A Synergistic Approach for Enhancing Image Encryption by Implementing Double Random Permutation and Memristive Chaos

Ritu Sharma, Sunil Kumar

Abstract: ***The growing academic interest in the secure transmission of optical digital images has led to a surge in awareness of information security within photonics circumstances. This work presents a hybrid encryption strategy based on the memristor hyperchaotic system and a double random transform for pictures in the frequency and spatial domains. This study presents a robust and secure picture encryption technique that combines compressed sensing, double random phase encoding (DRPE), and Lorenz map. We also make double-random-phase masks using Lorenz maps, which enhance the unpredictability and key sensitivity, thereby improving the security of the encryption method. Experimental studies utilize a range of performance metrics, such as the PSNR, NPCR, MSE, and SSIM, to show the value of the suggested approach.***

Keywords: Image Encryption, Double Random Phase Encoding, Lorenz Maps, Compressed Sensing, Security, Robustness.

Abbreviations:
DRPE: Double Random Phase Encoding
TDES: Triple Data Encryption Standard
DES: Data Encryption Standard
AES: Advanced Encryption Standard
CSS: Compressed Sensing System
LASSO: Least Absolute Shrinkage and Selection Operator
DRT: Double Random Transformation
PSNR: Peak Signal-to-Noise Ratio
SSIM: Structural Similarity Index
NPCR: Normalized Partial Correlation Coefficient
MSE: Mean Squared Error
NPCR: Normalized Pixel Change Rate
SSIM: Structural Similarity Index

I. INTRODUCTION

A wide range of new information technologies are evolving quickly these days. As people enjoy the benefits of information technologies, hidden security issues become more apparent. In the big data world, the search for dependable and effective security methods is becoming increasingly important.

Manuscript received on 16 November 2024 | First Revised Manuscript received on 01 December 2024 | Second Revised Manuscript received on 17 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.
***Correspondence Author(s)**

Ritu Sharma*, Department of Computer Science and Information Technology, Central University of (Haryana), Mahendergar, India. Email ID: ritu.kaushik1384@gmail.com, ORCID ID: 0009-0008-0147-7202

Sunil Kumar, Assistant Professor, Department of Computer Science and Information Technology, Central University of (Haryana), Mahendergar, India. Email: drsunilk@cuh.ac.in

The safe transfer of digital photos has become a critical issue in the big data era and has attracted a lot of scholarly interest [1]. Safeguarding against theft or leakage and maintaining the confidentiality of these images during transmission has emerged as a major area of scientific interest [2]. On the other hand, cryptographic protection that makes use of conventional text encryption algorithms has a difficult time meeting real-time performance requirements [4]. This is because digital images have distinctive characteristics, including a high correlation between adjacent pixel points, a scattering distribution of critical information, and a high information redundancy [5]. High sensitivity to beginning circumstances and control parameters, outstanding pseudo-randomness, periodicity, and long-term Unpredictability of orbits are some of the traits that are associated with chaos [6]. Additionally, chaos itself has many characteristics that are associated with confusion, diffusion, and other properties that are typical of cryptography [7].

As a result, it is of the utmost importance examine the chaos theory-based image encryption approach within the framework of the era of big data [10].

This paper is broken up into several parts. The introduction and literature study is given in Section 1 [32]. The methods employed in the paper, such as DRPE, and compressed sensing, are defined in Section 2. The proposed paper contains a description of the proposed methodology given in Section 3. Concentrate on Section 4's numerical simulation and outcomes. And last section is the conclusion of the last paragraph [33].

II. LITERATURE STUDY

The huge breakthroughs that have been made in information technology and the Internet have had a major influence on every facet of our company, our industry, and our day-to-day lives. These technological breakthroughs have made it possible for us to generate huge amounts of data in our day-to-day lives at a lower cost and with greater convenience. Images have become the primary data type as a result of the pervasive adoption of mobile technologies over the past two decades, in addition to these advancements [13]. The confidentiality of images must be guaranteed and safeguarded against unauthorized access during the storage and sharing of them, as they contain highly sensitive data. The fact that this has occurred has attracted the attention of researchers, and it has also achieved a prominent place in the body of literature as picture encryption. A new dynamic and adaptive diffusion method is more flexible and more secure using numerical simulation and CNN is used to generate plaintext related that control plaintext attacks [9]. A new image encryption scheme is designed to reduce the security risk of cloud data [12].

In contrast to the encryption of text data, the encryption of visual data provides a few difficulty difficulties. With regard to practical applications, the initial size of picture data is substantially greater than that of text data. Because of this, the process of encrypting photos within a fair amount of time is made more difficult. In the second scenario, the image data contains extremely high correlations between adjacent pixels [14]. Through the use of statistical assaults, makes it possible for attackers to get access to the source photos. The encryption algorithm will be deemed useless if it is not adequately robust enough to handle information. Thus, the classical encryption algorithms, including Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple Data Encryption Standard (TDES), and Rivest-Shamir-Adleman algorithm (RSA), data encryption methods, which are often used to encrypt text data, are not suitable for use in the encryption of image data [15]. The deployment of various methods is required to encrypt image data.

Permutation, substitution, and diffusion are the three most common architectures employed by image encryption algorithms [16]. The permutation phase is intended to change the locations of the pixels in the picture without going through any changes to the values of those pixels [17]. Because of this, the correlation between pixels that are near to one another is significantly reduced. The statistical properties of image pixels are systematically altered during the substitution and diffusion stage [18]. To phrase it another way, it enables the changing of pixel values in a certain manner. The efficacy of encryption methods that solely use permutation is insufficient because they do not change the histogram of the pictures; rather, they change the locations of the pixels. This is the reason why these algorithms are not effective [19]. Permutation and diffusion should be implemented in conjunction in an effective encryption algorithm. Chaos-based encryption algorithms can fulfill the requirements of the diffusion and permutation phases of the encryption process. Chaos-based approaches have gained popularity in the field of image encryption due to their ability to provide a practical mechanism for both diffusion and confusion [9]. Chaos-based methodologies are exceedingly susceptible to initial circumstances. Additionally, the acquisition of random values, as opposed to periodic ones, has resulted in their pervasive application in the field of image encryption.

To augment the dynamic S boxes that were developed for pixel permutation, the Lorenz chaotic map was used with the intention of. In an additional investigation, the Chirikov chaotic map was implemented in conjunction with the two-dimensional Gingerbread man chaotic map [20] have proposed an additional hybrid system. In addition to the SHA512 hashing method, the approach is used in combination with the orthogonal matrix, the discrete Chirikov chaotic map, and the discrete cosine transform [31]. To reach high levels of computing efficiency and security, there is a considerable body of work that incorporates chaotic maps. The writings of Lyle and his colleagues provide a body of material that is both very detailed and comprehensive in terms of chaos-based cryptography (2022), Furthermore, these methods t are based on bitwise permutation [21], fractal sequencing matrix [22], piecewise merged map lattice [23].

A. Theoretical Review

i. *Double Random Phase Encoding (DRPE)*

Double random phase encoding is a typical technique for image encryption. The 4F principle of DRPE is depicted in Fig.1. DRPE, a prominent method for picture encryption and optical security applications, is based on the 4F principle [2]. DRPE is based on the encryption and decryption of pictures using two random phase masks and two Fourier transforms [3]. The 4F principle, which refers to the optical configuration utilized to implement DRPE, forms the basis of the encryption procedure. Two Fourier transforms, along with two lenses (F_1 and F_2), make up the four main parts of the 4F principle [24]. The optical arrangement may be summarised as follows on a sentence level: F_1 stands for the first Fourier transform. Once the input image has been multiplied by the first random phase mask, the spatial domain is next considered. After that, the Fourier spectrum of the masked image is generated by performing a Fourier transformation on the product using lens F_1.

Space-Free Propagation: Before reaching the second lens F_2 after the first Fourier process, light travels freely across a distance. Second Fourier Transform (F_2): Using lens F_2, the light from the first lens F_1 is once again Fourier transformed. The second random phase mask is applied in this step on the first step's Fourier spectrum.

Inverse Fourier Transform*:* Finally, the signal passes through an IFT to convert the modified Fourier spectrum back to the spatial domain, resulting in the encrypted image [16]. It is challenging to predict or reverse-engineer the two random phase masks used in the procedure without the proper decryption keys because they are produced using random integers or sequences [25].

A high degree of security is offered by the complexity of the encryption process, which is described here [2]. The encrypted image is subjected to the same 4F optical setup with the same random phase masks applied in reverse order during the decryption procedure [3]. If the appropriate decryption keys are used, it is possible to successfully reconstruct the initial picture by following the inverse route. DRPE's 4F principle ensures a high degree of security because of its complex optical operations and dependence on random phase masks, which are essential to both the encryption and decryption processes [29]. This is because random phase masks are essential to both processes [30]. As a result, DRPE [4] is a reliable and effective method for applications involving optical security and picture encryption. The encryption process is represented mathematically as follows:

Encryption: Create two random phase masks of the same size as the input image, P_1 and P_2. F signifies the Fourier transform to be applied to the input image. Multiply the random phase masks P_1 and P_2 elementwise by the Fourier transform F:

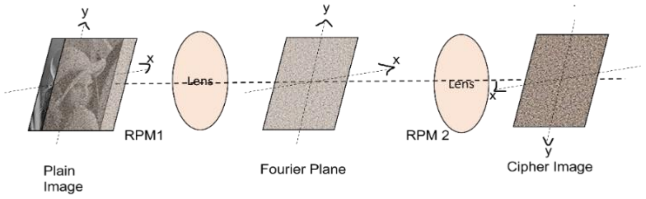
$$E = F * e^{(i * P_1)} * e^{(i * P_2)} \quad \dots \quad (1)$$

Where the fictitious unit i is used. To get the encrypted image C, apply the inverse Fourier transform to the input image E. The encrypted image C, designated as F_c, must undergo the Fourier transform in order to be decrypted.

Create the conjugate of P_1' and P_2', the random phase masks P_1 and P_2, respectively.

$D = F_c * e^{(-i*P1')} * e^{(-i*P2')}$ is the result of multiplying the Fourier transform F_c element-wise with the conjugates of the random phase masks [4].

The inverse Fourier transform on D can be used to acquire the decrypted image, known as D_{img}. The supplied image should preferably be an exact match to the decoded image D_{img} [5].



[Fig.1: Double Random Phase Encoding]

ii. *Compressed Sensing System (CSS)*

A signal processing method called CS enables the effective acquisition and reconstruction of sparse or compressible signals from a small number of observations [1].The CS framework can be mathematically represented as follows: Let's consider an original signal or image $x \in \mathbb{R}^n$, where n is the length or size of the signal[26]. We assume that x is sparse or compressible in some domain or basis.

Measurement Model: The compressed measurements, $y \in \mathbb{R}^m$, are obtained by linearly sampling the original signal x using a measurement matrix $\Phi \in \mathbb{R}^{(m \times n)}$, [8] where m < n. The following phrase may be used to describe the technique of measurement:

$$y = \Phi * x \quad \dots \quad (2)$$

In this case, the measurement matrix is Φ, and y is the compressed data. From these compressed values, the original signal x should be reconstructed.

Issue with Reconstruction: In compressed sensing, the reconstruction issue seeks to restore the original signal x from the compressed measurements [8]. This problem is intrinsically underdetermined since the number of measurements m is substantially less than the size of the signal [19]. It is possible to formulate the reconstruction problem as an optimization problem:

$$\min \left|\left|x\right|\right|_0 \rightarrow y = \Phi * x \quad \dots \quad (3)$$

where $\left|\left|x\right|\right|_0$ denotes the signal's l0-norm, or the number of non-zero elements. Finding the sparsest solution that fulfills the measurement equation $y = \Phi * x$ is the goal of the l0-norm optimization problem.

Relaxation to L₁-Norm: The l0-norm optimization problem is NP-hard and computationally infeasible for large-scale problems [8]. Therefore, practical CS algorithms relax the problem to an l1-norm optimization problem, which is convex and efficiently solvable [19]. The relaxed optimization problem becomes:

$$\min \left|\left|x\right|\right|_1 \rightarrow y = \Phi * x \quad \dots \quad (4)$$

This particular expression, denoted by the symbol $\left|\left|x\right|\right|_1$, is the l1-norm of the signal x, which is the total of the absolute values of its constituent parts. The l1-norm optimization problem promotes sparsity in the solution, encouraging many elements of x to become zero, leading to an approximate sparse solution [11]. To effectively solve the l1-norm optimization issue, a multitude of techniques, such as Basis Pursuit and Orthogonal Matching Pursuit (OMP), may be used, and LASSO (Least Absolute Shrinkage and Selection Operator), which can effectively reconstruct the original signal x from the compressed measurements y.

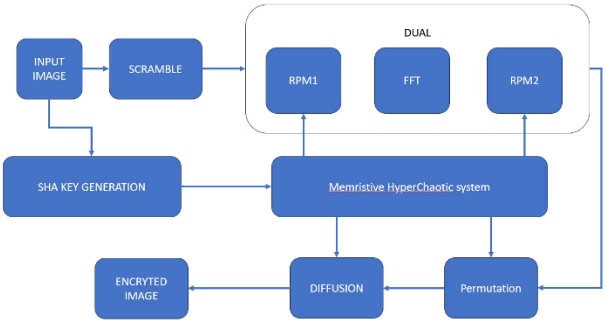
In the context of DRPE, Compressed Sensing is used to reduce the number of measurements required to represent the encrypted image, thereby reducing the data size and computational complexity during transmission and storage [20]. This is particularly advantageous when dealing with large images or videos, as it reduces the data bandwidth and storage requirements. The integration of Compressed Sensing with DRPE involves the following [15] steps.

Image Compression using Compressed Sensing: The original image is converted into a sparse representation utilizing Compressed Sensing methods before the DRPE encryption process is used. This entails utilizing a measurement matrix to get a compressed set of measurements (compressive measurements) of the image [18]. In the figure, these measurements are made at random or supposedly random sites. After that, the sparse representation of the image is put into the DRPE procedure. A high degree of security is provided by DRPE, which encrypts the picture by using two random phase masks and two Fourier transformations. This was described before. The encryption keys are used to generate the random phase masks [19]. Picture Decryption and Reconstruction: To acquire the encrypted Fourier spectrum during picture decryption, the same DRPE procedure is reversed using the appropriate decryption keys. The sparse representation of the encrypted image is then recreated using the inverse Fourier transform. Finally, using compressive measurements and compressed sensing methods, the original image is recreated from the sparse representation [6].

Compressed Sensing and Double Random Phase Encoding work together to increase the efficiency of encryption and decryption, resulting in smaller data files with higher levels of security. This integration is particularly useful in scenarios where both data efficiency and image security are essential, such as secure image transmission and storage in various applications, including optical security and secure communication systems [18].

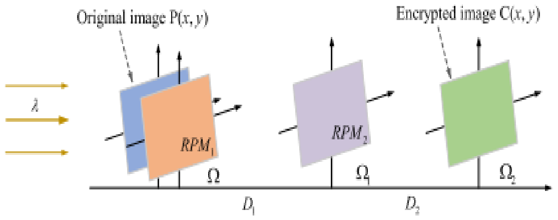
III. PROPOSED METHODOLOGY

This paper proposed a novel methodology for encrypting images by combining Double Random Transformation (DRT) with Memristive Chaos. DRT provides robust encryption capabilities by utilizing complex spatial and temporal transformations, albeit with high computational and operational complexities. On the other hand, Memristive Chaos leverages chaotic dynamics toachieve efficient encryption, primarily in the spatial domain. However, both methods exhibit vulnerabilities when used individually due to inherent algorithmic limitations. By integrating DRT and Memristive Chaos, this study aims to harness their complementary strengths, thereby enhancing overall encryption security and mitigating their respective weaknesses. The proposed methodology integrates sophisticated transformational and chaotic encryption techniques to achieve superior protection of sensitive image data against modern cryptographic attacks. The flow chart of the proposed scheme and Fig. 2(b) show the block diagram.



[Fig.2: Proposed Flow Diagram]

Here is a brief description of the DRPE encryption principle. This paper derives the DRPE for image encryption from Fresnel diffraction FD. Fig.1 depicts the encryption procedure, which involves placing the original digital image P (x, y) on the input plane Ω. Initially, it is exposed to perpendicular incident light (λ). RPM1 modulates P (x, y) in unit amplitude, which is close to the encryption input surface.



[Fig.3: Process Diagram for Double Random Phase Encryption]

Subsequently, it undergoes the complete encryption process involving applying the Fresnel diffraction transformation at distances D_1 and D_2, resulting in the encrypted image C (x, y) in the output plane Ω_2. RPM_1 is represented as $e^{[j^2\pi\phi(x,y)]}$, and RPM2 as $e^{[j^2\pi\phi(u,v)]}$.

$$\mathrm{C(x,y)} = \mathrm{fft}^{-1}\{\mathrm{fft}\{\mathrm{p(x,y)} \times e^{[j^2\pi\phi(x,y)]}\}e^{[j^2\pi\phi(u,v)]}\}$$

$$\mathrm{FD}\,\{\mathrm{P(X,Y)}\} = \frac{\exp(JKD)}{J\lambda D} \iint P(X,Y) \times \exp\left[jk\frac{(m-x)^2+(n-y)^2}{2D}\right] dxdy$$

The FFT and the IFFT are shown by fft and fft^{-1}, respectively. (m, n) are the RPM pixel's coordinates, and (x, y) are the original image pixel's coordinates. The diffraction distance is represented by DDD, the wavelength of light by λ, the wave number by k=2π/λ and j is the imaginary unit. The function ϕ(u,v) is in the frequency domain, while ξ(x,y) is in the space domain. They are all patterns of white noise that are evenly distributed and are not reliant on the interval [0, 1]. There is a possibility that the process of encryption does not need the use of a lens system. Instead, a computer with simulation software can simulate encryption. Additionally, the plural nature of the encrypted data necessitates its conversion into real numbers before its subsequent encryption.

A. Memristive Hyper Chaotic System

Chaotic encryption has already been studied and used a lot in the area of image encryption. Chaos is good because it is unpredictable, sensitive to the original value, and uncertain. It has become more adult and safe as it keeps getting better and new ideas are added. When compared to a normal chaotic system, the hyper-chaotic system has more complicated folding properties, a better growth path, and more safety. This is a general model of a hyperchaotic Lorenz system [10]:

$$\begin{cases} x = a(y-x) \\ y = cx - y - xy \\ z = xy - bz \\ w = -yz + rw \end{cases}$$

The hyperchaotic Lorenz system comprises four factors: a, b, c, and r. Assuming that 1.52 < r 0.06, a = 10, b = 2.667, c = 28, and the system is currently in a state of extreme chaos. The idea of a memristor was first put up by Professor Cai Shaotang, and the first practical model of a memristor was built in a laboratory belonging to HP. It is possible to create chaotic systems more easily because of the advent of the memristor, which also makes the process of creating hyperchaotic systems more straightforward. The model of a memristor used in this work is:

$$q(\phi) = -a\phi + 0.5b\phi|\phi| \quad \ldots \quad (5)$$

ϕ is the memristor's magnetic flux, and both a and b are positive.

Here is the memristor equation:

$$\mathrm{W}(\varphi)=\frac{dq(\varphi)}{d\varphi} = -a + b|\varphi| \quad \ldots \quad (6)$$

In this particular piece of writing, the memristor hyper chaotic Lorenz system model that was used may be summarized as follows:

$$\begin{cases} x = d(y-x) \\ y = -xz + cy + (e+fc)x + kw(w)x \quad \ldots \quad (7) \\ w = x \end{cases}$$

The parameters c, d, e, f, k, c, d, e, f, k, and g typically represent the coefficients or constants that define the dynamics of the system. The study utilizes the parameters: a = 15, b = 0.02, c = -10, d = 35, e = 95, f = -4, k = 1, and g = -3.

B. Memristive Chaotic Encryption Sequences: In the course of this investigation, a cryptosystem key is used, which is comprised of two distinct components: the static secret key and the dynamic secret key. The hash function generates a 256-bit hash value based on the plaintext, which is then used to calculate the dynamic secret key from the plaintext. In Fresnel diffraction, the static secret keys encompass essential parameters like the diffraction distance DDD, wavelength λ, and the initial values of the memristive hyperchaos system. These parameters form a unique key space denoted as {hash256, x(0), y(0), z(0), w(0), D1, D2, λR, λG, λB}. This comprehensive set defines the conditions under which Fresnel diffraction occurs and plays a crucial role in determining its outcomes. Initially, utilize the constructed memristor to generate the encryption sequence and mask. Subsequently, use the plain image size to Obtain the corresponding coordinates in

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

both spatial and frequency domains. Thirdly, create the DRPE environment, which is the parameter's starting value.

Decide on the diffraction distance D and wavelength λ. These parameters are included in the keys; for various sub-images, the keys can have different values specified. Finding the SHA-256 value of the plain picture is the fourth step, and it has a significant impact on the initial value of the hyperchaotic system. This makes unique keys for each plain, which can make it more resistant to CPA.

$$\begin{cases} x(0) = x(o) + (s_1 \oplus s_2 \oplus s_3 \oplus s_4)256/1000 \\ y(0) = y(o) + (s_5 \oplus 6 \oplus s_7 \oplus s_8)256/1000 \\ z(0) = z(o) + (s_9 \oplus s_{10} \oplus s_{11} \oplus s_{12})256/1000 \\ w(0) = w(o) + (s_{13} \oplus s_{14} \oplus s_{15} \oplus s_{16})256/1000 \end{cases}$$

Where the hyperchaotic system's initial parameters are x(0), y(0), z(0), and w(0).The initial values upon disturbance are (x(0))˙, (y(0))˛, (z(0)) ί, and (w(0)) ί. The bitwise XOR operation is represented by ⊕, and the plain image's hash value is denoted by s_i .

FFT-Initially, separate the gray image channel subgraphs of the plaintext image and then individually encrypt each subgraph. Here, the R-channel submap serves as an illustration. This results in the picture being converted from the spatial domain to the frequency domain by the FFT, which ultimately produces the frequency domain image P1. During the subsequent stage, P1 will go through a phase shift in the optical domain that is both random and double-random. To define the equation, the following is what it means:

$$p_1 = fft(p) \quad \dots \quad (8)$$

P is the encoded version of the original picture, and P_1 is a matrix that has been altered using the Fourier transform.

C. The first DRPE- Develop the phase mask RPM_1 by the pre-processed sub-image P_1 in the frequency domain. To complete the operation for double-random encryption, the application of the angular spectrum propagation function requires the following equation to be defined:

$$\begin{cases} Rt_1 = \exp\,(2\pi j \times mask_1) \\ Fai_1 = p_1 . Rt_1 \\ Ft = h_2(fx, fy, D_{1,\lambda_1}).fai \end{cases} \quad \dots \quad (9)$$

D. The multiplication of P_1 and Rt_1 points yields FaI_1, while $mask_1$ represents the random phase mask RPM_1. The frequency domain coordinate location is denoted by the notation (fx, fy), while the angular spectrum propagation function is denoted by the notation h2(•). Rt_1 is an abbreviation for the value of $mask_1$. According to the Fresnel diffraction distance, λ_1 is the wavelength of the light that is incident with a single amplitude, and D_1 is the distance. F_t is the first picture to be encrypted using a random number generator.

E. The second DRPE: To achieve the second random phase encryption, multiply the image by the phase mask RPM_2 after double random encryption, and Follow the angular spectrum propagation function. As a given equation:

$$\begin{aligned} Rt_2 &= \exp\,(2j \times mask_2) \\ Fai_2 &= Ft . Rt_2 \quad \dots \quad (10) \\ c_1 &= h_2(fx, fy, D_2\ \lambda_2).Fai_2 \end{aligned}$$

It is important to note that mask2 represents the random phase mask RPM_2, and Fai_2 is the product of the multiplication of F t and Rt2 points. The second randomly encrypted image is represented by c_1, the single-amplitude incident light wavelength is represented by λ_2, the Fresnel diffraction distance is represented by Rt_2, and the value of Ft is represented by Rt_2.

F. IFFT: To translate from plural to real cipher, use the floor and abs functions. Finally, change the values of the pixels in C_1 to [0, 256] using the IFFT function. The equation's definition is as follows:

$$C_2 = fft^{-1}(\text{floor}(\text{abs}(C_1))) \quad \dots \quad (11)$$

The floor (•) function rounds the element of C_1 to the nearest integer that is greater than or equal to negative infinity, while the abs (•) function takes the absolute value of C_2. The normalize (•) command masks the value of C_2, representing the DRPE-encrypted picture, between 0 and 255.

G. Permutation: By using Matlab's ascending function sort (•), the pixel values of a chaotic matrix are arranged in ascending order, from the smallest to the largest. Next, take note of the location of the sorted coordinates [index H, index W]. The new coordinates of the image's pixels should be encrypted as a precautionary measure [index H, index W]. The only thing that is modified throughout the permutation process is the location of the pixel value; the pixel value itself remains unchanged. As a brief overview, the formula is as follows:

$$\sum_{i=1}^{H} \sum_{J=1}^{W} u = c_2[indexH(i), indexW(J)]$$

With U representing the cipher image that has been generated using permutation, and C_2 representing the picture that has to be encrypted. H and W represent the color pictures C_2 and U's height and width, respectively. The row random sequence used for permutation is denoted by index H(i), and the column random sequence by index W(j).

H. Diffusion: Take advantage of the preparation for step 1 of You are provided with a chaotic random sequence S that is of length H × W. The first pixel of the cipher picture, R1, should be set to 0. Therefore, to to acquire the second cipher pixel R_2, you must first compute the total of S1, U1, and R_1, and then take the modulus of the sum. The iterative relationship to create the cipher pixel R_i sequentially. In this case, U_1 represents the first pixel of the encrypted image, while S_1 represents the first pixel of the random sequence S. To completely eliminate the plain information from the cipher pixels, it is required to perform reverse diffusion, which involves diffusing informationfrom the H × W direction to the 1 position. The following is the precise formula for two diffusions.

$$\begin{cases} R_I = (R_{I-1} + S_I + U_I) mod256 \quad i\,[1, H \times w] \\ R_I = (R_{I+1} + S_I + U_I) \quad i\,[1, H \times w, 1 \end{cases} \quad \dots \quad (12)$$

R_i represents the final encrypted cipher after encrypting the R channel subgraph of the plain picture. U represents the original image before diffusion, R_i represents the image after modulus diffusion, and R_i represents the final encrypted cipher. Through the use of S as a random chaotic sequence and the application of the modulus operator, the computation that was performed ultimately

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

produced values that ranged from 0 to 256. The dimensions of P determine the range of values for H × W.

Image compositing: To obtain the ciphers of the clear picture subgraphs on an individual basis, it is necessary to repeat the steps that were previously stated. Utilize the concatenation function to combine the three encrypted sub-images into a single encrypted picture that has all of the information.

$$C = \mathrm{cat}\,(3, R_i', G_i', B_i') \quad \ldots \quad (13)$$

Where the final cipher is C, Ri represents the cipher for the plain image R channel, Gi represents the cipher for the plain image G channel, and Bi represents the cipher for the plain image B channel.

IV. SIMULATION RESULTS

The performance of the proposed photo encryption system may be evaluated using standard metrics such as the peak signal-to-noise ratio (PSNR), the structural similarity index (SSIM), the normalized partial correlation coefficient (NPCR), and the mean square error (MSE). These metrics can be used to assess the resilience of the scheme and to compare the quality of the encrypted image to the original plaintext image. The picture specifications used for analysis purposes are shown in Table-I.

A. Histogram Analysis

The recommended technique was also validated by doing a histogram analysis on both the original pictures and the decrypted versions of those photographs. It is important to note that the histogram of the encrypted picture should be completely distinct from the histogram of the original image when using image encryption methods. Figure 4 displays the histograms for the encrypted and decrypted versions of Lena's photos [28] that were generated using a different approach, such as DRPE, compressed sensing, and the way that was recommended throughout the process. The histograms of the original and decrypted pictures are identical, as seen in this diagram. In addition, it is evident that the histograms of the encrypted photographs for the DRPE and the approach that is advised are distinct from those of the photographic pictures that were originally taken Fig.4. displays a comparison of the histograms produced by the suggested technique on several photos. The original and encrypted histograms for each of the examined photographs differ, which indicates a strong encryption technique

B. Noise Analysis

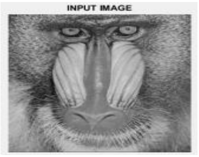
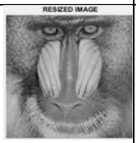
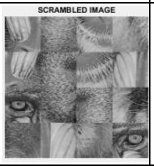
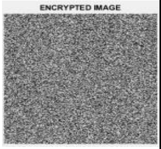
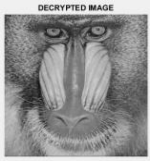
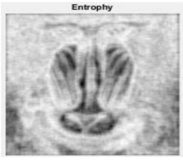
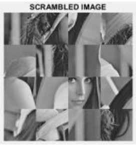
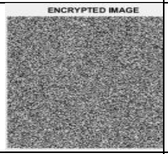
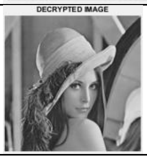
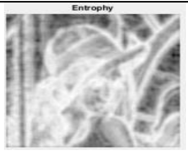
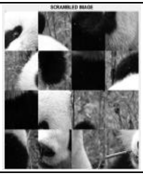
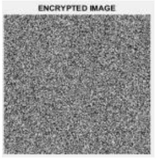
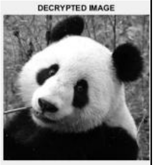
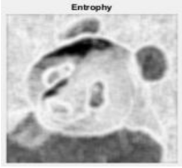
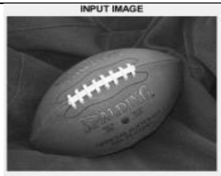
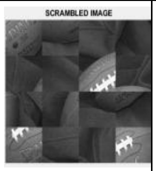
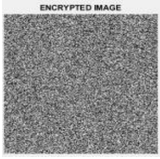
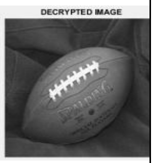
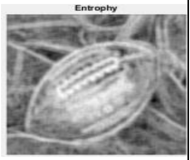
i. Peak signal-to-noise ratio (PSNR):

A metric known as the peak signal-to-noise ratio (PSNR) is used to evaluate the quality of a picture after encryption has been performed. It is determined as the difference between the strongest signal that can be produced and the noise that degrades the accuracy of the signal's representation. The PSNR equation is presented below:

$$\mathrm{PSNR} = 10 * \log 10\left(\frac{(\mathrm{MAX}^2)}{\mathrm{MSE}}\right) \quad \ldots \quad (14)$$

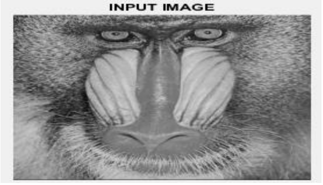
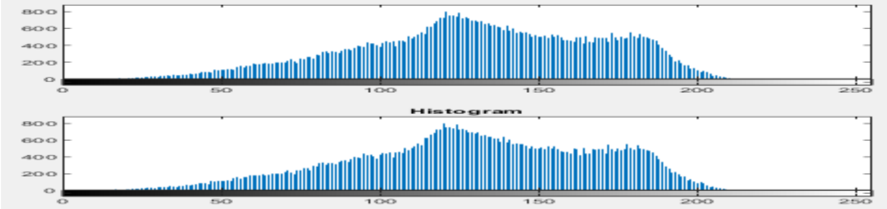
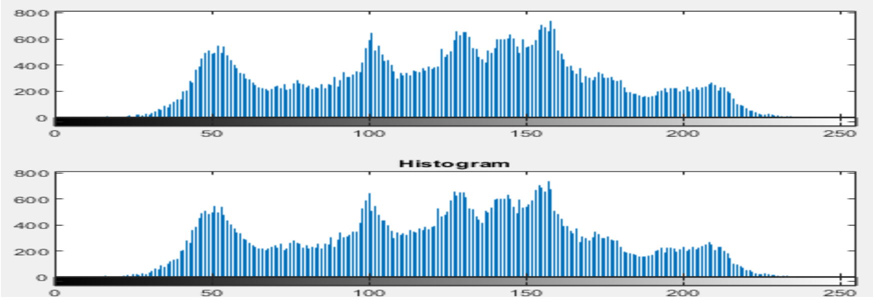
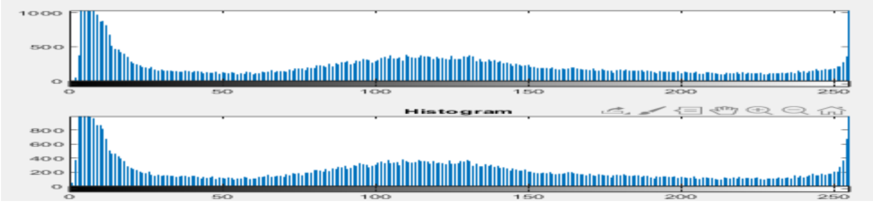
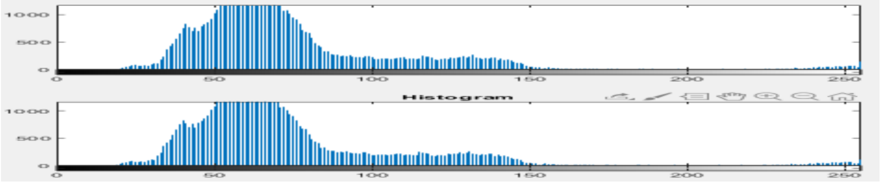
where the maximum pixel value that may be utilized in an image is denoted by MAX and the mean squared error (MSE) is the difference between the encrypted and unencrypted versions of the same image. The quality of the decrypted image improves with a greater PSNR value [19]. The average squared difference between the pixel values of the original and encrypted images is what this metric measures. Lower MSE values signify greater encryption performance since they show that the encrypted image's pixel values are more similar to those of the original image [5].

Table-I: Result Image

	Input Image	Resize	Scramble	Encrypted	Decrypted	Entropy
Barbo On						
Lena						
Panda						
Football						

Retrieval Number: 100.1/ijeat.D457714040425
DOI: 10.35940/ijeat.D4577.14040425
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Sample Images	Histogram
	
	
	
	

[Fig.4: Show the Comparative Analysis of the Histogram Generated on Image Lena for Different Schemes]

C. Mean Squared Error (MSE)

MSE is a measure that is typically used to evaluate the degree to which two images are distinct from one another. The MSE is a calculation that determines the squared difference between the raw pictures and the encrypted ones [26]. MSE is calculated as follows

$$\mathrm{MSE} = \left(\frac{1}{N}\right) * \sum(\mathrm{i} = 1 \text{ to } N)\left[\left(\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{K}(\mathrm{i},\mathrm{j})\right)^2\right] \ldots \quad (15)$$

Where I(i, j) represents the intensity of the pixel in the original picture at position (i, j), K(i, j) represents the intensity of the pixel in the encrypted image at position (i,j), and N represents the total number of pixels in the image. The mean squared error (MSE) number may vary anywhere from zero to a maximum value, depending on the dynamic range of the pixel values being used in the picture. A stronger encryption method is indicated by a lower MSE value [6].

D. Normalized Pixel Change Rate (NPCR)

NPCR is a metric that is used to determine the degree of correlation between two digital pictures, notably in the context of image encryption or watermarking. It does this by taking into account the total number of pixels in both photos and calculating the percentage of pixels that are different between the two images respectively [23].The value of the NPCR may be determined by utilizing the equation that is shown below:

$$\mathrm{NPCR} = \left(\mathrm{N}_{diff} — \mathrm{N}_{total}\right) * 100 \ldots \quad (16)$$

The Normalized Pixel Change Rate, presented as a percentage, is denoted by the acronym NPCR. The total number of pixels that are different between the two pictures is denoted by the numeric value N_{diff}. The entire number of pixels in the photographs is denoted by the variable N_{total}, and it is the same for both of the images that are being compared. To calculate the N_{diff} value, you compare the corresponding pixels in the two images. If the pixel values are different, you increment the N_{diff} counter. Once you have compared every pixel in both photos, you will be able to determine the total number of pixels that are different. Simply counting the total number of pixels in one of the photos is all that is required to get the N_{total}, value, since this value is same for both of the images that are being compared [27]. A higher NPCR score shows that a greater proportion of pixels have been altered between the two photos, which is indicative of a greater degree of image modification. In this paper, the NPCR we are getting is 99.82 which is very good range.

E. Structural Similarity Index (SSIM)

A popular statistic for determining how similar two photos are is called SSIM.

It takes into account disparities in pixels as well as structural data and how

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

people perceive the quality of an image.

The range of SSIM values is from -1 to 1, with a value of 1 indicating that the two photos are completely similar to one another, a value of 0 indicating that there is no resemblance between them, and negative values indicating that there is a significant difference between them. The following equation can be used to calculate the SSIM index:

$$\mathrm{SM}(y,x) = [\mathrm{L}(y,x) * \mathrm{C}(y,x) * \mathrm{S}(y,x)]^{\alpha} \quad \dots \quad (17)$$

Where the two photos that are being compared are denoted by x and y. The luminance comparison, denoted by the notation L(y, x), is a measurement of the degree to which the intensities and brightness of the pixels are comparable. It is defined as:

$$\mathrm{L}(y,x) = \frac{2 * \mu_y * \mu_x + c_1}{\mu_y^2 + \mu_x^2 + c_1} \quad \dots \quad (18)$$

The variables μ_x and μ_y represent the average values of the images x and y, respectively. Additionally, c_1 is a minor constant that is provided to ensure numerical stability. C(y, x) represents the contrast comparison, which measures the similarity in image contrasts. It is defined as:

$$\mathrm{C}(y,x) = \frac{(2 * \sigma_y * \sigma_x + c_2)}{(\sigma_y{}^2 + \sigma_x{}^2 + c_2)} \quad \dots \quad (19)$$

The standard deviations of pictures x and y are denoted by σ_x and σ_y, respectively, in this context. Additionally, c_2 is classified as a tiny constant. S (y, x) represents a comparison of structures, which determines the degree of similarity between the information structure and structure. The following is a definition of it:

$$\mathrm{S}(y, x) = (\sigma_{yx} + c_3) / (\sigma_y * \sigma_x + c_3) \quad \dots \quad (20)$$

σ_{yx} represents the covariance of images x and y, while c_3 is a small constant. When it comes to adjusting the relative significance of L, C, and S components, α is a control parameter that is used. It is usually set to 1. To produce a full similarity measure that takes into consideration luminance, contrast, and structure, the SSIM index combines the three components L, C, and S. Higher SSIM values show a greater degree of similarity between the two pictures, while lower values indicate greater dissimilarity. SSIM is widely used in image quality assessment and image processing applications to evaluate the fidelity and similarity of processed or compressed images to the original reference images. The SSIM values obtained by performing the image in the p proposed work comes under the normal range of -1 to 1 which means the proposed work satisfies the SSIM parameters.

Table-II: Comparative Analysis of PSNR, NPCR and MSE Values of Techniques like DRPE, Compressed Sensing and Proposed Work

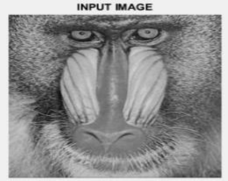
IMAGES	ATTACK	PSNR	MSE	SSIM	NCPR
	Text Attack	48.13	1.00	1.00	0.00
	Cipher Attack	47.23	0.9	1.0	1.0
	Brute Force Attack	78.23	1.0	0.98	0.0
	Text Attack	48.13	1.00	0.99	0.00
	Cipher Attack	48.25	0.9	1.0	1.0
	Brute Force Attack	48.36	1.0	1.0	0.
	Text Attack	48.27	0.96	0.99	0.00
	Cipher Attack	47.25	0.9	1.0	0.0
	Brute Force Attack	48.32	1.0	0.9	0.0
	Text Attack	48.13	0.99	0.99	0.00
	Cipher Attack	48.65	1.0	1.0	1.0
	Brute Force Attack	48.12	0.9	0.0	0.1

Table-II provides a comparative examination of performance measures for three different picture encryption approaches. These metrics include the Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Number of Pixel Change Rate (NPCR): Double Random Phase Encryption (DRPE), Compressed Sensing, and the proposed method. Across various images subjected to different types of attacks (Text Attack, Cipher Attack, Brute Force Attack), the proposed method consistently demonstrates competitive results. It achieves high PSNR values, indicating minimal distortion between encrypted and original images, and low

MSE values, suggesting accurate preservation of image quality. SSIM scores near 1.0 indicate strong structural similarity, crucial for retaining image fidelity. NPCR values vary depending on the attack type, with the proposed method showing resilience against Cipher Attacks and exhibiting effectiveness comparable to or better than DRPE and Compressed Sensing in resisting image decryption attempts. These findings underscore the robustness and efficacy of the proposed encryption approach in safeguarding image integrity against a range of security threats.

V. CONCLUSION

The proposed methodology for encrypting images integrates Double Random Transformation (DRT) with Memristive Chaos to enhance security against cryptographic attacks. DRT employs complex spatial and temporal transformations, while Memristive Chaos utilizes chaotic dynamics from a hyperchaotic Lorenz system facilitated by memristors. This combination aims to capitalize on DRT's robust encryption capabilities and Memristive Chaos's efficiency in spatial domain encryption, addressing their respective limitations when used individually. By integrating these methods, the approach ensures comprehensive encryption through FFT/IFFT transformations, phase masking, angular spectrum propagation, permutation, and diffusion processes. Evaluation using standard metrics like PSNR and SSIM, alongside histogram analysis, confirms the method's effectiveness in altering image characteristics significantly, ensuring robust protection of sensitive image data against potential cyber threats.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it has been conducted without any external sway.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Liang X, Zhang C, Luo Y, Wang X, Qiu K. Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion. Journal of Lightwave Technology. 2023 Mar 15;41(6):1619–25. Doi: https://doi.org/10.1109/jlt.2022.3226768
2. Luo Y, Zhang C, Wang X, Liang X, Qiu K. Robust key update with controllable accuracy using support vector machine for secure OFDMA-PON. Journal of Lightwave Technology .2023 Jul 15;41(14):4663–71. Doi: https://doi.org/10.1109/jlt.2023.3244202
3. Wu T, Zeng W, Liu Y, Song S, Zhao L, Chen C, et al. Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping. Optics Letters . 2023 Jan24;48(3):684. Doi: https://doi.org/10.1364/ol.480981
4. Li C, Lin D, Lü J, Hao F. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimedia.2018 Oct1;25(4):46–56. Doi: https://doi.org/10.1109/mmul.2018.2873472
5. Li X, Zhou L, Tan F. An image encryption scheme based on finite-time cluster synchronization of two-layer complex dynamic networks. Soft Computing. 2021 Nov 22;26(2): 511–25. Doi: https://doi.org/10.1007/s00500-021-06500-y
6. Tiwari D, Mondal B, Singh SK, Koundal D. Lightweight encryption for privacy protection of data transmission in cyber physical systems. Cluster Computing. 2022 Oct 26;26(4):2351–65. Doi: https://doi.org/10.1007/s10586-022-03790-1
7. Ding Y, Liu W, Wang H, Sun K. A new class of discrete modular memristors and application in chaotic systems. The European Physical Journal Plus. 2023 Jul 21;138(7). Doi: https://doi.org/10.1140/epjp/s13360-023-04242-4
8. Liu X, Sun K, Wang H, He S. A class of novel discrete memristive chaotic map. Chaos Solitons & Fractals. 2023 Sep 1;174:113791. Doi: https://doi.org/10.1016/j.chaos.2023.113791
9. Man Z, Li J, Di X, Sheng Y, Liu Z. Double image encryption algorithm based on neural network and chaos. Chaos Solitons & Fractals. 2021 Nov 1;152:111318. Doi: https://doi.org/10.1016/j.chaos.2021.111318
10. Chen L, Li C, Li C. Security measurement of a medical communication scheme based on chaos and DNA coding. Journal of Visual Communication and Image Representation. 2022 Feb 1;83:103424. Doi: https://doi.org/10.1016/j.jvcir.2021.103424
11. Hu M, Li J, Di X. Quantum image encryption scheme based on 2D $\varvec{Sine^{2}-Logistic}$ chaotic map. Nonlinear Dynamics. 2022 Oct 23;111(3):2815–39. Doi: https://doi.org/10.1007/s11071-022-07942-1
12. Man Z, Li J, Di X, Zhang R, Li X, Sun X. Research on cloud data encryption algorithm based on bidirectional activation neural network. Information Sciences. 2023 Apr 1;622:629–51 Doi: https://doi.org/10.1016/j.ins.2022.11.089
13. Slimane NB, Aouf N, Bouallegue K, Machhout M. A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model. Multimedia Tools and Applications. 2018 Jun 4;77(23):30993–1019. Doi: https://doi.org/10.1007/s11042-018-6145-8
14. Abduljabbar ZA, Abduljaleel IQ, Ma J, Sibahee M a. A, Nyangaresi VO, Honi DG, et al. Provably secure and fast color image encryption algorithm based on S-Boxes and Hyperchaotic Map. IEEE Access. 2022 Jan 1;10:26257–70. Doi: https://doi.org/10.1109/access.2022.3151174
15. Kumari P, Mondal B. An encryption scheme based on grain stream cipher and Chaos for privacy protection of image data on IoT network. Wireless Personal Communications. 2023 Apr 3;130(3):2261–80. Doi: https://doi.org/10.1007/s11277-023-10382-8
16. Andono PN, Setiadi DRIM. Improved Pixel and Bit Confusion-Diffusion based on mixed chaos and hash operation for image encryption. IEEE Access. 2022 Jan 1;10:115143–56. Doi: https://doi.org/10.1109/access.2022.3218886
17. Zahid AH, Arshad MJ, Ahmad M, Soliman NF, El-Shafai W. Dynamic S-Box Generation Using Novel Chaotic Map with Nonlinearity Tweaking. Computers, Materials & Continua/Computers, Materials & Continua (Print). 2023 Jan 1;75(2):3011–26. Doi: https://doi.org/10.32604/cmc.2023.037516
18. Manzoor A, Zahid AH, Hassan MT. A new dynamic substitution box for data security using an innovative Chaotic map. IEEE Access. 2022 Jan 1;10:74164–74. Doi: https://doi.org/10.1109/access.2022.3184012
19. Mondal B, Singh JP. A lightweight image encryption scheme based on chaos and diffusion circuit. Multimedia Tools and Applications. 2022 Jan 8;81(24):34547–71. Doi: https://doi.org/10.1007/s11042-021-11657-7.
20. Durafe A, Patidar V. Comparative analysis of chaotic image encryption using improved 2D Gingerbreadman Map and Chirikov Standard Map. 2022 International Conference for Advancement in Technology (ICONAT) .2022Jan21. Doi: https://doi.org/10.1109/iconat53423.2022.9725986
21. Wei D, Jiang M, Deng Y. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Systems With Applications. 2023 Mar1;213:119074. Doi: https://doi.org/10.1016/j.eswa.2022.119074

22. Xian Y, Wang X. Fractal sorting matrix and its application on chaotic image encryption. Information Sciences. 2021 Feb 1;547:1154–69. Doi: https://doi.org/10.1016/j.ins.2020.09.055
23. Wang X, Yang J. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. Information Sciences. 2021 Aug 1;569:217–40. Doi: https://doi.org/10.1016/j.ins.2021.04.013
24. Chai X, Wang Y, Chen X, Gan Z, Zhang Y. TPE-GAN: Thumbnail preserving encryption based on GAN with key. IEEE Signal Processing Letters. 2022 Jan 1;29:972–6. Doi: https://doi.org/10.1109/lsp.2022.3163685
25. Kumari P, Mondal B. Lightweight image encryption algorithm using NLFSR and CBC mode. The Journal of Supercomputing. 2023 May 29;79(17):19452–72. Doi: https://doi.org/10.1007/s11227-023-05415-9
26. Liu W, Sun K, He S, Wang H. The Parallel Chaotification Map and its application. IEEE Transactions on Circuits and Systems I Regular Papers. 2023 Sep 1;70(9):3689–98. Doi: https://doi.org/10.1109/tcsi.2023.3279371
27. Wang Z, Zhuang L, Yu J, Jiang H, Xu W, Shi X. Hidden Dynamics of a New Jerk-like System with a Smooth Memristor and Applications in Image Encryption. Mathematics. 2023 Nov 10;11(22):4613. Doi: https://doi.org/10.3390/math11224613
28. USC School of Cinematic Arts. Leena. USC SIPI; n.d. [cited 2024 Sep 25]. https://sipi.usc.edu/database/database.php?volume=misc&image=12#top
29. Suneetha, CH., Surendra, T., & Neelima, CH. (2020). Implementation of Double Fold Text Encryption Based on Elliptic Curve Cryptography (ECC) with Digital Signature. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 5, pp. 3840–3846). Doi: https://doi.org/10.35940/ijrte.e6446.018520
30. Munish Mehta, Vijay Goyar, Vishnu Bairwa, Security and Authentication through Text Encryption and Decryption based on Substitution Method. (2019). In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 9S, pp. 112–115). Doi: https://doi.org/10.35940/ijitee.i1017.0789s19
31. Jaswanth, P. V., Reddy, B. R., Kumar, M. S. P., & Priyadarsini, M. J. P. (2020). Color Image Encryption using AES and RSA. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 5, pp. 547–550). Doi: https://doi.org/10.35940/ijeat.e9648.069520
32. Muthukrishnan, Dr. R., & Prakash, N. U. (2023). Validate Model Endorsed for Support Vector Machine Alignment with Kernel Function and Depth Concept to Get Superlative Accurateness. In International Journal of Basic Sciences and Applied Computing (Vol. 9, Issue 7, pp. 1–5). Doi: https://doi.org/10.35940/ijbsac.g0486.039723
33. Nagar, K., & Chawla, M. P. S. (2023). A Survey on Various Approaches for Support Vector Machine Based Engineering Applications. In International Journal of Emerging Science and Engineering (Vol. 11, Issue 11, pp. 6–11). Doi: https://doi.org/10.35940/ijese.k2555.10111123

AUTHOR'S PROFILE

Ritu Sharma is a research scholar in the Department of Computer Science and Information Technology, Central University of Haryana, Mahendergarh, Haryana, India. She has completed her Master's in Computer Science and is qualified NET/JRF in the same specialization. Her area of research interest is Cybersecurity, Blockchain, Network Security, Image Encryption, Quantum Cryptography, Object Detection etc. She aims at finding new advanced hybrid image encryption techniques in cryptography.

Sunil Kumar is an Assistant Professor in the Department of Computer Science and Information Technology, the Central University of Haryana, Mahendergarh, Haryana, India. He has qualified MCA, M. Tech, UGC NET, and Ph.D in Computer Science. He has research experience of more than 12 years with an area of specialization is Network Security, Computer Networks, Cyber security, the Internet of Things (IOT), and Internet of Vehicles (IOV). He has an educational experience of more than 10 years. He is currently working in the domain of Network security and Internet of vehicles. He has experience in organizing social activities and has achieved various award at different platforms of the university.
