symmetric image encryption algorithm based on an intertwining logistic map”. Neurocomputing, 251, pp.45-53.

[21] Jain, Kurunandan, Aravind Aji, and Prabhakar Krishnan. “Medical image encryption scheme using multiple chaotic maps”. Pattern Recognition Letters 152 (2021): 356-364.

[22] Suchithra, M., Sikha, O.K. (2015). “”A Novel Image Encryption Scheme Using an Irrevocable Multimodal Biometric Key. In: Abawajy, J., Mukherjea, S., Thampi, S., Ruiz-Martínez, A. (eds) Security in Computing and Communications. SSCC. Communications in Computer and Information Science, vol 536 2015s. Springer, Cham. DOI: 10.1007/978-3-319-22915-7_25

[23] Li, Chunhu, Guangchun Luo, and Chunbao Li. “An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map”. Int. J. Netw. Secur. 21, no. 1 (2019): 22-29.

[24] Chen, Hang, Camel Tanougast, Zhengjun Liu, Walter Blondel, and Boya Hao. “Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform”. Optics and Lasers in Engineering 107 (2018): 62-70.

[25] Askar, Sameh S., et al. “An algorithm of image encryption using logistic and two-dimensional chaotic economic maps”. Entropy 21.1 (2019): 44.

[26] Heucheun Yepdia, L.M., Tiedeu, A. and Kom, G., 2021. “A robust and fast image encryption scheme based on a mixing technique”. Security and Communication Networks, 2021.

[27] B. Murugadoss, S. N. R. Karna, J. S. Kode and R. Subramani, “Blind Digital Image Watermarking using Henon Chaotic Map and Elliptic Curve Cryptography in Discrete Wavelets with Singular Value Decomposition”, 2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA), 2021, pp. 203-208, DOI: 10.1109/IRIA53009.2021.9588744.

[28] Liu, C. and Ding, Q., 2020. “A color image encryption scheme based on a novel 3d chaotic mapping”. Complexity, 2020.

[29] Chen, X., Gong, M., Gan, Z. et al. “CIE-LSCP: color image encryption scheme based on the lifting scheme and cross-component permutation”. Complex Intell. Syst. (2022).