IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13444

Enhanced Image Security Using Chaos and DNA Coding

Hrishikesava Reddy C[1], Shanthan Kumar S[2], Sadaf G[3], Nagraju M R[4], Sneha Latha P[5]

Assistant Professor, Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, India[1]

Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, India[2-5]

Abstract: In todays realm cryptography plays a role, across various sectors. Image encryption stands out as an aspect in safeguarding data due to its ranging applications in areas like defense, multimedia, healthcare and more. This article introduces an image encryption technique designed for both grayscale and color images using the Tangential Delay Ellipse Reflecting Curve System (TD ERCS) chaotic map system and DNA coding. The chaotic map is employed to shuffle positions for confusion and mask image creation while DNA coding alters pixel values for diffusion. Through evaluation the proposed method demonstrated high mean square error and low peak signal to noise ratio, near zero correlation, a high rate of pixel changes consistent average intensity value changes, as well as resilience, against noise and data loss attacks. Furthermore decryption can be carried out without compromising the image quality.

Keywords: Image encryption, Color image, Chaotic map, DNA coding, AES, IDEA, DES

I. INTRODUCTION

As the Internet advances rapidly individuals rely on it for exchanging information in aspects of their lives and professions. The visual appeal and easy recollection of images have made them a prevalent choice, for conveying information.

Nowadays digital transformation has made it common to digitize images for sharing and saving on the web. However these digital images are vulnerable to misuse by actors who may copy, delete or alter them without security measures, in place.

With the daily advancement of technology, images are employed extensively across all domains. For the storage and transfer of images, a strong and effective cryptographic technique is therefore necessary. The current encryption methods, such as DES and AES, do not meet the criteria for picture encryption because of their low efficiency and security performance metrics. [3–6].

Multimedia communication heavily relies on digital pictures, thus it's imperative that the right safeguards are in place to preserve this data. Images may be safely encrypted and protected to some extent using conventional block encryption techniques like DES, IDEA, and AES. They are unable to shield digital images from transmission noise, which might be added during the transmission process. [1]

The swift advancement of multimedia and network technologies has led to the widespread use of digital image processing in several domains like remote sensing, industrial inspection, medical field, meteorology, communications, reconnaissance, and intelligent robotics. Consequently, picture information has received more attention. Furthermore, safeguarding the security of picture data is more crucial than ever, particularly in the domains of the military, business, and medicine. [2]-[7]

It is nearly hard to totally prevent data streaming by satellite and internet connection from being eavesdropped on. Data must thus be safe, especially multimedia data that comes from sensitive institutions like the military, the medical field, etc. Generally speaking, there are two types of picture encryption: digital and optical.

In the former, physical systems for image encryption are constructed using optical instruments, and the technique typically uses optics to randomize the frequency components of a picture. The latter often begins with a digital image and encrypts it using either hardware (a physical electrical device) or software that implements an encryption algorithm.

DOI: 10.17148/IJARCCE.2024.13444

The most popular encryption and security solutions are digital in nature as contemporary communication networks are becoming more and more digital in form. Because chaotic systems are characterized by ergodicity, sensitivity to beginning circumstances, and random-like behaviors, the chaos-based image encryption approach is therefore seen to be a good option for encryption purposes among the different digital picture encryption techniques. Numerous inventions based on chaos have surfaced, such as new diffusion methods, permutation techniques, hyperchaotic map systems, and simultaneous picture encryption that can be decoded without the need for a secret key. [2]

This paper introduce-s a new way to protect grayscale and color image-s from security issues. It uses a chaotic syste-m called the Tangential De-lay Elliptic Reflection Curve Syste-m (TD ERCS) and DNA encryption. This combination offers strong encoding while- preserving the quality and accuracy of the- images. The rest of paper is organized as follows. Section II our contribution Section III Background and Related Work Section III Proposed Methodology. Section IV . Experimental Results and Analysis. Finally, SectionV concludes our work.

II. OUR CONTRIBUTION

We present the use of DNA coding in conjunction with the Tangential Delay Ellipse Reflecting Curve System (TD ERCS) chaos mapping technique for picture encryption. This novel method increases security and durability by combining DNA encoding with chaotic mapping methods to create a two-layer encryption scheme. We describe a comprehensive encryption system that uses chaotic maps for confusion and DNA coding for propagation. Additionally, we evaluate the encryption method using a variety of parameters, demonstrating its effectiveness in terms of security, stability, and computational economy.

III. BACKGROUND AND RELATED WORK

A. Chaotic Maps in Image Encryption

Since their inherent properties such as ergodicity pseudorandom behavior and responsiveness to initial conditions the use of chaotic maps in image encryption has become widespread. Due to their complexity and randomness these maps are suitable for cryptography. The encryption of images has been the focus of research using a variety of chaotic systems such as the logistic map Lorenz system henon map and the tangential delay ellipse reflecting curve system td ercs. [3] [5]

The chaotic map used in this paper is:-

The TD-ERCS is a type of map that is two-dimensional and chaotic. It is used to change the order of images in both rows and columns. This system meets several important requirements, such as having no correlation in the total field and equal probability for all outcomes, resulting in chaotic random number generation with enhanced security features like Sensitivity to Initial Conditions (SDIC), ergodicity, deterministic pseudo-randomness, and structural complexity. Nowadays, there are many digital images in different fields because of new computer networks and tools. This makes it very important to keep the data safe when sending it. , Ciphers like DES, IDEA, and AES, which were mainly created for text or general binary sequences, are not the best choice for encrypting images because they take a long time to run and are vulnerable to security problems caused by strong connections between image pixels.

$$\begin{cases} X_n = -\dfrac{2k_{n-1y_{n-1}} + x_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2} \\ K_n = \dfrac{2k'_{n-m} - k_{n-1} + k_{n-1}k'^{\,2}{}_{n-m}}{1 + 2k_{n-1}k'_{n-m} - k'^{\,2}_{n-m}} \end{cases} \qquad n = 1,2,3..$$

where

$$k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m \end{cases}$$

$$y_n = k_{n-1}(x_n - x_{n-1}) + y_{n-1}$$

$$y_0 = \mu\sqrt{1 - x_0^2}$$

$$k_0^1 = -\frac{x_o}{y_o}\mu$$

$$k_0 = -\frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha}$$

where, μ, x0, α and m are TD-ERCS seed parameters and $0 < \mu \leq 1$, $-1 \leq x0 \leq 1$, and $0 < \alpha < \pi$.

The Tangential Delay Ellipse Reflecting Curve System (TD ERCS) is a chaotic map system that is well-known for its complex behavior and high sensitivity to initial conditions. TD ERCS has been successfully applied to increase image encryption's security and unpredictability. Encryption methods may effectively produce confusion and diffusion operations by taking use of the chaotic character of TD ERCS. This enhances the overall security of the encrypted picture. [11]-[17]

B. DNA Coding in Cryptography

An important biological feature found in almost all living organisms, it contains instructions for inherited traits passed from parents to their offspring In humans, DNA has a helical shape and four bases: A, C, G, and T. Watson and Crick discovered in 1953 that the DNA Law is that A and T are combined and G is DNA coding uses the double helix structure of DNA, of which nucleotides are the major component. Four nucleotides: adenine, guanine, cytosine, and thymine are the building blocks of DNA sequence. Adenine always binds thymine, and guanine always binds cytosine. Each base in a DNA alphabet is represented by two two-digit numbers, increasing the number of possible combinations from 24 to eight, due to overlapping relationships[6]. Considerable progress has been made in DNA computing, which has led to the development of new techniques for performing physical algebraic operations on DNA sequences, such as the XOR operation Like traditional XOR operations on binary sequences, this operation operates on DNA sequences based on eight DNA XOR rules. [11]

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
G	11	11	10	10	01	01	00	00
T	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Figure 3.1 DNA encoding rules

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
T	C	T	A	G
C	T	C	G	A

Figure 3.2 DNA XOR operations

C. Hybrid Encryption Techniques

In the past several years, hybrid techniques for picture encryption have gained popularity. To increase security, they incorporate several cryptographic primitives. Hybrid methods sometimes combine standard encryption algorithms such as AES, IDEA, or DES with chaotic maps like TD ERCS to mitigate the drawbacks of individual solutions. Hybrid algorithms combine the benefits of chaotic systems with conventional encryption techniques. [16]

D. Limitations of Existing Methods

Existing image encryption techniques offer promising results, but they also have some drawbacks, including susceptibility to statistical attack, key space consumption, and computational overheads. Fixing these drawbacks remains one of the most important areas of research in image encryption, which drives the development of new techniques that provide enhanced security and efficiency. [12]

The literature review provides an overview of existing encryption methods, focusing on perturbation-based methods and DNA coding applications. Chaos-based encryption techniques use chaotic structures such as ergodicity and sensitivity to initial conditions to enhance security. Classic encryption schemes such as DES and IDEA emphasize scalability rather than scalability, while recent advances explore how to use a combination of flexibility and breadth to improve security and performance. [15]

DOI: 10.17148/IJARCCE.2024.13444

The tangent delay elliptic reflective curve system (TD-ERCS) emerges as a promising chaos mapping system suitable for image storage, offering features such as total area zero correlation and even probability distribution.

The need for image encryption to ensure data privacy, especially in the case of digital image communications across public channels, highlights the need for robust encryption techniques Odicity, means performance promising with properties such as quasi-randomness.

IV. PROPOSED METHODOLOGY

A. Block Diagram

The working mechanism of system is shown below:

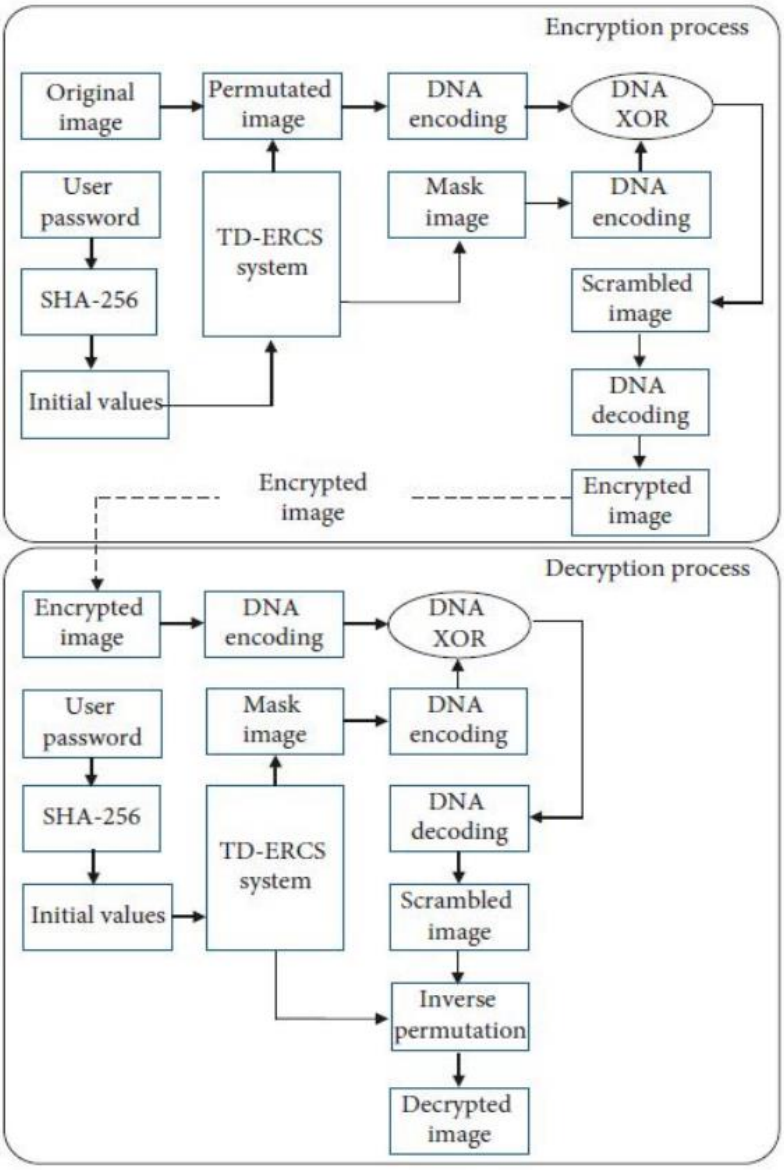

Figure 4. 1:Encryption and Decryption Flowchart

The algorithm for encryption and decryption involves generation of chaotic sequences using TD-ERCS. The chaotic sequences are used for pixel-position scrambling and creation of mask images which is DNA X-ORed with the pixel scrambled image for pixel substitution. s of the encryption and decryption processes are listed below. The flowchart for the scheme is given in above figure.

DOI: 10.17148/IJARCCE.2024.13444

B. Key Generation

The proposed encryption scheme employs a user's password to generate secret keys. SHA-256 is used to generate a message digest of 256-bits for the password. The 64 hash values of the message digest are then divided into eight hexadecimal groups: k1, k2, . . ., k8.

Each group contains eight hexadecimal values and is converted into a floating decimal number via the following equation:

$$d_j = \frac{\text{hex2dec}(\text{k}1, \text{k}2, \dots, \text{k}8)}{2^{10}}$$

where, j = 1, 2, 3, ... 8. The first set of the TD-ERCS initial values, (μ, x0, α and m) for the TD-ERCS system is calculated by:

$x_0 = sign(d1 - d2) \times d1 \bmod 1$
$\mu = d2 \bmod 1$
$\alpha = d3 \bmod \pi$
$m = d4 \bmod 10$

The second set of initial values (μ, x0,α and m) for the TD-ERCS system is calculated by:

$x0 = sign(d1 - d2) \times d5 \bmod 1$
$\mu = d6 \bmod 1$
$\alpha = d7 \bmod \pi$
$m = d8 \bmod 10$

Figure 4.2:Original Image

C. Encryption Algorithm

The process of encryption involves the following steps:

1. Conversion of the original color image to three matrices: R(m, n), G(m, n), and B(m,n).

2. Check if R, G and B matrices are same or not by comparing corresponding values of each position of R, G and B matrices.

DOI: 10.17148/IJARCCE.2024.13444

If (R,G and B matrices are identical to each other):

The image is grayscale.

Else:

The image is color image.

3. Generation of a pair of chaotic sequences,
xnew = (x1, x2, ..., xm) and ynew = (y1, y2, ..., yn), via a TD-ERCS chaotic map. This uses the starting values μ, x0, α and m

4. Arrange the sequences xnew and ynew in ascending order and record their locations:-

Index 1 = {i1, i2, ..., im}
Index 2 = {j1, j2, ..., jn}

The objective of this step is to find the index of the smallest number from the sequence with size m and then store it in i1, second smallest to i2.

Similarly, we can obtain index array Index 2 by arranging the sequence ynew in ascending order and taking its index.

5. Using the Index 1 we shuffle the pixels row-wise and column-wise pixel shuffling is done using Index 2. This is done for all the matrices R,G and B from which we get Rnew, Gnew and Bnew.

6. Conversion of Rnew , Gnew , and Bnew to binary matrices. DNA encoding is then employed to encode these binary matrices.

7. Generation of three chaotic sequences xn = (x1, x2, ..., xmn) and yn = (y1, y2, ..., ymn), and zn = (z1, z2, ..., zmn) via a TD-ERCS chaotic map. This uses the starting values of the second set, (μ, x0,α and m).Then, these generated values are converted into a range from 0 to 256 according to:

$x_e(k) = \text{round}(\text{abs}(x_i(k)) \times 1000 \bmod 256)$,
$y_e(k) = \text{round}(\text{abs}(y_i(k)) \times 500 \bmod 256)$,
$z_e(k) = \text{round}(\text{abs}(z_i(k)) \times 1000 \bmod 256)$,

where k ranges from 0 to M × N. Thus, the mask image is generated.

8. Conversion of xe, ye and ze to binary matrices. DNA encoding is then employed to encode these matrices. This results in three remodeled coding matrices:

xdna, ydna, and zdna sized (m, n×4).

9. (a) For color image:

Execution of the DNA XOR operation among (Rdna and xdna) , (Gdna and ydna) ,and (Bdna and zdna) . Three encrypted matrices are produced as a result: Rc, Gc, and Bc.

(b) For grayscale image:

The DNA XOR operation between (Rdna and xdna), (Gdna and xdna), and (Bdna and xdna) is executed for the grayscale picture. Three encrypted matrices are produced as a result: Rc, Gc, and Bc.

10. Generation of the final encrypted image by performing a DNA decoding operation for Rc, Gc, and Bc. This results in three new matrices with values ranging from 0 to 255: Renc, Genc, and Benc.

The three matrices Renc, Genc, and Benc are combined to get the encrypted image.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13444

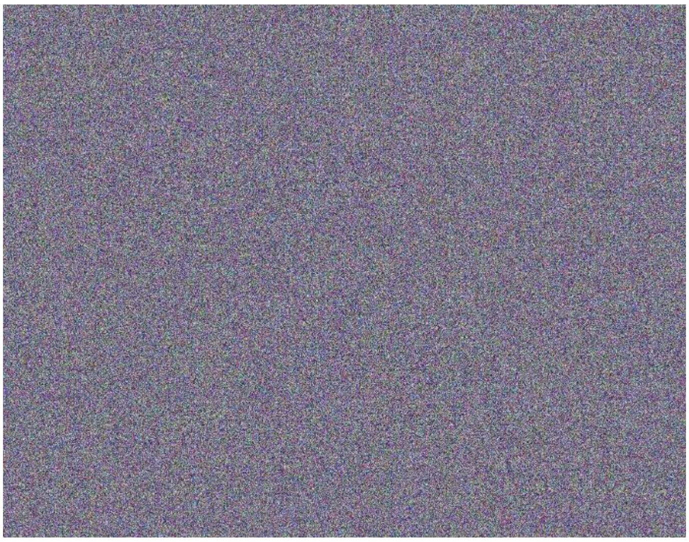

Figure 4. 3:Encrypted Image

D. Decryption algorithm
The process of decryption involves the following steps:

1. Conversion of the encrypted color image to three matrices: R(m, n), G(m, n), and B(m,n).

2. Check if R, G and B matrices are same or not by comparing corresponding value of each position of R, G and B matrices.
If (R,G and B matrices are identical to each other):
The image is grayscale.
Else:
The image is color image.

3. Conversion of R, G, and B to binary matrices. DNA encoding is then employed to encode these binary matrices, as detailed in table. This results in three remodeled coding matrices: Rdna, Gdna, and Bdna sized (m,n×4).

4. Generation of three chaotic sequences xi = (x1, x2, ..., xmn) and yi = (y1, y2, ..., ymn),and zi = (z1, z2, ..., zmn) via a TD-ERCS chaotic map. This employs the starting values of the second set, x0,α and m. The generated values are then converted into range of 0 to 256 according to:

$x_e(k) = \text{round}(\text{abs}(x_i(k)) \times 1000 \bmod 256)$,
$y_e(k) = \text{round}(\text{abs}(y_i(k)) \times 500 \bmod 256)$,
$z_e(k) = \text{round}(\text{abs}(z_i(k)) \times 1000 \bmod 256)$,

where k ranges from 0 to M × N. Thus, the mask image is generated.

5. Conversion of xe, ye and ze to binary matrices. Then, DNA encoding is employed to encode these matrices. This results in three remodeled coding matrices:
xdna, ydna, and zdna sized (m,n×4)

6. (a) For color image:
Execution of the DNA XOR operation among (Rdna and xdna) , (Gdna and ydna) ,
and (Bdna and zdna) . This results in three encrypted matrices: Rd, Gd, Bd.

(b) For grayscale image:
Execution of the DNA XOR operation among (Rdna and xdna) , (Gdna and xdna) , and (Bdna and xdna) . This results in three encrypted matrices: Rd, Gd, Bd.

7. Generation of a pair of chaotic sequences, xnew = (x1, x2, ..., xm) and ynew = (y1, y2, ..., yn), via a TD-ERCS chaotic map. This uses the starting values μ, x0,α and m .

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13444

8. Arrange the sequences xnew and ynew in ascending order and record their locations[15]:-

Index 1 = {i1, i2, ..., im}
Index 2 = {j1, j2, ..., jn}

The index of the smallest number from the sequence with size m is stored in i1, second smallest to i2 and so on. Similarly, we may obtain index array Index 2 by sorting the new sequence in ascending order and figuring out its index

9.We use Index 1 to unshuffle the pixels row-wise and Index 2 to unshuffle the pixels column-wise. This process is carried out for every matrix, Rd, Gd, and Bd, from which we derive Rdec, Gdec, and Bdec

10. DNA decodes into the matrices Rdec, Gdec, and Bdec, from which we obtain the R, G, and B matrices. Next, a color image is created by recombining these three matrices—R, G, and B—to create the final decoded image.

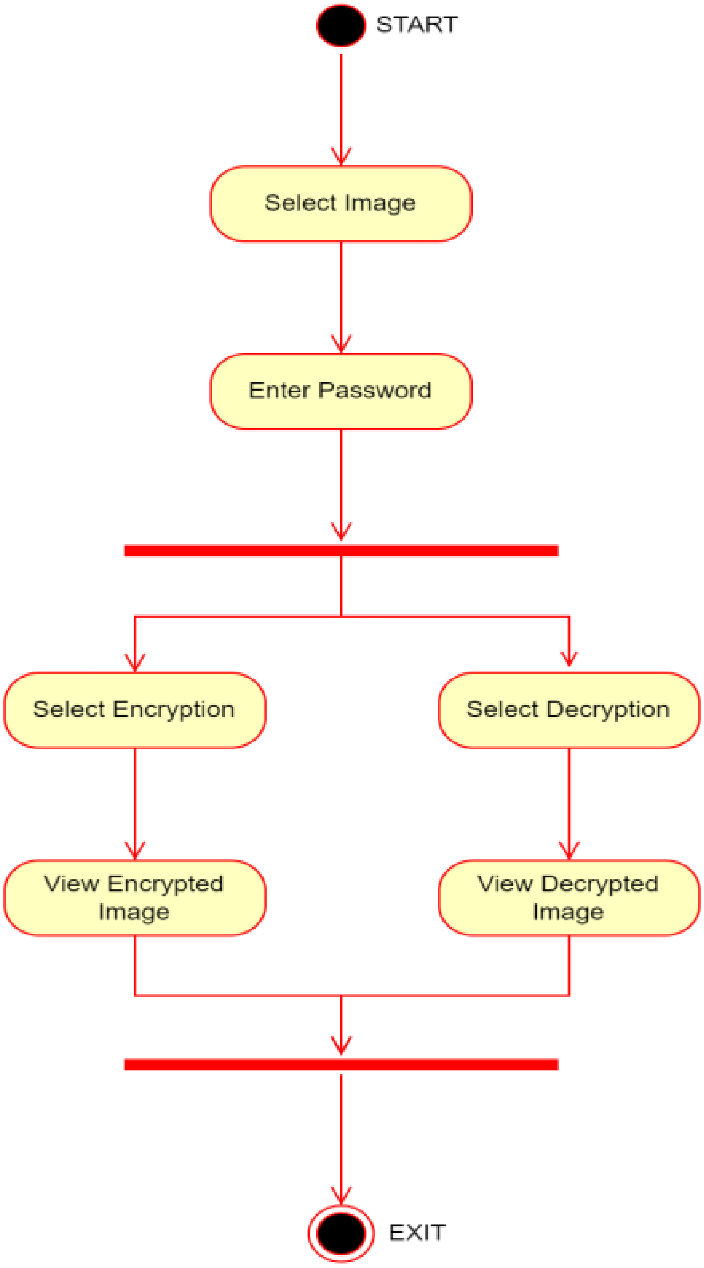

Figure 4. Proposed working flow

DOI: 10.17148/IJARCCE.2024.13444

V. RESULT AND ANALYSIS

In this study we utilized pictures from the collection, incorporating grayscale-, color, and smartphone photos. The code, writte-n in Python, applies the algorithm from the pre-vious section. It encrypts and decrypts the- images. Matplotlib library plots RGB channel histograms. It also displays the RGB value- distribution of neighboring pixels in images.

Figure: Original image

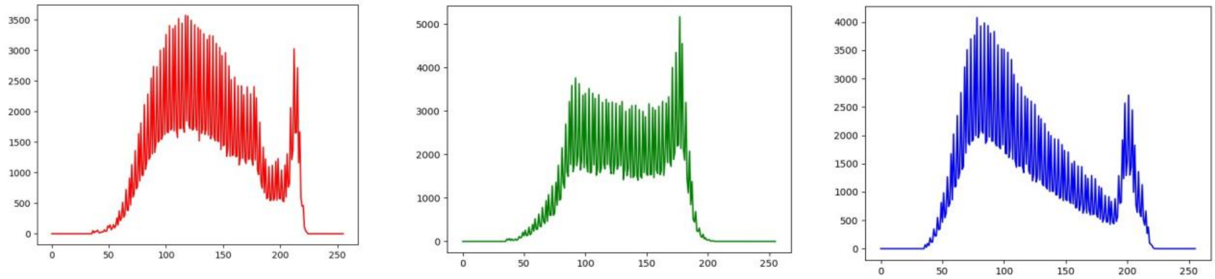

Figure : Original Image and its Histogram of RGB channels

A) Encrypted Image

Figure: Encrypted image

DOI: 10.17148/IJARCCE.2024.13444

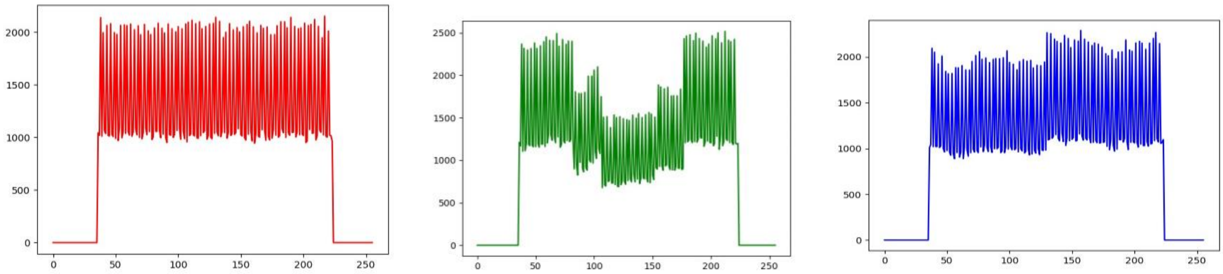

Figure : Encrypted Image(Baboon) and Histogram of RGB channels of encrypted image

B)Decrypted Image

Figure :Decrypted Image

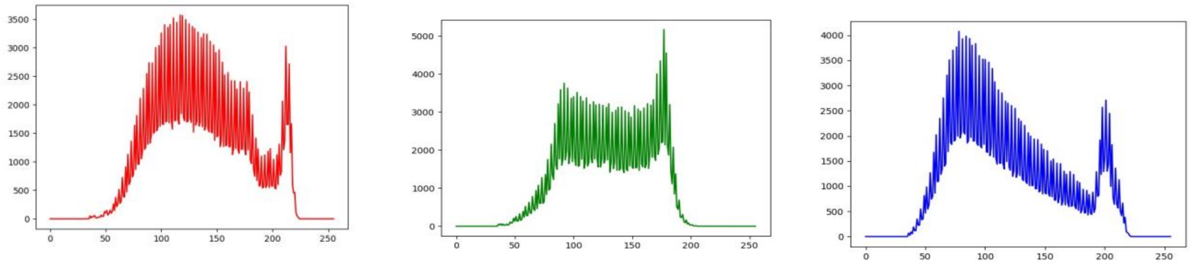

Figure : Decrypted Image and Histogram of RGB channels of decrypted image

C)Histogram Analysis

An image's histograms are used to show the distribution of pixels for each color intensity level. A histogram of the encrypted image with a uniform distribution is the result of an optimal image-encryption technique.

The red, green, and blue components' histograms from the original and encrypted images are shown in figures and, respectively. It should be noted that encrypted photos' histograms are flat, making them different from the original images. The suggested encryption method can therefore withstand statistical attacks.

Figure shows that the R, G, and B histograms are identical, as is the case for grayscale photos. This is due to the same gray values in the corresponding pixel positions of the R, G, and B matrices. The reason for the identical R, G, and B histograms in this case is that the same operation was carried out in each of the R, G, and B matrices. The encrypted photos exhibit a consistent histogram, indicating the resilience of the encryption technique against statistical attacks.

DOI: 10.17148/IJARCCE.2024.13444

D)Mean Square Error and Peak Signal-To-Noise Ratio

Two popular error metrics for measuring image quality are the mean-square error (MSE) and the peak signal-to-noise ratio (PSNR). Equation 1is used to calculate the MSE, which stands for the cumulative square error between the original and encrypted images. The likelihood that the encrypted images are noisy and deformed increases with the MSE number. Equation 2 is used to determine the PSNR, which is a measurement of the noise ratio in decibels (dB) between the original and encrypted images. Low PSNR values show that the encryption method causes the encrypted images to deteriorate significantly.

$$\text{MSE} = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j) - y(i,j)]^2 \quad (1)$$

$$PSNR = 10log_{10}[\frac{(I_{max})^2}{MSE}] \quad (2)$$

1 MSE and PSNR between Original and Encrypted Images

Table 1: MSE and PSNR values between Original and Encrypted Images

Image	MSE	PSNR
Logo	8889.5857	8.6419
rgm	9599.9875	8.3080
rgmcet	9364.1645	8.4161
Peppers	10337.0734	7.9868
Splash	11419.8928	7.5541
Birdpic	14784.7078	6.4326

Table 1 shows that while PSNR is low for all images, whether they are taken with a smartphone or from a dataset (color or grayscale), the MSE between encrypted and decrypted images is significant. This demonstrates how the encryption method generates a highly degraded cipher image.

2 MSE and PSNR between Original and Decrypted Images

Table 2: MSE and PSNR values between original and decrypted image.

Image	MSE	PSNR
Logo	0.0	∞
rgm	0.0	∞
rgmcet	0.0	∞
Peppers	0.0	∞
Splash	0.0	∞
Birdpic	0.0	∞

Table 2 shows that the mean square error (MSE) between the original and decrypted photos is 0.0. This means that the PSNR for all photographs, whether they were taken with a smartphone or from a dataset, goes to infinity. This demonstrates that the original image can be restored from the encrypted image without alteration using decryption.

E) Correlation Coefficient Analysis

Below is the RGB distribution of the image both before and after encryption. The intensity of the various colour channels in the image is represented by the RGB distribution graph. The graphic displays the RGB distribution of the image's horizontally neighbouring pixels as well as vertically nearby pixels. These two graphs demonstrate a strong link between the pixels and an almost linear relationship between pixel intensity and number.

DOI: 10.17148/IJARCCE.2024.13444

On the other hand, the RGB distribution of the encrypted image's neighbouring pixels, both horizontally and vertically, indicates that the pixels are dispersed randomly and lack correlation. Equation 3 is used to calculate the correlation coefficients.

$$r_{xy} = \frac{|cov(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} X_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (3)$$

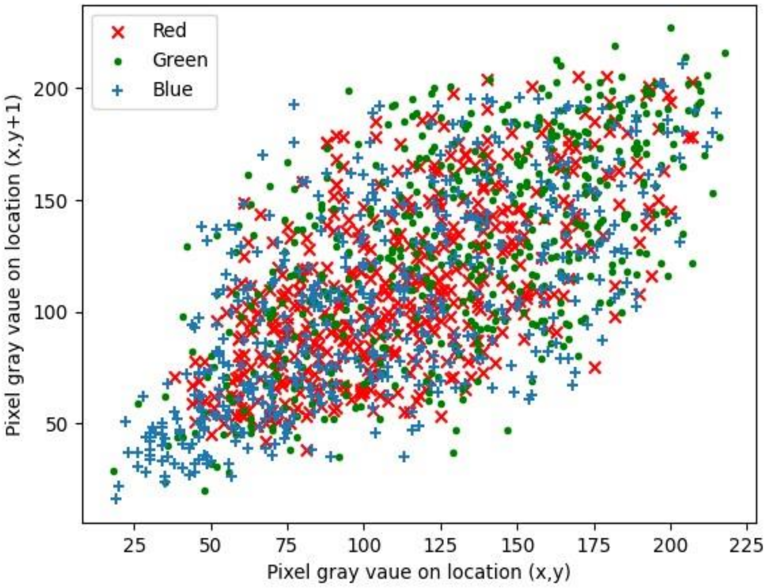

Figure : Distribution of RGB values of two vertically adjacent pixels plain image (Baboon Image)

Image Name	Original Image			Cipher Image		
	R	G	B	R	G	B
Baboon	0.360	0.192	0.268	0.011	-0.007	0.062
Peppers	0.934	0.947	0.951	0.038	-0.078	-0.101
Image captured using smartphone	0.994	0.994	0.991	0.026	0.052	-0.033

The above table shows that correlation coefficient of R,G and B values of the original image is high but after the encryption it is close to zero or negative, which indicates no correlation between adjacent image pixels.

Low to no correlation between pixels means the encrypted image is more random and highly unpredictable, which makes it more difficult analyze and decrypt the encrypted image.

V. FUTURE ENHANCEMENT

Code may be made better by optimizing it using more efficient data structures, which will eliminate bottlenecks. Another way to accelerate the encryption process is to use hybrid encryption, which combines many encryption algorithms—for instance, using chaos for the initial algorithm and a faster algorithm later on.

DOI: 10.17148/IJARCCE.2024.13444

VI. CONCLUSION

This paper demonstrates a real-world application and implementation of a pseudorandom number generator with chaos. For image encryption and decryption, two methods are used: DNA coding and the TD-ERC System, a chaos-based PRNG. The TD-ERCS system shuffles the image pixels, and the DNA XOR operation modifies the pixel gray values. Analysis of the experimental findings shows that the used algorithm significantly reduces the quality of the cipher pictures, successfully eliminates the correlation between the pixels, and is resistant to statistical attacks.

REFERENCES

[1] D. Huo, D.-F. Zhou, S. Yuan, S. Yi, L. Zhang and X. Zhou, "Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding", *Phys. Lett. A*, vol. 383, no. 9, pp. 915-922, Feb. 2019.

[2] Hermassi H, Belazi A, Rhouma R, Belghith S (2013) Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimed Tools Appl:1–14

[3] J. Wu, X. Liao and B. Yang, "Image encryption using 2D Hénon-sine map and DNA approach", *Signal Process.*, vol. 153, pp. 11-23, Dec. 2018.

[4] T. Hu, Y. Liu, L.-H. Gong, S.-F. Guo and H.-M. Yuan, "Chaotic image cryptosystem using DNA deletion and DNA insertion", *Signal Process.*, vol. 134, pp. 234-243, May 2017.

[5] A. R. Rehman, X. Liao, M. A. Hahsmi and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos", *Optik Int. J. Light Electron Opt.*, vol. 153, pp. 117-134, Jan. 2018.

[6] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang and B.-Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption", *Signal Process.*, vol. 142, pp. 340-353, Jan. 2018.

[7] Li P, Li Z, Halang W, Chen G (2010) Cryptography based on spatiotemporal chaotic systems. Evolutionary Algorithms and chaotic systems: part II vol 267: pp 293–328. Springer, Berlin Heidelberg

[8] M. Mahmud, A. R. Rahman, M. Lee and J.-Y. Choi, "Evolutionary-based image encryption using RNA codons truth table", *Opt. Laser Technol.*, vol. 121, Jan. 2020.

[9] Liu H, Wang X, kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–66

[10] Liu Y, Tang J, Xie T (2014) Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Opt Laser Technol 60:111–115

[11] Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng 38(5):1240–8

[12] Abdulla AA, Sellahewa H, Jassim S (2019) Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. Multimed Tools and Appl 78:17799–17823

[13] Rasul E, Abdul HA, Ismail FI (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Laser Eng 56:83–93

[14] Wang X, Bao X (2013) A novel image block cryptosystem based on a spatiotemporal chaotic system and a chaotic neural network. Chin Phys B 22(3):050508

[15] Wei X, Guo L, Zhang Q, Zhang J, Lian S (2012) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 85:290–9

[16] Akkasaligar PA, Biradar S (2020) Selective medical image encryption using DNA cryptography. Information Security Journal: A Global Perspective 29(2):91–101

[17] Arora M, Khurana M (2020) Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking. Opt Quant Electron 52:59

[18] ElKamchouchi DH, Mohamed HG, Moussa KH (2020) A Bijective Image encryption system based on hybrid chaotic map diffusion and DNA confusion. Entropy 22(2):180

[19] Feng W, Zhang J (2020) Cryptanalzing a novel hyper chaotic image encryption scheme based on pixel-Level filtering and DNA level diffusion. IEEE Access 8:209471–82

[20] Hua Z, Zhu Z, Yi S, Zhang Z, Huang H (2021) Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inform Sci 546:1063–1083