

# Authenticated image encryption using robust chaotic maps and enhanced advanced encryption standard

Rupaliben V. Chothe, Sunita P. Ugale, Dinesh M. Chandwadkar, Shraddha V. Shelke

Department of Electronics and Telecommunication Engineering, K. K. Wagh Institute of Engineering Education and Research, Savitribai Phule Pune University, Pune, India

## Article Info

### Article history:

Received Jul 4, 2024

Revised Sep 19, 2024

Accepted Oct 7, 2024

### Keywords:

Advanced encryption standard

Authenticated encryption

Color image encryption

Cryptography

Robust chaotic maps

## ABSTRACT

The ability of advanced encryption standard (AES) algorithm to protect information systems has given cryptography a new dimension. Recent encryption approaches to enhance randomness include the use of chaotic algorithms, which provide resistance to differential attacks. We have proposed the application of robust chaotic maps in the block cipher to design a secure authenticated encryption scheme to get advantages of both. The chaotic sequence is generated using hyperbolic tangent map and added to input image initially to increase randomness. The basic 256-bit AES key is generated using the robust Renyi modulo map. An additional 128-bit key enhances security. Instead of static values used in AES, dynamic initialization vector (IV), different for every image will be generated. The results are mathematically verified using various security parameters. The algorithm provides lower values of peak signal-to-noise ratio (PSNR) (7.81 to 9.10 dB) for encrypted images and higher dissimilarities between input and encrypted image histograms. Thus, it is highly resistant to statistical attacks. The experimental results and their comparison prove the superiority of our proposed cryptosystem against statistical, differential and brute-force attacks. Thus, the novel multi-chaotic AES-GCM (galois/counter mode) algorithm can be used for color image encryption in military and industrial applications demanding high data security and authentication.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Rupaliben V. Chothe

Department of Electronics and Telecommunication Engineering

K. K. Wagh Institute of Engineering Education and Research, Savitribai Phule Pune University

Pune, India

Email: rvchothe@kkwagh.edu.in

## 1. INTRODUCTION

The security of data is a major concern in the advanced communication networks. Encryption is employed to safeguard the information and maintain its confidentiality. Advanced encryption standard (AES) is widely recognized as the industry standard for encryption due to its unique blend of flexibility and security. Many studies are being conducted to fully utilize the potential of AES in various security applications ever since the National Institute of Standards and Technology (NIST) recognized it as the next generation security algorithm. Smart grid communications, wireless multimedia sensor networks (WMSN), smart cards, web servers, and internet of things (IoT)-enabled healthcare infrastructure [1] are some of the areas where enhanced AES is being researched and used.

Authenticated encryption (AE) systems are often employed in transport layer security (TLS) and IPsec. TLS 1.3, the most recent version, no longer supports non-AE schemes [2]. The United States NIST adopted the galois/counter mode (GCM) [3] to offer a fast method for authenticated cryptography. GCM has

been used in a number of standards, including the IEEE 802.1AE for media access control (MAC), the IEEE P1619.1 for storage devices and the IETF RFC 4106 for IPsec encapsulating security payload [4]. An additional authenticated data (AAD), initialization vector, plaintext, and an AES key are the inputs to the GCM. The output consists of an authentication tag which is used at the receiver to confirm the authenticity of the AAD and the ciphertext [3]. The researchers have improved throughput of AES by algorithmic modifications [5], [6]. The AES-GCM encryption algorithm was modified by rotating the initialization vector (IV) to raise the randomness [7].

Compared to the conventional encryption, which has a poor diffusion effect, the chaos theory has been believed to be an effective method. These chaotic systems are very sensitive to design parameters and initial values. Chaotic maps are used to provide random sequences that enable precise encryption, but the chaotic techniques with poor ergodicity are vulnerable to attacks [8]. The output of two chaotic maps were combined in order to create a hybrid chaotic map. The hybrid chaotic map outperforms the single chaotic encryption in terms of security [9]. Arnold transforms and fractional order chaotic sequence were used to encrypt the data. But the validity of the algorithm is to be verified in detail [10].

Kari *et al.* [11] introduced a novel image encryption algorithm in which Arnold's cat map is used for confusion and the combination of sine, logistic, and tent map provides diffusion. Sine map was used for parallel permutation and diffusion of pixel values in [12]. Xian *et al.* [13] introduced chaotic sub-block scrambling using spiral transformation, and digit selection diffusion, requiring the attacker to break each algorithm individually. Mondal and Singh [14], a light-weight, chaotic map-based concept was put into practice. They were able to execute substitution and transposition of the image pixels in a single scan, which decreased time complexity. The novel block-based encryption includes used of optical signals [15], fractional fourier transform based logistic map [16] and Fibonacci sequence [17], [18] to raise security. Research on hyper-chaotic algorithms includes the design of fourth order systems for medical image encryption [19], [20]. The literature includes the work on either improved AES or chaotic encryption. The previous research work on AES+chaos is not explored to its full potential and does not include authentication [21]–[23]. Also, less security and loss of image attributes are major concerns.

The summary of shortcomings of previous research work focusing on block and chaotic encryption:

- a) For some AES related implementations, resistance to attacks is not tested.
- b) In chaos-based image encryption, most of the research is based on medical grayscale images. Color image encryption is not included.
- c) The chaotic encryption research does not include a scheme with Authentication.
- d) The initial conditions of a chaotic system do not depend on the input image, which makes the system weak against differential attacks. The image attributes may be lost during encryption.
- e) The security against statistical attacks is hampered because histogram of the encrypted image is not uniform.

Recent research focused on comparing block cipher with chaotic and hybrid chaotic systems. The study demonstrated that AES is immune to statistical attacks, it has lower peak signal-to-noise ratio (PSNR) and more difference between histograms of input and encrypted images. The hybrid chaotic maps are more resilient to targeted plain text attacks or differential attacks [24]. Thus, both block cipher and chaotic schemes are providing advantages against different levels of attacks. For this reason, the development of new algorithm facilitating authenticated block encryption along with advantages of chaotic encryption, providing resistance to both differential and statistical attacks, is of interest. The unpredictable nature of chaotic systems enhances the complexity and widens the key space of traditional AES-GCM for enhancing the security.

The following is a research contribution of the work:

- a) The hybrid implementation of authenticated block cipher encryption along with chaotic improvements
- b) Increased randomness using hyperbolic tangent map
- c) Secret key generation using robust Renyi-modulo map
- d) Unique chaotic IV generation using parameters from input image data
- e) Additional 128-bit key for improved security
- f) Substitution box is shuffled using Arnold cat map for enhanced security
- g) Authenticated encryption - verification using tag at the receiver
- h) Analysis of the obtained results shows the excellent performance and robustness to attacks
- i) Applicable not only to grayscale images but also to colour images

The paper is arranged as follows: the section 2 provides detail description of proposed algorithm with block diagrams and equations. The section 3 presents results in terms of mathematical parameters and visual representation along with discussion and comparison with previous results. Section 4 concludes the research work.

**2. METHOD: THE PROPOSED ALGORITHM**

AES-GCM is a block encryption algorithm offering data integrity and authentication both. It combines universal hashing over the binary field GF (2128) with a block cipher running in counter mode. AES provides high security against statistical attacks. The advantages of chaotic systems include high randomness and sensitivity to initial conditions and control parameters. To get advantages of both to provide high security along with authentication, a novel algorithm is designed.

The algorithm requires following inputs: plaintext P (or input color image) split into blocks of 128-bit sequences, an IV, AAD and the secret key K. Chaotic sequence is generated using hyperbolic tangent map (explained in section 2.1) and input image is initially XORed with it to increase randomness. Chaotic AES key is generated using robust Renyi modulo map (explained in section 2.2). Unique IV is generated from the image data (explained in section 2.3). Traditional AES S-box is rearranged for additional security (explained in section 2.4). The authentication tag is correctly matching at the receiver for all images. The simulation is performed on MATLAB R2023a. Figure 1 presents the picture of MATLAB simulation. Figure 2 presents the block diagram of overall encryption.

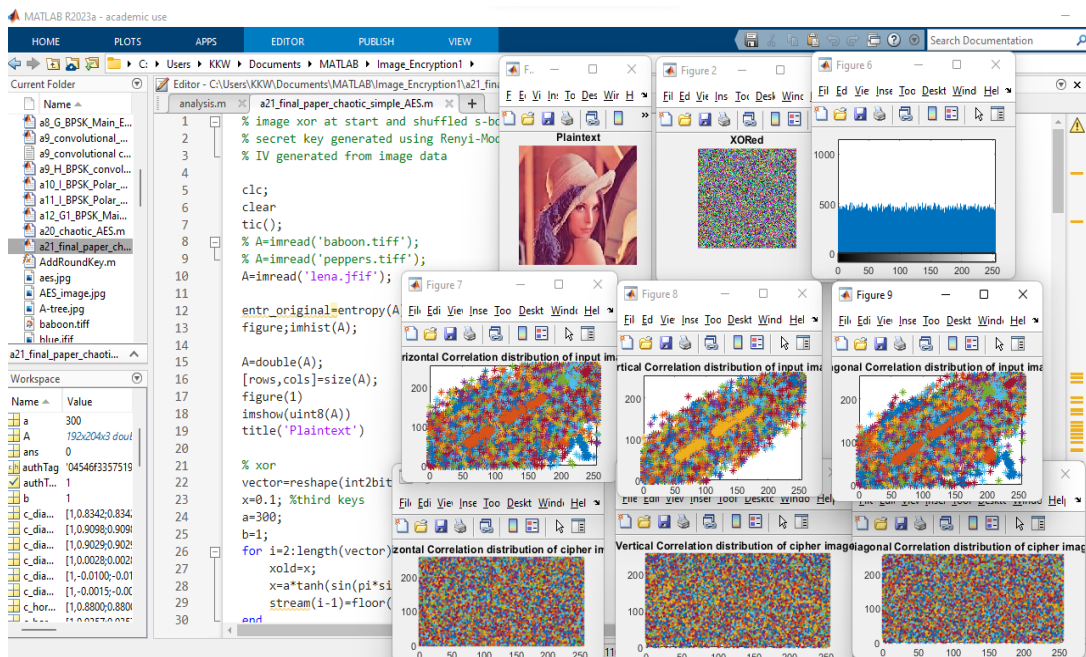


Figure 1. MATLAB simulation of color image encryption

**2.1. Chaotic sequence gen. using hyperbolic tangent map and XOR with input image**

Hyperbolic tangent map is used to generate the chaotic behavior. The research in [25], [26] demonstrates the use of hyperbolic tangent function to increase randomness in the image. This map is used to generate random stream of bits. Instead of using just present value  $x_n$  to generate sequence, past two values,  $x_n$  and  $x_{n-1}$  of chaotic map are used because the performance of this method is verified using NIST tests in [27]. Algorithm of generating bit stream for XOR operation:

- a) Read the color image I with size (M, N, 3).
- b) Generate a vector A of length  $M \times N \times 3$  and convert integers with values [0; 255] to bits.
- c) Calculate length of vector A as  $\text{len}(A)$ . Initialize the chaotic keys  $a=300$ ,  $b=1$  and  $x_0 = 1$ .
- d) Iterate the following steps  $\text{len}(A)$  times, where a, b and  $x_0$  are the initial parameters.  $x_n$  and  $x_{n-1}$  are the chaotic map values.  $[x]$  indicates the nearest integer less than or equal to x.

$$\left. \begin{aligned} x_n &= a \tanh(\sin(\pi \sin(\pi x_{n-1}))) + b \\ \text{Bit}_i &= [\text{mod}(x_n \times x_{n-1}, 2)] \end{aligned} \right\} n = 2, 3, \dots, [\text{len}(A) + 1] \tag{1}$$

- e) XOR generated bit stream with the image vector of step 2.
- f) Provide the resultant vector  $I_{\text{XORed}} = (A \oplus \text{Bit}_i)$  for AES encryption.

## 2.2. Key K1 generation using robust Renyi modulo map

Chaotification can be applied to any one-dimensional map to increase its complexity by involving the remainder operator. The resulting map can achieve increased statistical randomness [28], [29]. Moysis *et al.* [30], stated the bit generator using nonlinear hashing is proved to provide resistance to brute force attacks because of its sufficiently high key space. So, it is used here to generate 256-bit chaotic AES key. Robust Renyi modulo map is used as a source for the bit generator. The initial variables used are:  $a=5$ ,  $b=7$ ,  $r=10$ ,  $k = 9.99$  with  $x$  ranging in  $[0, 1)$ .

$$\text{For } i = 1 \text{ to } \lceil \text{key\_length}/64 \rceil : \quad (2)$$

$$\begin{aligned} M &= \text{mod}(r \times x, 1) \\ x &= \text{mod}(x + a + b \times M, 1) \end{aligned} \quad (3)$$

$$B_1 = \text{int\_to\_bits}[\text{rem}([10^{10} \times M], 2^{32}), 32] \quad (4)$$

$$B_2 = \text{int\_to\_bits}[\text{rem}([10^{10} \times x], 2^{32}), 32] \quad (5)$$

$$\text{Final\_64\_bits} = [B_1, B_2] \quad (6)$$

## 2.3. Generation of initialization vector

The IV is generated from the image pixel values and dimensions. Thus, a totally different value will be generated for every image even with same dimensions. This method can also be used to generate initial key of hyperchaotic system [17]. Algorithm to generate 96 bit IV from input image:

- Accept the color image I as the input.
- Get the height (M) and width (N) of the plaintext image I (image dimensions:  $M \times N \times 3$ ).
- Convert the image array to a vector V. Assign  $I_{IV}$ , length of IV as 96.
- Calculate  $\frac{\sum_{i=1}^{M*N} V(i) + (M*N)}{2^{23} + (M*N)}$  from the image, where, V(i) are image pixel values.
- Multiply it with the constant  $10^{10}$ .
- To convert the values within range of 0 to 255, divide by 256 and find the remainder.
- Iterate the process ( $I_{IV}$ ) times and convert the result to bit stream of 96 bits.
- Convert the binary vector to hex and provide as IV.

Final IV obtained can be given as

$$IV = \text{Integer\_to\_bitstream} \left[ \text{Mod} \left( \left( \frac{\sum_{i=1}^{M*N} V(i) + (M*N)}{2^{23} + (M*N)} * 10^{10} \right), 256 \right) \right] \quad (7)$$

## 2.4. S-box shuffling

The use of basic and modified Arnold cat map can be observed in previous research [10], [24]. It is used to randomly rearrange the original substitution box of AES. Arnold cat map can be represented using:

$$a = 13 + \text{mod}(T, 29) \quad (8)$$

$$b = 7 + \text{mod}(T, 47) \quad (9)$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & (a \times b) + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ mod } 16 \quad (10)$$

Where, T is sum of all s-box values. Original position is  $(x, y)$  and the shifted position will be  $(x', y')$ .

Diffusion and confusion operations are essential for cryptographic algorithms to achieve high security. To encrypt the block of data, each basic round of AES uses the following four transformations as shown in Figure 3: byte substitution using shuffled s-box, based on a matrix to replace a byte with another data. Cyclic shift of rows, which involves shifting of bytes of the state cyclically to the left as per row number. Mixing columns, column-wise multiplication and addition with round key. Multiple similar rounds are incorporated in AES encryption. The core function in AES-GCM is Galois counter (GCTR), which is presented in Figure 4.

**2.5. Algorithm for overall encryption**

- a) Read the color image I with size (M, N, 3).
- b) Initialize the keys for chaotic maps and set authentication tag bit-length (96 bits).
- c) Generate the random bit stream and XOR it with image vector to increase randomness before actual encryption (shown in Figure 2) (explained in section 2.1).

$$I_{XORed} = (I \oplus Bit) \tag{11}$$

- d) Generate secret key  $K_1$  using Renyi-modulo map (section 2.2). Select 128 bit additional key  $K_2$  for AES.
- e) Generate chaotic IV is from the image pixel values and dimensions (section 2.3).
- f) Initialize the counter and concatenate generated IV with counter.  $P_0 = IV \parallel 0^{31}1$

$$P_i = increment(P_{i-1}), i = 1, 2, \dots, n \tag{12}$$

- g) Initialize the s-box and shuffle it using Arnold cat map (section 2.4). It will be used for AES encryption process (Figure 3).
- h) Generate hash sub-key using AES encryption of stream of 128 bit zeros (shown in Figure 5). Use secret key  $K_1$ . Encry (X, K) indicates AES encryption of the block X with the key K.

$$H = Encry(0^{128}, K_1) \tag{13}$$

- i) Provide secret key  $K_1$ , additional key  $K_2$ , image vector and P (from step 6) to GCTR function.
- j) GCTR includes (shown in Figure 4) ( $P_i$  is the IV with counter-generated in step 6):

$$\left. \begin{aligned} Y_i &= Encry(P_i, K_1, K_2) \\ Cipher_i &= I_{XORed_i} \oplus Y_i \end{aligned} \right\} i = 1, 2, \dots, n \tag{14}$$

- k) AAD, cipher text and lengths of both are authenticated using GHASH function. The concatenation of Cipher, len (Cipher), AAD and len (AAD) is divided in 128-bit blocks.

$$Auth\_data = AAD \parallel Cipher \parallel len(AAD) \parallel len(Cipher) \tag{15}$$

- l) GHASH includes (shown in Figure 5):

$$Auth\_out_i = Auth\_data_i \oplus (Auth\_data_{i-1} \times H) \tag{16}$$

$$Auth\_Tag = GCTR(Auth\_out_i, P_0, K_1, K_2) \tag{17}$$

Tag is also calculated at the receiver end using similar process and compared with the received tag. In case of mismatch, the decrypted data is discarded.

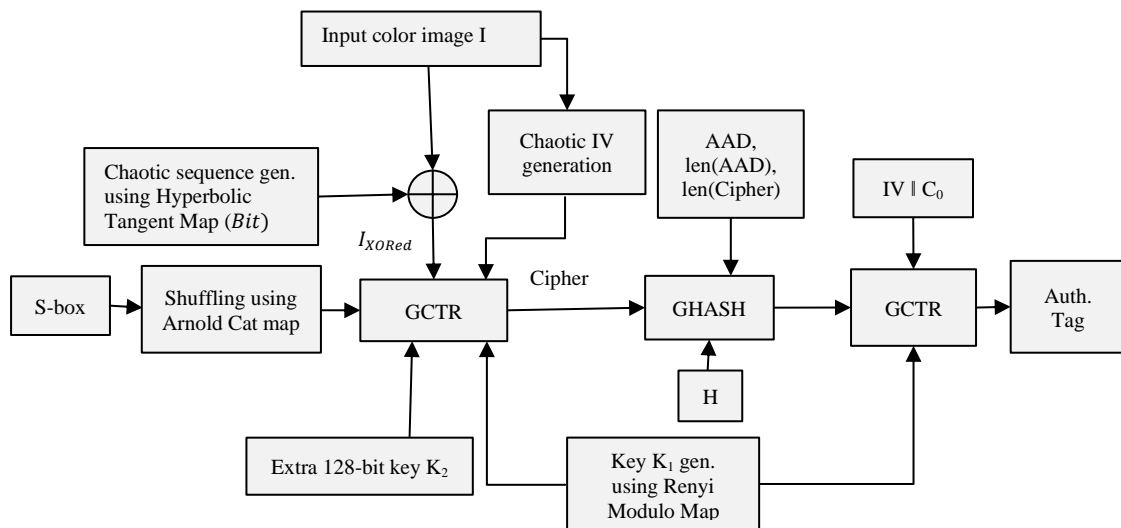


Figure 2. Authenticated encryption block diagram

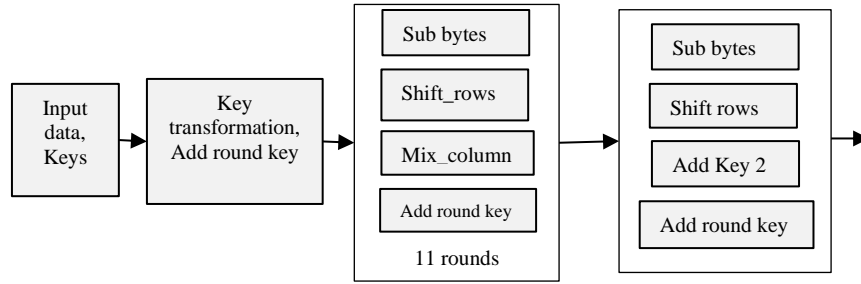


Figure 3. Advanced encryption standard encryption

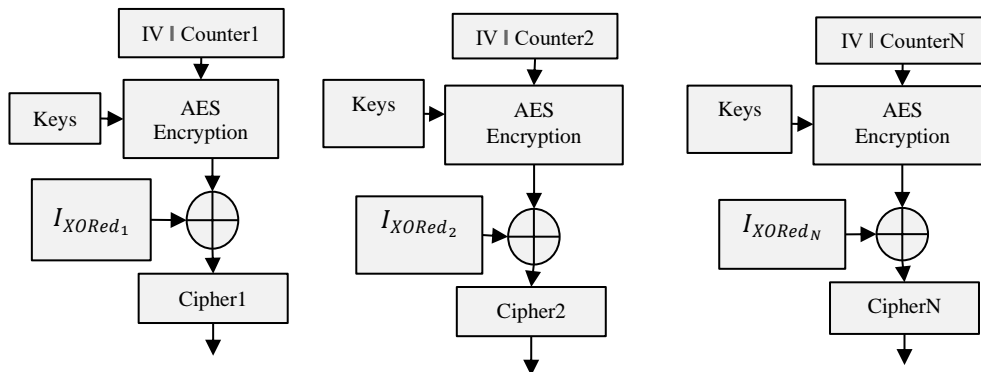


Figure 4. Galois counter (GCTR) block diagram

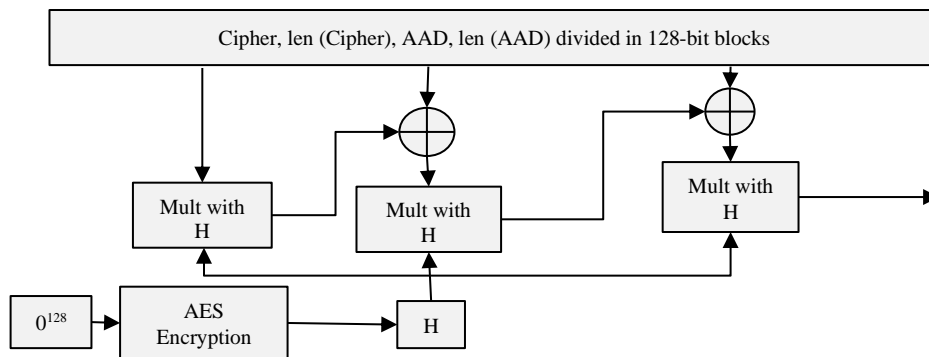


Figure 5. Galois hash (GHASH) generation for authentication

### 3. RESULTS AND DISCUSSION

The sample Lena, Pepper and Baboon images are taken from USC-SIPI database, because they are standard images used by most researchers. This section presents all details of the statistical parameters and the results obtained. The interpretation and the analysis are also presented.

#### 3.1. Histogram analysis

The intensity of pixels in an image is displayed through a histogram. The original and encrypted images as well as their histograms are presented in Figure 6. Figure 6(a) shows the actual images, Figure 6(b) includes their histograms, Figure 6(c) shows the cipher images, and associated histograms are added in Figure 6(d). As shown, the encrypted images are random and noisy. The histogram of the actual input image shows concentrations of pixels at specific levels and the histogram values of the encrypted output are uniform. Since the cipher image's histogram makes it difficult to anticipate the actual data, the method offers strong security against histogram attacks.

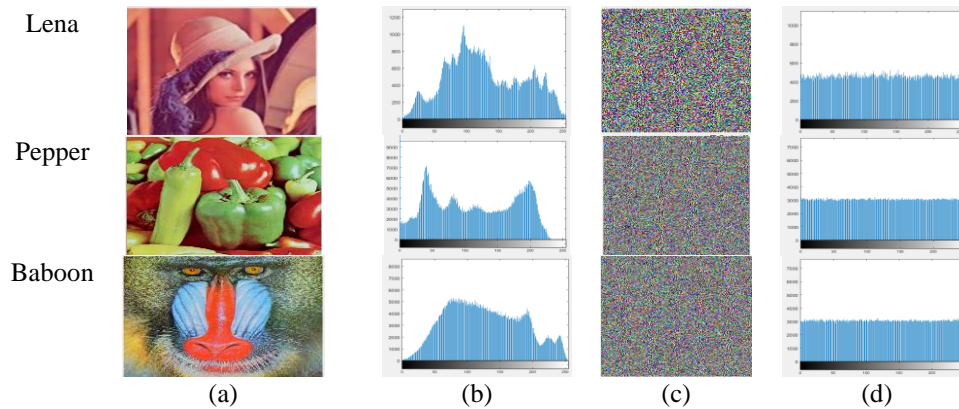


Figure 6. Original and encrypted images with their histograms: (a) input images (b) input image histograms (c) cipher images (d) cipher image histograms

**3.2. Information entropy**

Entropy H is the statistical parameter used to analyse confusion. It has a maximum value of 8. If M is the total count of pixels in the image, and  $p_i$  is the possibility of pixel redundancy, entropy can be given by

$$\text{Entropy } H = - \sum_{i=1}^M p_i \log p_i \tag{18}$$

As it can be seen from Table 1, the cipher image's entropy values are approaching 8. Thus, it proves that pixel values of cipher image are randomly distributed. So, it is quite difficult to derive the actual image from the cipher image.

**3.3. Analysis of encryption quality using maximum deviation**

Maximum deviation evaluates the difference in pixel values. For high security, plain and cipher images should be entirely different. So, the maximum deviation between input and cipher images should be high. High values for cipher images (232 to 254) as shown in Table 1 prove robustness of the algorithm against attacks. It is evaluated using:

$$\text{Max. Dev.} = \frac{D_0 + D_{255}}{2} + \sum_{i=1}^{254} D_i \tag{19}$$

where  $D_i$  is the difference in the histogram values between the input and the cipher images at index  $i$ .

**3.4. Frequency (Monobit) test suggested by NIST statistical test suite**

The randomness in the encrypted images can be measured using NIST statistical test suite. For the random sequence, p-value should be more than the significant level of 0.01. Our results are summarized in Table 1. The p-values ( $>0.01$ ) prove that our system is producing the cipher image with sufficient randomness.

Table 1. Entropy, maximum deviation, p-value analysis and MSE results

Sr. No.	Image	Entropy			Max. deviation		p-value (NIST test)	MSE for cipher images			MSE (Decry.)		
		R	G	B	Encry. images	Decry. images		R	G	B	R	G	B
1	Baboon	7.9993	7.9993	7.9993	253	0	0.5637	8.6518e+03	7.7439e+03	9.4968e+03	0	0	0
2	Pepper	7.9994	7.9993	7.9994	232	0	0.5637	8.0006e+03	1.1268e+04	1.1134e+04	0	0	0
3	Lena	7.9954	7.9960	7.9959	254	0	0.3173	1.0759e+04	8.9328e+03	7.1930e+03	0	0	0

**3.5. Analysis of mean square error**

Table 1 indicates mean square error (MSE) results for sample images. The Avalanche impact is assessed by MSE. It shows that even with minor changes to the input data or the key, the algorithm can yield a significant variation in the encrypted image. The high value between input and encrypted images (between  $7.1930e+03$  to  $1.1268e+04$ ) indicate dissimilarity between both [31]. Whereas, between input and decrypted images, MSE is zero indicating the extraction of correct original image without any loss [32]. If M and N are

the number of adjacent pixels in the images,  $Input\_image(i,j)$  and  $Cipher\_image(i,j)$  indicate input and encrypted image pixel values at location  $(i, j)$ , MSE can be calculated using:

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [Input\_image(i,j) - Cipher\_image(i,j)]^2}{M * N} \tag{20}$$

**3.6. Analysis of correlation coefficients**

To resist statistical attacks, adjacent pixels of encrypted image should be uncorrelated. Table 2 presents the correlation coefficients in horizontal, vertical, and diagonal directions. The values are between -1 and 1. The adjacent pixels of cipher images are weakly linked, so the values are close to zero. Figure 7 presents visual correlation distribution of Lena image. Figures 7(a)-(c) show horizontal, vertical and diagonal correlation analysis for original Lena image respectively. Figures 7(d)-(f) show horizontal, vertical and diagonal correlation analysis for encrypted image respectively. The scattered graphs for the cipher images demonstrate that this method offers strong resistance against attacks based on correlation.

Table 2. Correlation coefficient values for input and cipher images

Image	Channel of image	Correlation coefficients for input image			Correlation coefficients for cipher image		
		Hori.	Vert.	Diag.	Hori.	Vert.	Diag.
Baboon	R	0.9231	0.8660	0.8543	0.0025	-0.0005	-0.0013
	G	0.8655	0.7650	0.7348	-0.0005	-0.0016	-0.0011
	B	0.9073	0.8809	0.8399	-0.0010	0.0058	0.0001
Pepper	R	0.9635	0.9663	0.9564	-0.0003	-0.0012	-0.0003
	G	0.9811	0.9818	0.9687	0.0001	0.0036	0.0028
	B	0.9665	0.9664	0.9478	0.0001	0.0013	-0.0028
Lena	R	0.9317	0.9668	0.9029	0.0097	-0.0038	-0.0200
	G	0.9357	0.9692	0.9098	-0.0013	0.0078	-0.0017
	B	0.8800	0.9388	0.8342	0.0023	-0.0040	0.0071

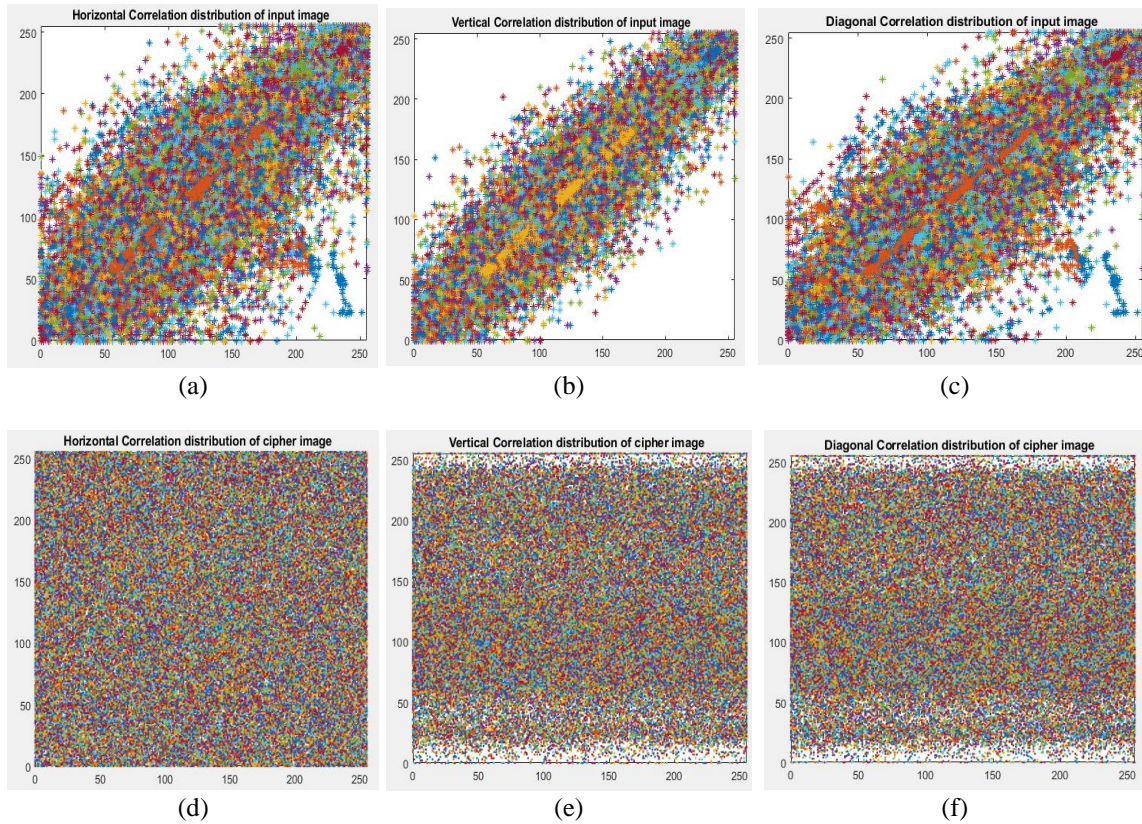


Figure 7. Visual correlation distribution of Lena image: (a) horizontal, (b) vertical, (c) diagonal correlation distribution for input image, (d) horizontal, (e) vertical, and (f) diagonal correlation distribution for cipher image



**3.7. Analysis of inconsistency of pixels using peak to signal noise ratio**

Table 3 shows PSNR values for encrypted and decrypted images. Lower (<10 dB) PSNR values obtained between the input and encrypted images indicate less noise ratio in encrypted images [24]. Thus, it is highly resistant to statistical attacks. The infinite values for decrypted images indicate that the image is reconstructed properly. PSNR is determined mathematically as [31]:

$$PSNR = 10 * \log_{10} \frac{(255)^2}{MSE} \text{ (dB)} \tag{21}$$

**3.8. Structural similarity index measure**

Structural similarity index measure (SSIM) compares two images based on three parameters: contrast, luminance and structure. SSIM=1 represents similarity between both images, while a value of 0 indicates that both images are different [32]. It ranges between 0 and 1. Table 3 represents SSIM values. Close to zero values for encrypted images and one for decrypted images prove the correctness of the algorithm.

**3.9. Key sensitivity analysis**

An encryption algorithm should have a key space of at least  $2^{100}$  to reduce risk of Brute-force attacks. Here the key space of  $2^{256}$  along with extra 128-bit key is used. The chaotic map parameters also serve as keys enhancing the security performance. Thus, the system is safe against brute-force attacks. For checking key sensitivity, 256-bit key is incremented by 1 and used for decryption. Thus, the key was modified by the factor of  $1/2^{256}$ . The image was not correctly decrypted using it. So, it can be concluded that the crypto system is secure even if the attacker has some partial information of the key.

Table 3. Analysis of inconsistency of pixels using PSNR and SSIM

Image	PSNR						SSIM					
	For encry. images			For decry. images			For encry. images			For decry. images		
	R	G	B	R	G	B	R	G	B	R	G	B
Baboon	8.7598	8.7731	8.7527	Infinite	Infinite	Infinite	0.0102	0.0088	0.0077	1	1	1
Pepper	9.0996	9.0941	9.1098	Infinite	Infinite	Infinite	0.0107	0.0086	0.0074	1	1	1
Lena	7.8132	7.8852	7.8560	Infinite	Infinite	Infinite	0.0082	0.0116	0.0099	1	1	1

**3.10. Discussion**

The authors in previous research mentioned that the major issues that the hybrid chaotic approaches must tackle is to maintain the picture attributes that are likely to be lost during decryption [7]. The proposed algorithm has achieved infinite PSNR for decrypted images. Thus, our method preserves image visual properties after encryption and achieves proper reconstruction of original image without any loss. Also, lower PSNR for cipher images and totally different histograms of actual and encrypted images prove that the algorithm is secure against statistical attacks [24]. Recent research [32], [33] including medical image encryption works on grayscale images. Our algorithm can be used in color images related applications too.

In the presented results, for every cipher image, the SSIM is extremely near to 0, the PSNR is below 10 dB, and the MSE is quite high. This indicates a substantial difference between the actual and cipher images. Thus, it is difficult to derive original data from the encrypted one. Also, for the decrypted images, the maximum deviation and MSE values are zero, the SSIM values are 1 and correlation coefficients are close to 0. These parameters prove a good reproduction of the decrypted images without loss. The results are in agreement with previous research works [24], [32].

Our algorithm enables great randomization of the image data by using various chaotic parameters as secret keys. The chaotic keys of initialization vector depend on original image parameters, making the algorithm resistant to differential attacks. The system performance is compared with previous research in Table 4. Table 5 compares the entropy values using different algorithms for the Lena image. Close to ideal entropy and lower correlation of cipher images achieved by our algorithm prove that it is providing higher security.

Future studies may explore the creation of crypto-coding algorithms combining error correcting channel codes with encryption. The security of our algorithm is verified using statistical parameters as done in [34], [35]. As AES-GCM [3] is already employed in security standards, the chaotic maps can be easily integrated for advanced applications.

Table 4. Comparison of results for Pepper image



Image	Ref.	Entropy			Correlation coefficients (Cipher image)		
		R	G	B	Vertical	Horizontal	Diagonal
	Proposed algorithm	7.9994	7.9993	7.9994	R: -0.0012 G: 0.0036 B: 0.0013	R: -0.0003 G: 0.0001 B: 0.0001	R: -0.0003 G: 0.0028 B: -0.0028
	[36]		7.9973		R: 0.0231 G: 0.0220 B: 0.0121	R: -0.0009 G: -0.0053 B: -0.0056	R: -0.0003 G: -0.0045 B: -0.0035
	[37]		7.9989		0.0020	-0.0035	0.0016
	[38]		7.9974		-0.0018	-0.0025	0.0030

Table 5. Comparison with previous work for Lena image

Image	References	R	G	B
	[39]		7.7228	
	[40]		7.9913	
	[41]	7.9913	7.9914	7.9916
	[16]	7.579	7.6321	7.5589
	[15]	7.7771	7.7190	7.7150
	Our method	7.9954	7.9960	7.9959

#### 4. CONCLUSION




The purpose of the presented research was to develop a novel image encryption scheme combining the chaos sequences with the improved Galois counter mode of AES to provide higher security with authentication. The chaotic algorithms are sensitive to initial conditions and control parameters, which are used as the keys of block encryption algorithms to make them resist the differential attacks. The crypto system is implemented and tested using various security parameters like entropy, histogram and mathematical as well as visual analysis of correlation. PSNR value and structural similarity index measure values demonstrate the robustness of the algorithm against statistical attacks. The NIST Frequency test of statistical test suite is also successful. The proposed crypto system is secure even if the attacker has partial knowledge of the key. Thus, the multi-chaotic AES-GCM provides high security against all differential, statistical and brute-force attacks. So, it is suitable for the confidential data transmission. As TLS 1.3 is declining support to non-authenticated encryption methods, the proposed algorithm with chaotic improvements can be easily adopted for data security with authentication. From the perspective of presented work, the authors plan to implement the hyperchaotic maps with block codes. The error correcting codes can also be combined with encryption algorithm in future to enhance the performance.

#### REFERENCES




- [1] S. Das and S. Namasudra, "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure," *Computers and Electrical Engineering*, vol. 101, p. 107991, Jul. 2022, doi: 10.1016/j.compeleceng.2022.107991.
- [2] E. Rescorla, "The transport layer security (TLS) protocol version 1.3," Aug. 2018, doi: 10.17487/RFC8446.
- [3] M. Dworkin, "SP 800-38D: recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," *NIST Special Publication*, vol. 800, no. 38D, pp. 1–39, 2007.
- [4] J. Viega and D. McGrew, "The use of Galois/counter mode (GCM) in IPsec encapsulating security payload (ESP)," RFC 4106, Network Working Group, Jun. 2005, doi: 10.17487/rfc4106.
- [5] J. S. Baladhay and E. M. De Los Reyes, "AES-128 reduced-round permutation by replacing the MixColumns function," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1641–1652, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1641-1652.
- [6] R. V Chothe, S. P. Ugale, D. M. Chandwadkar, and S. V Shelke, "A combined cryptography and error correction system based on enhanced AES and LDPC," in *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, Aug. 2023, pp. 1–6, doi: 10.1109/ICCUBEA58933.2023.10392218.
- [7] A. S. Bader and A. M. Sagheer, "Modification on AES-GCM to increment ciphertext randomness," *International Journal of Mathematical Sciences and Computing*, vol. 4, no. 4, pp. 34–40, Nov. 2018, doi: 10.5815/ijmsc.2018.04.03.
- [8] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *Journal of Information Security and Applications*, vol. 54, p. 102566, Oct. 2020, doi: 10.1016/j.jisa.2020.102566.
- [9] S. J. Sheela, K. V Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25223–25251, Oct. 2018, doi: 10.1007/s11042-018-5782-2.
- [10] C. Chen, H. Zhang, and B. Wu, "Image encryption based on Arnold transform and fractional chaotic," *Symmetry*, vol. 14, no. 1, p. 174, Jan. 2022, doi: 10.3390/sym14010174.
- [11] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2753–2772, 2021, doi: 10.1007/s11042-020-09648-1.
- [12] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020, doi: 10.1109/ACCESS.2020.2971759.

- [13] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Optics and Lasers in Engineering*, vol. 134, 2020, doi: 10.1016/j.optlaseng.2020.106202.
- [14] B. Mondal and J. P. Singh, "A lightweight image encryption scheme based on chaos and diffusion circuit," *Multimedia Tools and Applications*, vol. 81, no. 24, pp. 34547–34571, 2022, doi: 10.1007/s11042-021-11657-7.
- [15] O. S. Faragallah *et al.*, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2019, doi: 10.1109/ACCESS.2018.2879857.
- [16] O. S. Faragallah *et al.*, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3–4, pp. 2495–2519, 2020, doi: 10.1007/s11042-019-08190-z.
- [17] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11837–11857, 2020, doi: 10.1007/s00521-019-04667-y.
- [18] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electronics (Switzerland)*, vol. 10, no. 9, 2021, doi: 10.3390/electronics10091066.
- [19] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iiyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Information Sciences*, vol. 515, pp. 191–217, 2020, doi: 10.1016/j.ins.2019.10.070.
- [20] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 4, pp. 1637–1657, 2019, doi: 10.1007/s11045-018-0622-0.
- [21] C. H. Lin, G. H. Hu, C. Y. Chan, and J. J. Yan, "Chaos-based synchronized dynamic keys and their application to image encryption with an improved aes algorithm," *Applied Sciences (Switzerland)*, vol. 11, no. 3, pp. 1–16, 2021, doi: 10.3390/app11031329.
- [22] K. Assa-Agyei, K. Owa, F. Olajide, and T. Al-Hadhrami, "A multi-chaotic key expansion for advanced encryption standard (AES) algorithm," in *2024 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2024, pp. 1–7, doi: 10.1109/ICNC59896.2024.10556263.
- [23] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1708–1723, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.
- [24] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *Journal of Imaging*, vol. 8, no. 6, p. 167, Jun. 2022, doi: 10.3390/jimaging8060167.
- [25] N. Jiteurragool, T. Masayoshi, and W. San-Um, "Robustification of a one-dimensional generic sigmoidal chaotic map with application of true random bit generation," *Entropy*, vol. 20, no. 2, 2018, doi: 10.3390/e20020136.
- [26] G. Ablay, "Chaotic map construction from common nonlinearities and microcontroller implementations," *International Journal of Bifurcation and Chaos*, vol. 26, no. 7, 2016, doi: 10.1142/S0218127416501212.
- [27] L. Moysis, I. Kafetzis, C. Volos, A. V. Tutueva, and D. Butusov, "Application of a hyperbolic tangent chaotic map to random bit generation and image encryption," *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, pp. 559–565, 2021, doi: 10.1109/ElConRus51938.2021.9396395.
- [28] L. Moysis, I. Kafetzis, M. S. Baptista, and C. Volos, "Chaotification of one-dimensional maps based on remainder operator addition," *Mathematics*, vol. 10, no. 15, 2022, doi: 10.3390/math10152801.
- [29] L. Moysis, M. Lawnik, I. P. Antoniadis, I. Kafetzis, M. S. Baptista, and C. Volos, "Chaotification of 1D maps by multiple remainder operator additions—application to B-spline curve encryption," *Symmetry*, vol. 15, no. 3, 2023, doi: 10.3390/sym15030726.
- [30] L. Moysis, M. Lawnik, M. S. Baptista, C. Volos, and G. F. Fragulis, "A family of 1D modulo-based maps without equilibria and robust chaos: application to a PRBG," *Nonlinear Dynamics*, vol. 112, no. 14, pp. 12597–12621, 2024, doi: 10.1007/s11071-024-09701-w.
- [31] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004, doi: 10.1109/TIP.2003.819861.
- [32] S. Dib, A. Benchiheb, and F. Benmeddour, "A new 6D hyperchaos-based medical image encryption scheme using k-Fibonacci numbers," *International Journal of Electrical and Electronic Engineering and Telecommunications*, vol. 13, no. 2, pp. 148–159, 2024, doi: 10.18178/ijeetc.13.2.148-159.
- [33] Y. S. Najaf and M. K. Mahmood Al-Azawi, "Public key cryptosystem based on multiple chaotic maps for image encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, p. 1457, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1457-1466.
- [34] A. Gaffar *et al.*, "A technique for securing multiple digital images based on 2D linear congruential generator, silver ratio, and Galois Fieldet," *IEEE Access*, vol. 9, pp. 96125–96150, 2021, doi: 10.1109/ACCESS.2021.3094129.
- [35] A. Gaffar, A. B. Joshi, D. Kumar, and V. N. Mishra, "Image encryption using nonlinear feedback shift register and modified RC4A algorithm," *Journal of Applied Mathematics and Informatics*, vol. 39, no. 5–6, pp. 859–882, 2021, doi: 10.14317/jami.2021.859.
- [36] D. Kumar, A. B. Joshi, S. Singh, and V. N. Mishra, "Digital color-image encryption scheme based on elliptic curve cryptography ElGamal encryption and 3D Lorenz map," *AIP Conference Proceedings*, vol. 2364, 2021, doi: 10.1063/5.0062877.
- [37] D. F. Chalob, A. A. Maryoosh, Z. M. Esa, and E. N. Abbud, "A new block cipher for image encryption based on multi chaotic systems," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, p. 2983, Dec. 2020, doi: 10.12928/telkommika.v18i6.13746.
- [38] D. Kumar, A. B. Joshi, and V. N. Mishra, "Optical and digital double color-image encryption algorithm using 3D chaotic map and 2D-multiple parameter fractional discrete cosine transform," *Results in Optics*, vol. 1, p. 100031, Nov. 2020, doi: 10.1016/j.rio.2020.100031.
- [39] L. Coulbaly, F. Ouallouche, and V. Oduol, "Joint cryptography and channel-coding based on low-density parity-check codes and advanced encryption standard for 5G systems," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 10, no. 6, pp. 397–406, 2021, doi: 10.18178/ijeetc.10.6.397-406.
- [40] P. Liu, T. Zhang, and X. Li, "A new color image encryption algorithm based on DNA and spatial chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 14823–14835, 2019, doi: 10.1007/s11042-018-6758-y.
- [41] A. Kadir, M. Aili, and M. Sattar, "Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections," *Optik*, vol. 129, pp. 231–238, 2017, doi: 10.1016/j.jleo.2016.10.036.




**BIOGRAPHIES OF AUTHORS**

**Rupaliben V. Chothe**    is working as an Assistant Professor in Electronics and Telecommunication Engineering Department of K. K. Wagh Institute of Engineering Education and Research, Nashik, Maharashtra since last 16 years. She is pursuing Ph.D. in Electronics and Telecommunication from Savitribai Phule Pune University. She can be contacted at email: rvchothe@kkwagh.edu.in.






**Dr. Sunita P. Ugale**    is working as a Professor in Electronics and Telecommunication Engineering Department of K. K. Wagh Institute of Engineering Education and Research, Nashik, Maharashtra since last 28 years. She holds Ph.D. degree and her special fields of interest include fiber optics communication, optical sensors, automation, and VLSI technology. She can be contacted at email: spugale@kkwagh.edu.in.



**Dr. Dinesh M. Chandwadkar**    is a Professor and head of E & TC Department at K. K. Wagh Institute of Engineering Education and Research, Nashik, India. His area of interest includes signal processing, power electronics, mechatronics, and automotive electronics. He holds Ph.D. degree and he has published More than 50 research papers in reputed journals. He is working as Board of Studies member of Electronics and Telecommunication Engineering for Pune University. He can be contacted at email: dmchandwadkar@kkwagh.edu.in.



**Shraddha V. Shelke**    is working as an Assistant Professor in Electronics and Telecommunication Engineering Department of K. K. Wagh Institute of Engineering Education and Research, Nashik. She is perusing her Ph.D. in Electronics and Telecommunication from Savitribai Phule Pune University. She can be contacted at email: svshelke@kkwagh.edu.in.