A Novel Three-Key Mixing Text Encryption Based on A New 3-D Chaotic System

Kriti Suneja*1, Arpit Garg*2, Agam Sharma*3, Arpit Yash*4
Department of Electronics and Communication Engineering,
Delhi Technological University
Delhi, India
1suneja212@gmail.com, 2arpit1722@gmail.com, 3michaelsharma.tech@gmail.com,
4unofficialyash69@gmail.com

***Abstract*— In today's data centric world, data security in communication has become an inevitable need of the hour. In this research paper, we present a new three-dimensional chaotic system and a three-key mixing algorithm for text data encryption along with its implementation. The distinctive chaotic behaviour of the suggested new chaotic system is validated by its Lyapunov exponents and Kaplan-Yorke fractal dimensions. Additionally, we did the electronic circuit implementation in the LT Spice simulation which also confirms the theoretical model of the suggested new chaotic system. In addition, we also implemented a three-key mixing algorithm which uses a three-dimensional chaotic map to generate three cryptographic keys, on which XOR operation is performed to generate the final key sequence. The experimental result shows that the encryption algorithm is highly dependent on the initial conditions and is able to curb the eavesdropping capability of possible attacks, such as brute-force attacks.**

***Keywords*—** *Chaotic system, Kaplan yorke fractal, Lyapunov exponents, three-key mixing, LT Spice, Histogram*

I. The Introduction

Chaos theory is a branch of mathematical field of study that focuses on the seemingly random but deterministic nature of non-linear dynamic systems [1]. Some areas where chaos theory is widely used are mathematics, geology, microbiology, biology, computer science, engineering, finance, meteorology, politics, population dynamics, and robotics.

Chaos theory in data cryptography has found many applications due to high dependence on initial conditions.[2] The majority of recent research on chaotic encryption has been applied to the image and video encryption spaces, using techniques like the one described in [3], leaving the text encryption space largely unexplored. Additionally, the most popular chaotic maps for text encryption, like in [4], are the logistic map and logistic map modifications. The logistic map has certain limitations, such as sensitivity to single-valued initial conditions and a lack of physical interpretation, that contrast with the richer spatial dynamics inherent in 3D chaotic systems, making it less suited for text encryption algorithms.

In this paper, a text encryption algorithm based on utilising the three-key mixing of the 3D chaotic map for the key sequence generator is introduced. The proposed new chaotic system has rotational symmetry along the x-axis. The numeric performance of chaotic attractor is confirmed by its Lyapunov exponents, phase portrait, and Kaplan-Yorke fractal dimensions.

Additionally, the new chaotic attractor is implemented onto the LtSpice circuit simulator (Version 17.1.15), using op-amps as integrators and inverters, AD633 multipliers, resistors, and capacitors. Through simulation analysis, its stability and chaoticity have been confirmed, further enhancing its performance.

In the proposed encryption system, the three random sequences or three cryptographic keys generated by the 3D chaotic system, which are then mixed to form the final key sequence using the XOR operation to create a highly sensitive key.

This paper will also discuss the results of the encryption process, showing sensitive dependence on initial condition and histogram analysis of ciphertext, which provide us with statistical information. Our design overcomes the shortcomings of earlier encryption techniques to provide increased security and stability.

II. The Proposed New Chaotic System

As the chaotic system is characterised with their non-linear and dynamic nature, they must be represented with use of differential equations or set of differential equations. This research paper suggests a new three-dimensional chaotic system described using the three differential equations:

$$\begin{cases} \dot{x} = \sigma x - zy \\ \dot{y} = \rho(z - y) \\ \dot{z} = ay - bz + xy \end{cases} \tag{1}$$

where x, y, and z represent states of variable, and a, b, σ, and ρ are constant parameters of the new proposed chaotic system (1). It contains three nonlinear quadratic terms and showcases functional nonlinearity.

If the parameter values of the proposed system take the following values, the system is chaotic:

$$(a, b, \sigma, \rho) = (28, 1, -8/3, 10) \tag{2}$$

The initial conditions under which the system is chaotic are:

$$X(0) = (x_0,\ y_0, z_0) = (0.2, 0.2, 0.2) \tag{3}$$

When the parameter values and the initial conditions are taken as in equation (2) and equation (3). The Lyapunov exponent which measures the degree of divergence and convergence of the nearby trajectories in the dynamic system are calculated using the methods and algorithm as described by Sandri [5] and used to validate the chaotic behaviour of the new proposed chaotic system (1) through time as:

$$(L_1, L_2, L_3) = (0.910363, -0.003606, -14.573321) \tag{4}$$

Since the spectrum of all three Lyapunov exponents value (4) of the new proposed chaotic system (1) has a positive, a negative and a close to zero value, it follows that the new proposed chaotic system (1) is chaotic.

Also, as the sum of all the Lyapunov exponents value of the proposed chaotic system (1) is found as:

$$L_1 + L_2 + L_3 = -13.666564 < 0 \qquad (5)$$

As the sum of all the Lyapunov exponents value is negative, as shown in (5), it is a dissipative (stable) chaotic system as all its trajectories are eventually confined to a bounded region.

Equilibrium points are the points of differential equation where the rate of change of variable is zero which often define the long-term behaviour of the system. If the equilibrium points are stable, means the phase space will be approaching the equilibrium point.

The equilibrium points are calculated by solving the equations (each derivative) of the new proposed chaotic system (1) equal to zero, i.e., by solving the equations:

$$\begin{cases} \sigma x - zy = 0 \\ \rho(z - y) = 0 \\ ay - bz + xy = 0 \end{cases} \qquad (6)$$

Additionally, the equilibrium points and corresponding eigenvalues of the Jacobian matrix are determined:

TABLE I. EQUILIBRIUM POINTS AND THEIR EIGENVALUES

Equilibrium Point	***Eigenvalues***	***Nature***
O (0,0,0)	*11.8277, -22.8277, -2.6667*	*Saddle point of index 1*
E_1(27,8.374,8.374)	*-13.8155, 0.0745 ± 10.0751i*	*Saddle point of index 2*
E_2(27,-8.374,-8.374)	*-13.8155, 0.0745 ± 10.0751i*	*Saddle point of index 2*

The Kaplan-Yorke fractal dimension of the suggested new chaotic system (1) is calculated as:

$$D_{KY} = 2 + \frac{L_1 + L_2}{|L_3|} = 2.062220 \qquad (7)$$

It quantifies the chaoticity or the chaotic behaviour and the complex behaviour of the new suggested chaotic system (1).

The new chaotic system (1) has a special property that it has rotational symmetry across the x-axis and is in line equilibrium which is invariant under the change of coordinates as follows:

$$(x,\ y,\ z) \to (x, -y, -z) \qquad (8)$$

This chaotic system presents distinctive chaotic behaviour, validated through Lyapunov exponents, Kaplan-Yorke fractal dimension, Equilibrium points, dissipative nature and rotational symmetry across the x-axis. The 3-D phase portraits of the new chaotic system (1) are shown by Figure 1.

III. CIRCUIT REALISATION OF THE NEW PROPOSED CHAOTIC SYSTEM

In this section, the suggested chaotic system electronic circuit is realised and implemented using LT Spice Simulation (Version 17.1.15). The schematic model of the circuit as shown in Figure 3 are simulated in LT Spice Circuit Simulation (Version 17.1.15).

For circuit schematic accomplishment, the state variables need to be rescaled of the new suggested chaotic system (1) as follows:

$$X = 10x\,, Y = 10y\,, Z = 10z \qquad (9)$$

Now the equation in the new coordinates (X, Y, Z) after rescaling as in (9), would be deduced to:

$$\begin{cases} \dot{X} = \sigma X - \frac{1}{10} ZY \\ \dot{Y} = \rho(Z - Y) \\ \dot{Z} = aY - bZ + \frac{1}{10} XY \end{cases} \qquad (10)$$

The circuit realization and translation of the proposed system is built by using an operational amplifier LT1057A as integrators and inverters used to represent the differential equation. Also, AD633 multipliers have been used to carry out the product of two signals.

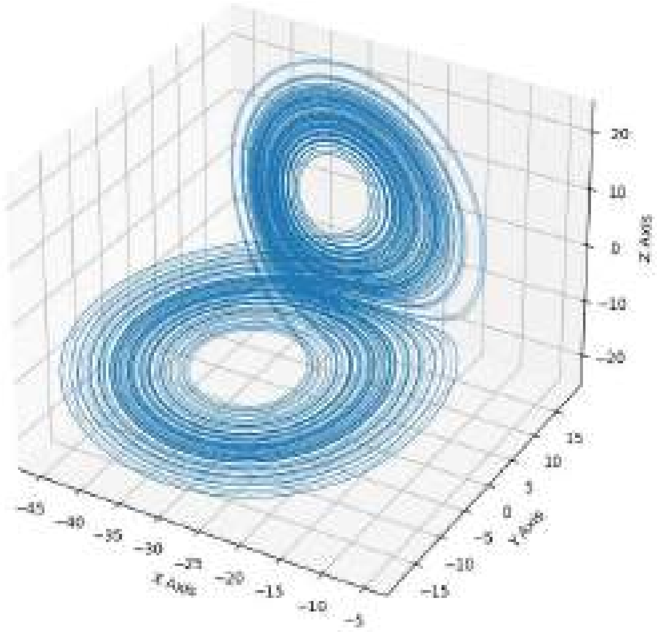


Fig. 1. 3D phase portraits of the proposed chaotic system (1) with parameter values X_0 = (0.2, 0.2, 0.2) and (a, b, σ, ρ) = (28, 1, -8/3, 10)

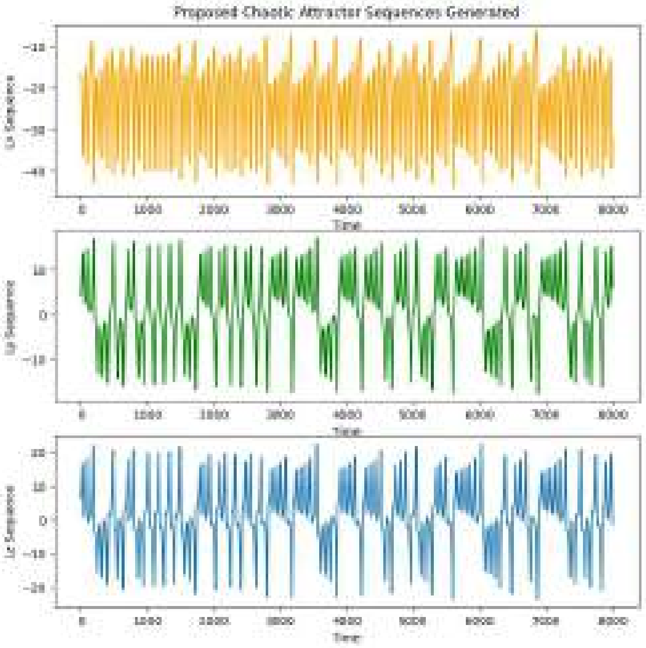


Fig. 2. Iteration of three sequences L_x, L_y *and* L_z with parameter values X_0 = (0.2, 0.2, 0.2) and (a, b, σ, ρ) = (28, 1, -8/3,10)

In the designed circuit, by applying Kirchoff's laws the non-linear equations are of the form:

$$\begin{cases} \dot{X} = -\frac{1}{C_1R_1}X - \frac{1}{10C_1R_2}ZY \\ \dot{Y} = \frac{1}{C_2R_3}Z - \frac{1}{C_2R_4}Y \\ \dot{Z} = \frac{1}{C_3R_5}Y - \frac{1}{C_3R_6}Z + \frac{1}{10C_3R_7}XY \end{cases} \qquad (11)$$

where X, Y, and Z are voltages, and the values of resistance and capacitance have been chosen to meet the values of given coefficients.

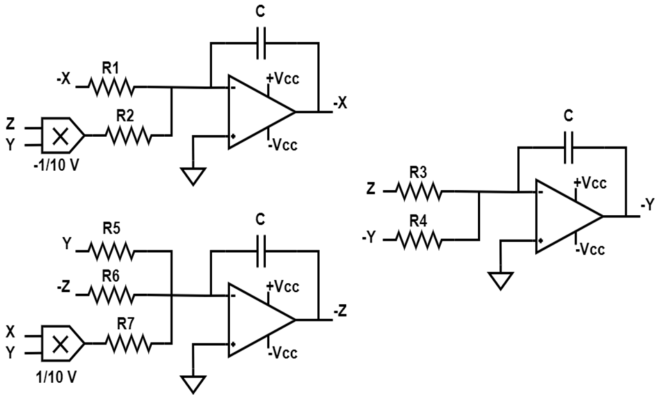


Fig. 3. Circuit Realisation of the new chaotic system(1)

The values of selected circuit components will be as follows:

C = 1nF , R$_1$ = 375$k\Omega$, R$_2$ = R$_3$ = R$_4$ = R$_7$ = 100kΩ, R$_5$ = 35.71kΩ, R$_6$ = 1MΩ, R$_7$ = 100kΩ

The biasing supplied to all these devices are ±9 Volts $(Vcc = 9V, -Vcc = -9V)$

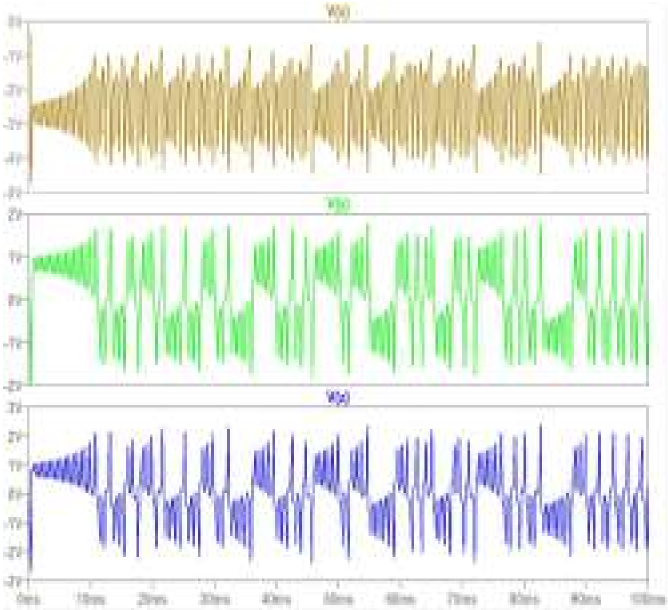


Fig. 4. LT Spice simulation result

The comparison between the theoretical model numerical results (Figure 2) and LTSpice simulation results (Figure 4) shows good qualitative agreement and the feasibility of the suggestyed chaotic system.

IV. Text Encryption

In this section, a novel three-key mixing text encryption algorithm using the proposed new 3D chaotic system is applied to defend against statistical attacks, brute force attacks, and differential attacks. The algorithm is based on three key mixings to form a single key for encryption. The flow chart of the text encryption system is shown in Figure 6.

A. The Proposed Cryptosystem

1) Key Generation

The initial values x$_0$, y$_0$, and z$_0$ and parameter values σ, ρ, a, and b of the 3D chaotic system are given. Then the suggested 3D chaotic system represented by states x, y and z will generate three pseudo-random sequences are generated which are denoted by Lx, Ly, and Lz sequences, accordingly.

The three sequences Lx, Ly, and Lz are pre-processed according to equation (12) into Lx', Ly', and Lz' sequences. While preprocessing, the sequences are multiplied with initial values to increase the randomness and dependence on the initial values in the desired range of (0,255) to be used for text encryption.

$$L_x' = mod(floor(10^{15} \times L_x \times x_0),256)$$
$$L_y' = mod(floor(10^{15} \times L_y \times y_0),256)$$
$$L_z' = mod(floor(10^{15} \times L_z \times z_0),256) \qquad (12)$$

The final keystream is generated by mixing three sequences using the XOR operation using equation (13). The sample key sequence generated is shown in Figure 5.

$$KS = L_x' \oplus L_y' \oplus L_z' \qquad (13)$$

2) The Proposed Encryption Algorithm

The steps of the given proposed algorithm are as follows:

- Initially, transform plain text P of length L into its ASCII value.
- The initial values x$_0$, y$_0$, and z$_0$ and parameter values a, b, σ, and ρ of the 3D chaotic system are set initially.
- After traversing the 3D chaotic system, and getting rid of some initial values to curb the transient effect. The three pseudo-random sequences Lx, Ly, and Lz representing states x, y and z respectively of length L are obtained.
- The sequence Lx, Ly, and Lz can be preprocessed according to equation (12) to bring it into the desired range.
- The final key sequence is generated by mixing three sequences using the XOR operation according to equation (13).
- Cipher Text is generated after using the XOR operation of the text with key Sequence
- Convert Sequence back to the string, i.e. the Encrypted Text C

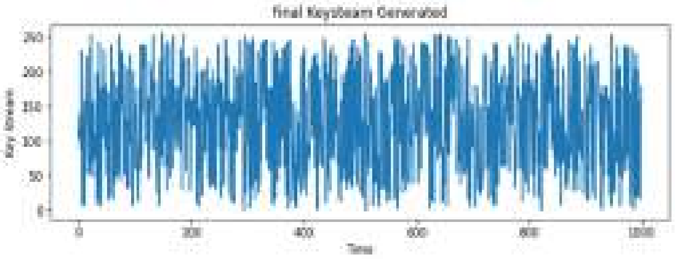


Fig. 5. Final Key Sequence generated after mixing

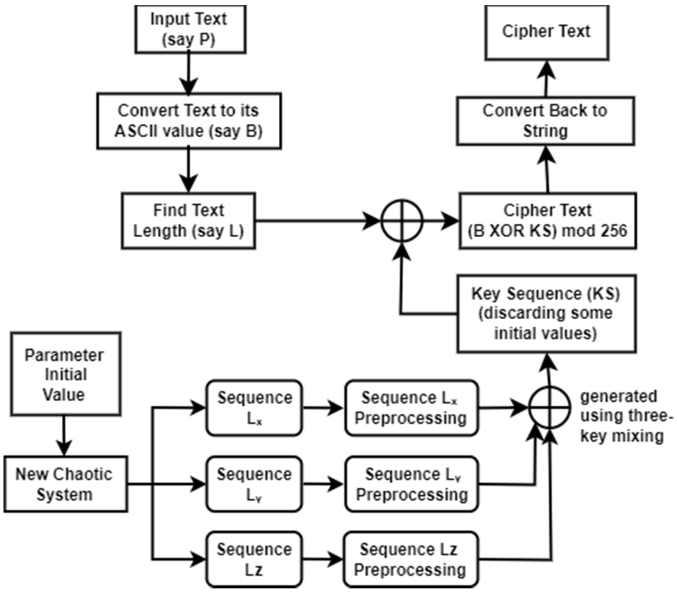

Input Text (say P)
Convert Text to its ASCII value (say B)
Find Text Length (say L)
Cipher Text
Convert Back to String
Cipher Text (B XOR KS) mod 256
Key Sequence (KS) (discarding some initial values)
Parameter Initial Value
New Chaotic System
Sequence Lx
Sequence Ly
Sequence Lz
Sequence Lx Preprocessing
Sequence Ly Preprocessing
Sequence Lz Preprocessing
generated using three-key mixing

Fig. 6. Encryption Algorithm

V. Experimental Results and Analysis

Three different test texts with different lengths (T1, T2 and T3) as shown in Table II are taken for testing the performance of the proposed algorithm. Given the initial values (x_0, y_0, z_0) = (0.2, 0.2, 0.2) and parameter values (a, b, σ, ρ) = (28, 1, -8/3, 10). The security measures are carried out based on the aspects of the histogram, and key dependence analysis.

TABLE II. Plaintext Examples

Plaintext	Input
T1	Electronics and Communication Engineering
T2	The Delhi Technological University (DTU) is a renowned technical institution in India, known for its commitment to excellence in engineering and technology education.
T3	It is a .txt file that consists of 13 paragraphs with total characters (length) is 4753

A. Encryption and Decryption Results

After implementing the proposed encryption algorithm, the following cipher text is found from input text T1 and T2.

TABLE III. Ciphertext of P1 and P2

<table>
<tr><th>Plaintext</th><th>Ciphertext</th></tr>
<tr><td>CT1</td><td>Ç\x0b\x82êö\x11K\x1aÕ¨·ðE7¸\x14û\x8b?î-æ\x94À\x9c:D\r1V>|\x7fëò\x80a\x97áwG</td></tr>
<tr><td>CT2</td><td>Ö\x0f\x82©Æ\x06H\x1cÕë\x90µG1²[Ô\x8b5ê;é\x91\x83¨D\x14:\x04\x08{lû¼Í@±Ý0\x00÷f4Ã9CÝëò¿Å¦¿'gP\x12ôRíÏr|¼L\x1cy\x9a\x14{\x03\x1eÕ\x1b?ì®Å¸C\x9cSÞÑqiø\nb\x19£+\x94ËÄî\x0f\x16=&®Üºè)\ni\x95.\x0f\x878hÂ\xad&©:Ù©44«³\x90\x9bÿ\x98»\x18U\x01ëHT@¢\x0emw·\x17n¾^2&ÌQ\x8e\x05Ã\x8c1Ëé²\x0f\x97F4)\x8e,Ý</td></tr>
</table>

The following decrypted text is found in CT1 and CT2 when the decryption algorithm with different secret initial and parameter values is shown in Table IV, V, and VI. We can see the sensitive dependence on the initial condition, as even with a slight change, the text cannot be decrypted correctly.

TABLE IV. Decrypted Text when secret initial values X'$_0$= Y'$_0$= Z'$_0$= 0.2 and parameter values a = 28, b = 1, σ = -8/3 and □ =10

Plaintext	Ciphertext
CT1	Electronics and Communication Engineering
CT2	The Delhi Technological University (DTU) is a renowned technical institution in India, known for its commitment to excellence in engineering and technology education.

TABLE V. Decrypted Text when secret initial values X'$_0$= Y'$_0$= Z'$_0$= 0.2 and parameter values a = 28, b = 1, σ = -8/3 and □ =10.001

Plaintext	Ciphertext
CT1	q\x83?½\x82\x07ÝÙý¼\x90\x1bul\x1f\x13xRð¼0\x12\x7fÒ\x1a\x95â
CT2	\x96Ú\x83h;êgEIÀáÙuj\x15\\WRú¸&\x1dz\x91.\x8fâ\x04uG\x00ÌÛ\x9d»9\x0eNøÅù\x14GénÊ~\x19éÍ\x8c\x16!4´gÔWj\x80\x0bè\x92@a\x95\x0bÆ»Yý\x1a\x8b$\x94ºt@Ò\x01ÚJ©\x8dù½\x99\x93¤å\x04çe\x97Uä\x1e\x8da\x19ï\x075p,ú>eê8áÈj?áw\x98+¥ïÄÆ\x12yD^½dg¨!\xa0\x87\xa0¿Ã®N-ÈÞqÛáäp@ÅíÃÀ:`\x95ÿ¾Ô¿>ÂOet

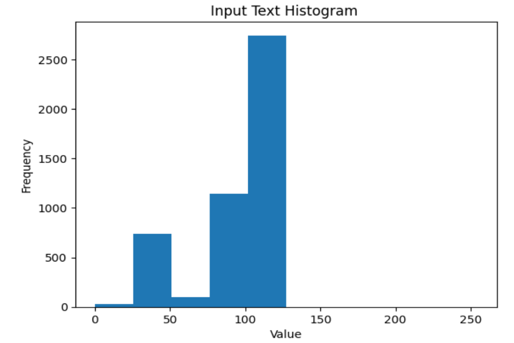
TABLE VI. Decrypted Text when secret initial values X'$_0$= 0.2001, Y'$_0$= Z'$_0$= 0.2 and parameter values a=28, b=1,σ=-8/3 and □=10

Plaintext	Ciphertext
CT1	6\x0b/\x0bjÒ<\x86÷úH®%ñÒôN-\x10oâý¿W¡à¾
CT2	ÑR\x93ÞÓ?\x86\x1aC\x869l%÷Ø»a-\x1akôòº\x14\x95ú¾·\xad".÷\x16\x81Èh{n\x9dgHÈ\x8fú\x10:Ò\x94\x88\x16.Æ\x14iÈ\x84\x03\x1b`ú\x8e\x18\r\x10\x87³/\x1b¡\x9a\x94_\x06ø\x10¢e×UpNï\x9bÅ·æÄwy¬_\x91o;zâËbuk\x8f\x8b\x06\x82\x8a\x14fq\x01Ý<\x85\x16Ü\x19Q^\x12\x9d^8I\x9e;Êå\x15iå\t\x9b.Eô2\x15$\x0f\x9aÓÜBÓã\x0bö>«@\x8e¤\x02¢¶!6AÄ(À\x15\x0e\x96

B. Histogram Analysis

A histogram is used to describe the data distribution. It showcases the ability of encryption algorithms to protect against statistical attacks. The histogram of plain text has some statistical information hidden, while a cipher text should contain show minimal statistical information. Plaintext T3 has been tested, and histogram analysis can be seen in Table VII.

TABLE VII. Plaintext and Ciphertext Histogram

Text	Histogram
T3	

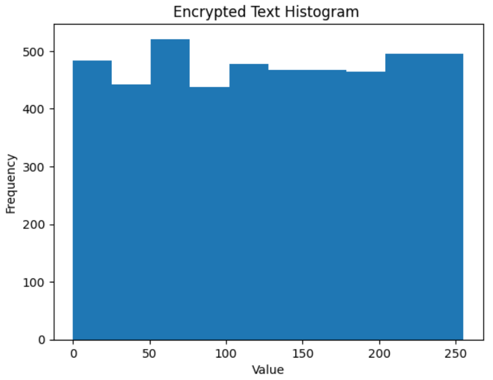
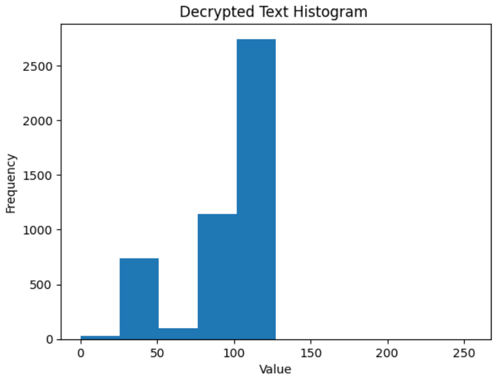
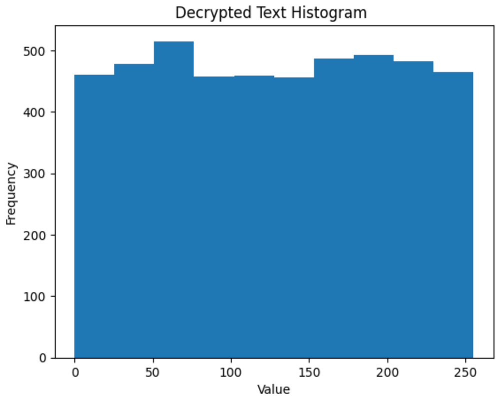
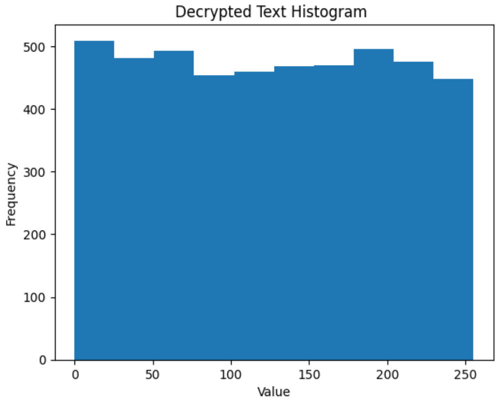
Text	Histogram
CT3	

TABLE VIII. DECRYPTED TEXT HISTOGRAM

Secret Key	Histogram
X_0= 0.2, Y_0= 0.2, Z_0= 0.2 A = 28, B = 1, σ = -8/3 ⍰ = 10	
X_0= 0.2, Y_0= 0.2, Z_0= 0.2, A = 28, B = 1, σ = -8/3, ⍰ = 10.001	
X_0= 0.2001, Y_0= 0.2, Z_0= 0.2 A = 28, B = 1, σ = -8/3 ⍰ = 10	

Even with a slight change, the text cannot be decrypted correctly as our algorithm is sensitively dependent on initial condition, as shown in histogram analysis of three different sets of keys in Table VIII.

VI. CONCLUSIONS AND FUTURE SCOPE

In this paper, a new 3-D chaotic system-based text encryption through two key components, a novel 3-D chaotic system and the implementation of three-key mixing algorithm, by using three cryptographic keys to generate the final key sequence, is proposed. The proposed new chaotic system chaotic behaviour is confirmed by its Lyapunov exponents and Kaplan-Yorke fractal dimensions. In addition, an electronic circuit implementation of the new chaotic system in the LT-Spice simulation also validates the theoretical model in the Python simulation and feasibility of the proposed chaotic system.

The text encryption algorithm involves a three-key mixing algorithm in which the three cryptographic keys generated by the new chaotic system are mixed using the XOR operation to generate the final key sequence. To increase sensitive dependence on initial conditions, initial values are multiplied with sequence while preprocessing. The experimental result shows that the ciphertext is uniformly distributed and extremely sensitive to initial conditions using the histogram analysis, showing that ciphertext is secured to brute force attacks and some other recognized plaintext attacks. As long as the secret key is equivalent to the encryption's secret key, then only the original text can be decrypted back. Based on the encryption and decryption results, the suggested method in this research is satisfied as a high-security encryption technique.

REFERENCES

[1] Biswas, H. R., Hasan, M. M., & Bala, S. K. (2018). Chaos theory and its applications in our real life. Barishal University Journal, 5(1&2), 123-140. ISSN 2411-247X.

[2] Zhang, H. and J.-x. Dong. "Chaos theory and its application in modern cryptography in Computer Application and System Modeling (ICCASM)", International Conference on, 2010.

[3] Sambas, A., Vaidyanathan, S., Zhang, X., Koyuncu, I., Bonny, T., Tuna, M., Alçin, M., Zhang, S., Sulaiman, I. M., Awwal, A. M., & Kumam, P. (2022). A Novel 3D Chaotic System With Line Equilibrium: Multistability, Integral Sliding Mode Control, Electronic Circuit, FPGA Implementation, and Its Image Encryption. IEEE Access, 10.1109/ACCESS.2022.3181424.

[4] Irsan, M. Y. T., & Antoro, S. C. (2019). Text Encryption Algorithm based on Chaotic Map. In The 3rd International Conference On Science. Journal of Physics: Conference Series, 1341(6), 062023. doi:10.1088/1742-6596/1341/6/062023.

[5] Sandri, M. (1996). Numerical calculation of Lyapunov exponents. Math. J., 6.