Proceedings of the Jangjeon Mathematical Society
28 (2025), No. 4, pp. 495 – 524

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2025.28.4.009

AUTHENTICATION-BASED IMAGE ENCRYPTION SCHEME USING RSA DIGITAL SIGNATURE AND MULTI-DIMENSIONAL CHAOTIC MAPS

SANDEEP KUMAR, KHUSHI, AND DEEP SINGH*

Abstract. This paper proposes an authenticated digital image security algorithm by combining the digital signature and multilayer encryption. The RSA digital signature with SHA-256 hash function is utilized to verify the sender's authenticity. The digital signature is generated independently from the original image using the signer's private keys. Further, the encryption is done in multilayers by employing a Gingerbreadman map, a two-dimensional piecewise smooth nonlinear chaotic map (2D-PSNCM), and Baker's map. First, the confusion among the pixel values of the original image is created using the Gingerbreadman map. The partially encrypted image undergoes diffusion using the chaotic sequence generated from 2D-PSNCM. Further, Baker's map is applied for a suitable number of times to enhance the encryption quality and decrease the correlation among pixel values. The obtained digital signature is appended with the finally encrypted image. The main contribution of this work lies in integrating the RSA digital signature with a multilayer chaotic encryption framework, employing diverse chaotic maps for confusion and diffusion. Most existing schemes focus either on confidentiality or authentication, but the proposed scheme ensures both confidentiality and authentication verification simultaneously. Further, proposed technique's robustness, efficiency, and security are examined with the help of some statistical analysis like entropy, energy, correlation, classical attacks, structure similarity index, key sensitivity, and histogram analysis.

2000 Mathematics Subject Classification. 94A60, 11T71, 34C28.

Keywords and phrases. Gingerbreadman map, 2DPSNCM, Baker's map, confusion-diffusion, digital signature and SHA-256 hash function.

Submission Date: 14.10.2024

1. Introduction

Network security has become a significant concern as computers and technology are used increasingly. Since, we use computers for nearly everything in our daily lives, there are many security challenges regarding the data that we exchange via open networks. For this reason, it is essential to improve the security and authenticity in ownership of digital data. Cryptography is one of the essential for protecting digital conversations, transactions, and information in the present world where information is increasingly transmitted through these open networks. We have been using cryptography for a long time to keep data safe and secure, and several cryptosystems providing data security, authenticity, and safety are presented in [33, 24, 10, 30, 23, 42, 30, 45].
In order to prevent digital data from third party during the data delivered across the

*Corresponding Author.

channel, the data is transferred in the form of cipher text using the cryptographic algorithms [25]. Symmetric and asymmetric key cryptography are the two main types of cryptography [41] [35]. Asymmetric cryptography is generally preferred because it uses two distinct types of keys—a public key which is known to everyone and a private key which is generated by receiver and known to receiver only that increases the security in the cryptosystem. In addition to keys, the confusion and diffusion in the digital data is used most popularly. The confusion is used to generate randomized encrypted text. Further, diffusion is used to increase the complexity of the original message in the significant part of the encrypted text to make it unclear for the cryptanalysis [9] [31]. The AES [24] [42], triple DES [10], RSA cryptosystem [30], ElGamal encryption technique [23](a version of DSA [28]), DES (Data Encryption Standard) [42] [30] are the well known methods used for encryption of digital data. Triple data encryption standard, known as triple DES, is a symmetric cryptographic system based on block ciphers [45].

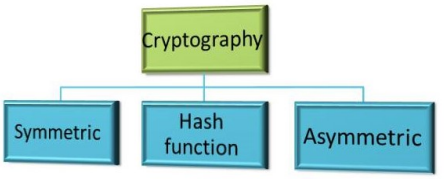


FIGURE 1. Types of Cryptography

A digital signature is a cryptographic method that ensures the non-repudiation, integrity, and authenticity of digital communications or papers [33]. It provides significantly greater security and usefulness than a handwritten signature or a stamped seal.

Digital signatures offer several benefits like authentication and integrity:

(1) **Authentication:** Only the sender's private key can produce a valid signature for a message, thus proving the sender's identity.
(2) **Integrity:** Any tampering with the message or document, even a minor alteration, will lead to the failure to verify the computed hash value and the decrypted hash value of the signature, indicating that the content has been altered.

A digital signature includes three stages [30]. The first stage is key creation, which is accomplished using an algorithm [17]. A hash function is applied over the original digital message and the obtained output is then employed to create the signature using the generated key [33]. A hash function assigns the given input digital data of arbitrary size to a fixed value and the values is known as message digests or hash values. Final stage is of verification of sender's authenticity, for this, the recipient will next use the public key produced by the signer/ sender to decrypt the digital signature. Further, the decrypted digital signature is compared with the obtained hash value by applying the same hash function to the data that have received to receiver [7]. Finally, the receiver will be able to verify the signer's authenticity if obtained hash value correlates with the output produced after decrypting the digital

signature.
RSA cryptosystem is one of the most widely used asymmetric cryptosystems, named after its three inventors: Ron Rivest, Adi Shamir, and Leonard Adleman [26]. It works on the principle of modular arithmetic and the mathematical characteristics of large prime numbers.
The RSA algorithm is as follows [26], [34]:

(1) Firstly, The sender will use the SHA (Secure Hash Algorithm) function (which is also known as the message digest algorithm) to generate the message digest or hash values.
(2) Now, the sender will use own private key to encrypt the message digest, known as a digital signature.
(3) Then, the sender will send the encrypted message along with the produced digital signature.
(4) The receiver will use the public key and same SHA function to verify the algorithm used in the digital signature, that authenticate the message ownership.

The maps that produces pseudo-random values in addition to the starting parameters are called chaotic maps [19]. Corresponding to given initial seed values, the generated values show pattern which is highly arbitrary and random. Numerous linear and nonlinear chaotic maps are now in use for encryption, like logistic map, sine map, tent map, Gingerbreadman map, two-dimensional piecewise smooth nonlinear chaotic map(2D-PSNCM), Arnold's cat map, Baker's map, and Henon map, etc [15, 15, 15, 18]. Nonlinear chaotic maps, which involve nonlinear equations whereas, linear chaotic maps are based on linear equations. Despite their simplicity, linear chaotic maps can exhibit complex and unpredictable behavior only under certain conditions. Unlike linear systems, whose output varies according to the input only, nonlinear systems show complex and unpredictable behavior, even when subjected to small changes in initial conditions [19]. A chaotic map holds a non-periodicity property and is sensitive to the initial parameters. The following are some benefits of the encryption technique using chaotic maps.

(1) Can be used to encrypt images of any size and is suitable for both color and grayscale images;
(2) Since high sensitivity towards initial condition and secret key parameters, the encryption technique will be able to resists all types of classical attacks.
(3) Security may be enhanced by using two or more distinct maps at a time for encryption and decryption [3].

In paper [26], an asymmetric encryption technique is introduced for colored images, which involves the encryption of three layers using the RSA cryptosystem and a chaotic map. In paper [13], a new cryptographic technique is proposed using a two-dimensional piecewise smooth nonlinear chaotic map (2D-PSNCM). It is based on the confusion and diffusion method. In paper [19], a nonlinear system is used to encrypt the plaintext by using the Gingerbreadman chaotic map and S_8 permutations. In paper [8], the five-step encryption technique is used based on the confusion and diffusion method and a 3D modular chaotic map to enhance the security level. In paper [40], many encryption techniques have been summarized, like RSA, AES, and DES. For the comparsion, the quality tests of the techniques have been done

by some statistical analysis, including peak signal-to-noise ratio (PSNR), structure similarity index method (SSIM), and mean square error (MSE).
In paper [38], chaotic colored image encryption is proposed. At first, the colored image is divided into RGB layers. Then, segregate the RGB layer, encryption using confusion and diffusion are used along with chaotic logistic map. In paper [4], the digital image is encrypted using a digital signature where the hash function is applied with the application of the logistic map for the encryption [29], and the RSA cryptosystem is used in the digital signature. In paper [37], a practical approach for detecting manipulation and supporting image compression is presented.

By getting motivation from above literature and to combine the authentication approaches with the encryption, in this article, we have presented a multilayer authentication based encryption scheme by combing two dimensional piecewise smooth nonlinear chaotic map (2D-PSNCM), Baker's map and RSA cryptosytem along with $SHA-256$ hash function. We have integrating the RSA digital signature with a multilayer chaotic encryption framework, employing diverse chaotic maps for confusion and diffusion. Hence, the proposed scheme ensures both confidentiality and authentication verification simultaneously.

The rest of the sections of this manuscript includes following sections: the third section, which reviews the insights and framework of the work. The fourth section introduces the proposed techniques used for encryption and decryption. Experimental tests of the presented work are shown in Section 5. The conclusions and references are provided in the last section.

2. Insights and Framework:

2.1. **Gingerbreadman Map:** The "Gingerbreadman map" is a chaotic map used in chaos theory and dynamical systems [19]. It is named after Ian Stewart, who created this map and is a fundamental example of a chaotic system. In this map, a binary grid is used, and each point on this grid represents a state in the system. The map, controlled by equations, shows how each area evolves. It is known for its chaotic nature, where minimal changes in the initial parameters may result in drastically different outputs.

The Gingerbreadman map provides a valuable tool for exploring the theory of chaos, nonlinear dynamics, and the intricate behaviors of complex systems. Plotting this map's chaotic solution set reveals a gingerbread man-like shape. Mathematically, it is given by the following piecewise linear transformation [16]:

$$s_{i+1} = 1 - t_i + |s_i|,$$

$$t_{i+1} = s_i,$$

where s_0 and t_0 are initial parameters and $i \in N \cup \{0\}$. The Gingerbreadman map is selected for pixel-level confusion in the proposed scheme due to its distinct chaotic trajectory and high sensitivity to initial conditions. Its strong randomness efficiently disrupts the spatial correlation of pixel values in a given image.

2.2. **Two-dimensional Piecewise Smooth Nonlinear Chaotic Map (2D-PSNCM):.** The two-dimensional piecewise smooth nonlinear chaotic map (2D-PSNCM) serves as a mathematical framework employed to replicate chaotic dynamics within two-dimensional systems [13]. "Piecewise" means that the equations governing the dynamics change abruptly at certain boundaries or thresholds.

"Smooth" indicates that these equations are continuous and differentiable, ensuring that the system's evolution is well-behaved. In linear chaotic maps, relying on linear equations are used, whereas, in the 2D-PSNCMs, nonlinear equations are used and exhibit piecewise smooth characteristics delineated by several smooth segments. The general form of the 2D-PSNCM can be represented as follows:

$$g_{1,t+1} = g_{1,t} + k_1 g_{1,t}[1 - 2(1 + C_1)g_{1,t} - \theta g_{2,t}], \tag{1}$$

$$g_{2,t+1} = \begin{cases} g_{2,t}[1 + \theta k_2 - 2k_2(C_2 + \theta)g_{2,t}], & \text{if } g_{1,t} \geq f(g_{2,t}) \\ g_{1,t}, & \text{if } g_{1,t} < f(g_{2,t}) \end{cases},$$

where

$$f(g_{2,t}) = \frac{g_{2,t}[1 + \theta k_2 - 2k_2(C_2 + \theta)g_{2,t}]}{1 + \theta k_2 g_{2,t}}.$$

In above equations, c_1 and c_2 are the shift cost parameters satisfying the condition $c_1 > c_2$. The parameter θ stands with the condition $c_2 < \theta$ and $0 < \theta < 1$. Its chaotic behavior depends upon the values of the parameters: c_1, c_2, θ, k_1, k_2 and on the initial values $g_{1,0}$, $g_{2,0}$. The 2D-PSNCMs can handle complex nonlinear behaviour while being flexible, vigorous, insightful, and efficient in calculations. Further, the bifurcation diagram for the 2D-PSNCM concerning the parameter k_1 is presented in Figure 2. To obtain this diagram, we have taken a fix value of 2 for the parameter k_2 and the parameter k_1 is varies in from 0 to 3. Similarly, the graphical interpretation for the Lyapunov exponent for the parameter k_1 is provided in Figure 3.

The 2D-PSNCM is selected in the proposed scheme due to its ability to generate a highly complex and diverse chaotic sequence. This property enhances the diffusion process and provides a capability for the encryption process to be resistant to statistical and differential attacks.

2.3. **Baker's Map.** The Baker's map is a 2D chaotic map that works on a square grid. Stretching and folding processes are used to confuse the placements of the grid points [18]. It is a one-one map, that maps the unit square onto itself [20]. Mathematically, it is represented as follows:

$$(p_{n+1}, q_{n+1}) = \begin{cases} (ap_n, \frac{q_n}{a}) & \text{for } 0 \leq p_n < a \\ (a + bp_n, \frac{q_n - a}{b}), & \text{for } a \leq p_n < 1 \end{cases}$$

where (p_{n+1}, q_{n+1}) are the coordinates of the grid points after applying the Baker's map on the grid points (p_n, q_n), and a & b are the secret key parameters. The process of Baker's map for confusion is as follows:
Firstly, consider an image of size n × n, which is further divided into c vertical rectangles of width n_i such that each n_i divides n, i.e., (n_i/n) and $\sum n_i = n$, where the height of each rectangle is n [27]. Further, divide these vertical rectangles into small rectangles containing n elements. Lastly, place these small rectangles (having n elements) into rows from bottom to top. This placement of rectangles produces a confused image. Baker's map is incorporated into the proposed scheme due to its exceptional capability for shuffling pixel positions and ensures robustness against structural similarity and histogram-based attacks. By applying it iteratively, the map substantially reduces pixel correlation, further increasing the encryption quality.

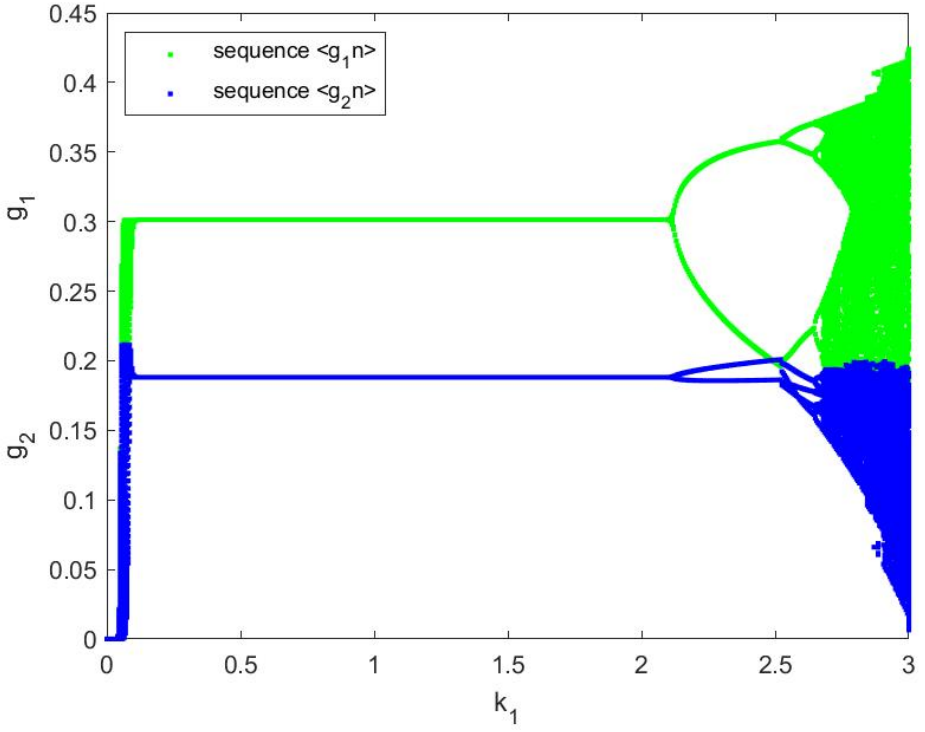


FIGURE 2. Bifurcation diagram for the parameter k_1 in the 2D-PSNCM by condering the fix values: initial conditions $g_{(2,0)} = 0.0000000000023$ & $g_{(1,0)} = 0.0000000000067$ and parameters $\theta = 0.35$ and $c_2 = 0.3$, & $c_1 = 0.55$.

2.4. **RSA Cryptosystem.** The RSA cryptosystem, devised by Rivest, Shamir, and Adleman, is a popular public-key encryption system facilitating secure communication and digital signatures across untrusted networks [26] [35]. It is mostly used for digital signatures to verify authenticity and provides a method to verify data integrity. The RSA cryptosystem operates as follows [7]:

(1) Key Generation:
Consider two large prime numbers, t and s. Compute the product $k = t \times s$. Now, calculate the Euler's function

$$\phi(k) = (t-1) \times (s-1).$$

Select a public exponent E that is co-prime to $\phi(k)$. Calculate corresponding private exponent D such that

$$D \times E \equiv 1 \pmod{\phi(k)}.$$

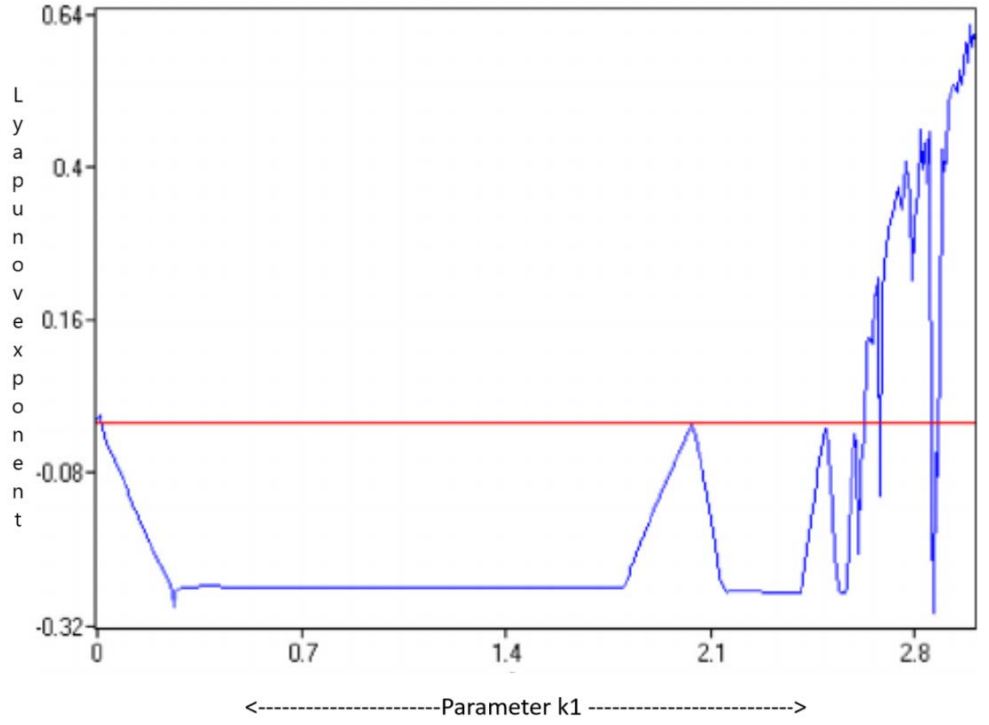


FIGURE 3. Lyapunov exponent for the parameter k_1 in the 2D-PSNCM by condering the fix values: initial conditions $g_{(2,0)} = 0.0008$ & $g_{(1,0)} = 0.0002$ and parameters $\theta = 0.35$ and $c_2 = 0.3$, & $c_1 = 0.55$.

(2) Encryption:
Let the original message be M. Encrypt M using the public key (E, k) with

$$C \equiv M^E \pmod{k},$$

and send the resulting ciphertext C.

(3) Decryption:
Decrypt C using the private key D as follows:

$$M \equiv C^D \pmod{k},$$

the obtained value of M is the required plaintext.

The choice of the RSA cryptosystem with the SHA-256 hash function for authentication is motivated by the robustness and compatibility of the RSA cryptosystem established across diverse systems and, combined with the SHA-256 hash function, produces a strong collision resistance and computational efficiency. While alternative cryptosystems offer shorter key lengths, the RSA cryptosystem provides comparable security with broader support and more straightforward implementation in various platforms. Further, the SHA-256 hash function is a widely adopted cryptographic

hash function that includes collision resistance and is a good choice for digital signature schemes. Its integration with the RSA cryptosystem ensures the authenticity and integrity of transmitted data without introducing additional vulnerabilities.

3. Proposed Techniques and Framework

In this paper, we propose an authentication-based color image encryption scheme that verifies the authenticity of users while maintaining confidentiality. The RSA digital signature, by applying the SHA-256 hash function, is used to verify authenticity.

3.1. **Proposed Technique for Encryption.** The Gingerbreadman map creates confusion by shuffling the pixel positions of the original image, significantly reducing its spatial coherence. The 2D-PSNCM generates chaotic sequences to achieve diffusion by utilizing the bitXOR operation, ensuring high sensitivity to initial conditions and enhancing security. Finally, Baker's map further refines the encryption quality by iteratively reducing pixel correlation and improving statistical properties. In this proposed work, the level of confusion and diffusion is well maintained during encryption. A comprehensive explanation of the proposed technique is summarized in Figure 4, and step by step explanation is provided below.

(i) Taking an original image H.
Chaotic sequences generation:

(ii) Apply $SHA-256$ hash function to the original image (H)

$$Hash_h = SHA-256(H).$$

(iii) Generate two decimal numbers with the help of the hash value ($Hash_h$)

$$Hash_1 = Hash_h(1:10),$$
$$Hash_2 = Hash_h(11:20),$$
$$dec_1 = hex2dec(Hash_1),$$
$$dec_2 = hex2dec(Hash_2).$$

(iv) Divide the above decimal numbers by 10^{13} to obtain initial conditions of 2D-PSNCM in the range (0,1)

$$\alpha_0 = \frac{dec_1}{10^{13}},$$
$$\beta_0 = \frac{dec_2}{10^{13}}.$$

(v) Generate chaotic sequences $< \alpha_n >$ and $< \beta_n >$ by using 2D-PSNCM defined in Section 2.2 by considering the above generated initial values α_0, β_0 and secret parameters c_1=0.55, c_2=0.25, $\theta = 0.35$, k_1=2.95, k_2=2, $\alpha(1) = \alpha_0$, and $\beta(1) = \alpha_0$.

(vi) Generate sequence corresponding to $< \alpha_n >$ and $< \beta_n >$ having numbers between 0 and 255

$$< \alpha'_n >= mod(floor(abs(< \alpha_n > 10^{14}), 256),$$
$$< \beta'_n >= mod(floor(abs(< \beta_n > 10^{14}), 256).$$

(vii) Obtain a single sequence $< \gamma_n >$ with the help of bitXOR

$$< \gamma_n >= bitXOR(\alpha'_n, \beta'_n).$$

(viii) Taking initial values for Gingerbreadman (viz., a_1 and b_1), and apply Gingerbreadman map defined in Section 2.1 to generate chaotic sequence $< a_n >$.
(ix) Sort the sequence generated in the above step and store the index for confusion

$$\text{I=index(sort}(< a_n >)).$$

Segregation of color components:
(x) Segregate H into three color components, R, G, and B, and take the first layer R.
Individual layer encryption:
(xi) Apply confusion using the index sequence $< I >$, which is generated from the Gingerbreadman map (please refer to Step (iii))

$$R1 = R,$$

$$R1(i) = R(I).$$

(xii) Diffuse the pixel values of the above partially encrypted image using sequence $< \gamma_n >$

$$R2 = bitXOR(R1, \gamma_n).$$

(xiii) Apply Baker's map (defined in Section 2.3) to the obtained image R2 in previous step.
(xiv) Repeat Step (ix) to Step (xi) again for the second and third layers.
Concatenation of ciphered components:
(xv) Concatenate all three encrypted layers to get the final ciphered image (E) corresponding to the original image (H).

Algorithm 1: Image Encryption Process

Input: Original Image H, Chaotic Map Parameters $\{c_1, c_2, \theta, k_1, k_2\}$, Gingerbreadman Initial Values a_1, b_1

Output: Encrypted Image (E)

Generate message digest of H: $Hash_h \leftarrow \text{SHA-256}(H)$;

Extract decimal values from hash:

$$Hash_1 \leftarrow Hash_h(1:10), \quad Hash_2 \leftarrow Hash_h(11:20)$$

$$dec_1 \leftarrow \text{hex2dec}(Hash_1), \quad dec_2 \leftarrow \text{hex2dec}(Hash_2)$$

Generate initial conditions for 2D-PSNCM:

$$\alpha_0 \leftarrow \frac{dec_1}{10^{13}}, \quad \beta_0 \leftarrow \frac{dec_2}{10^{13}}$$

Generate chaotic sequences $< \alpha_n >$ and $< \beta_n >$ using 2D-PSNCM with initial values α_0, β_0, and secret parameters c_1, c_2, θ, k_1, k_2;

Generate sequences $< \alpha'_n >$ and $< \beta'_n >$:

$$< \alpha'_n > \leftarrow \text{mod}\left(\text{floor}\left(|\alpha_n|\, 10^{14}\right), 256\right)$$

$$< \beta'_n > \leftarrow \text{mod}\left(\text{floor}\left(|\beta_n|\, 10^{14}\right), 256\right)$$

Generate the sequence $< \gamma_n > = \text{bitXOR}(< \alpha'_n >, < \beta'_n >)$;

Generate Gingerbreadman chaotic sequence $< a_n >$ using initial values a_1 and b_1;

Sort the sequence $< a_n >$ and store the index for confusion:

$$I \leftarrow \text{index}(\text{sort}(< a_n >))$$

Segregate H into three color components: Red (R), Green (G), and Blue (B).

Apply confusion on the color component using index I:

$$R1(i) \leftarrow R(I)$$

Apply diffusion using sequence $< \gamma_n >$:

$$R2(i) \leftarrow \text{bitXOR}(R1(i), < \gamma_n >)$$

Apply Baker's map on the partially encrypted component $R2$.

Repeat the above steps for the Green (G) and Blue (B) components.

Concatenate the encrypted color components to form the final encrypted image E:

$$E \leftarrow \text{Concatenate}(R2, G2, B2)$$

3.2. **Proposed Technique for Digital Signature.**

(i) Generate a message digest by using the hash function, namely, SHA-256, on the original image

$$O_H = SHA - 256(H).$$

(ii) Consider its ASCII (American Standard Code for Information Interchange) values and name it A_s

$$A_s = ASCII(O_H).$$

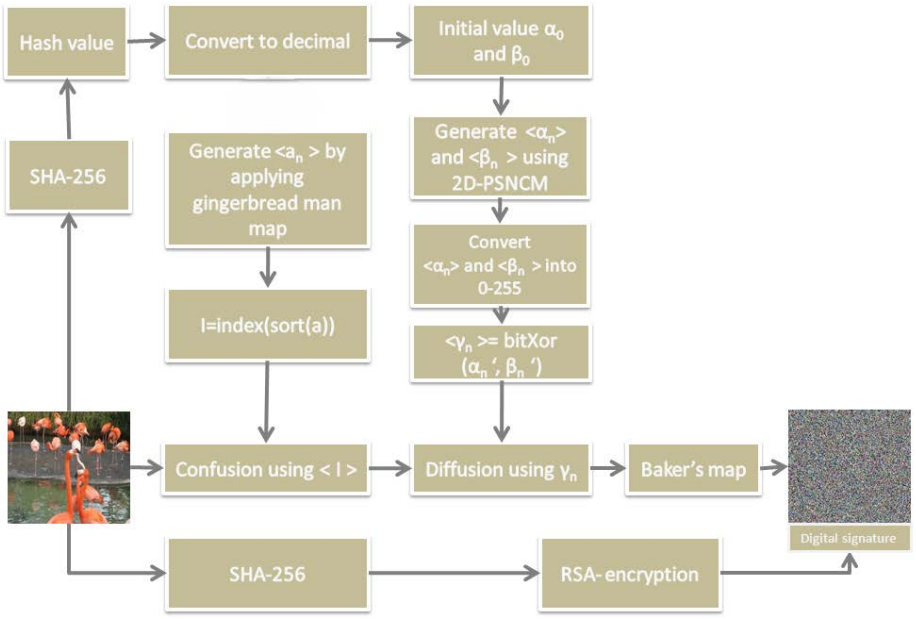


FIGURE 4. Flow chart of encryption/digital signature

(iii) The public key (E,k) and the private key (D,k) are generated by the signer with the help of the algorithm discussed in Section 2.4. The private key is utilized to generate the digital signatures and is kept secret, whereas the public key is available to everyone for verification purposes.

(iv) Now, apply the RSA encryption algorithm on A_s to generate a digital signature E_s

$$E_s = A_s^D \mod k.$$

3.3. **Proposed Technique for Decryption.** To obtain the original image (H) back from the encrypted one, repeat all the steps in the reverse order. The flowchart for combined verification and decryption is shown in Figure 5, and the step-by-step explanation is given below.

(i) Segregate the corresponding three layers from the encrypted image E.

(ii) Taking the first layer R of the image E without the digital signature.

(iii) For the reverse process, firstly applying the inverse Baker's map on the encrypted image, then inverse diffusion, and lastly, inverse confusion.

(iv) Concatenate all the three layers of the decrypted image and name it as D.

(v) Now, decrypting the digital signature by applying the RSA cryptosystem with public key (E,k) of signer

$$D_s = E_s^E \mod n.$$

(vi) Applying the hash function on D and taking its ASCII values, say A_d.

(vii) Then verify whether

$$A_d = D_s$$

.

- If Yes, then the digital signature is verified, and the data is authenticated.
- If No, then verification fails and data is altered or modified by the third party.

(viii) Repeat Step (*ii*) to Step (*viii*) for the second and the 3rd layer, respectively.

Algorithm 2: Decryption Process

Input: Encrypted Image I_{enc}
Output: Decrypted Image I_{dec}
Segregate the three layers from the encrypted image E
Take the first layer R of E (without the digital signature)
Apply the inverse Baker's map
Apply inverse diffusion
Apply inverse confusion
D=Concatenate the decrypted layers

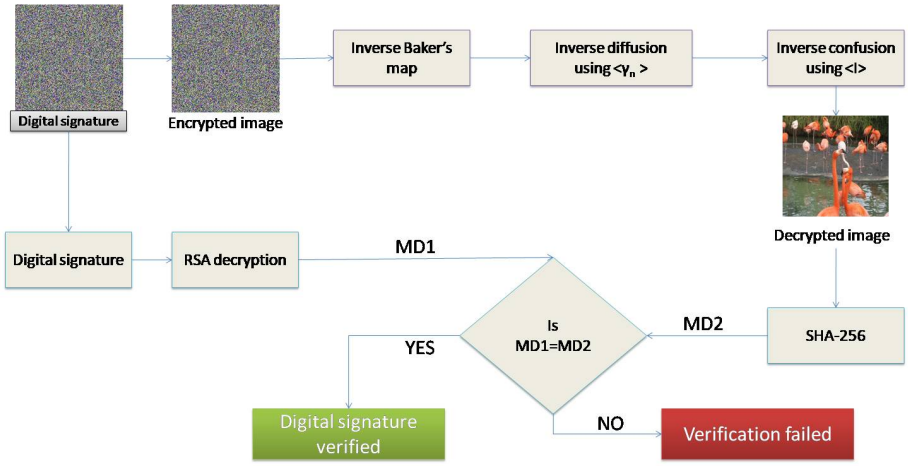


FIGURE 5. Flow chart of decryption/verification

4. Assessment of Outcome Through Simulation

The proposed work has tested various experiments on six colored images of size 256×256. The experimented images are taken from the USP-SIPI image database, and presented in Figure 6, where the first row represents the original images, and the second row represents their corresponding encrypted images.Further, corresponding decrypted images are presented in the third row. All the experiments are tested in MATLAB R2024a. The tests computed are structure similarity index, histogram analysis, chi-square test, key sensitivity, correlation coefficient, mean square error, peak signal-to-noise ratio, differential attack, entropy, noise attack, and cropping attack.

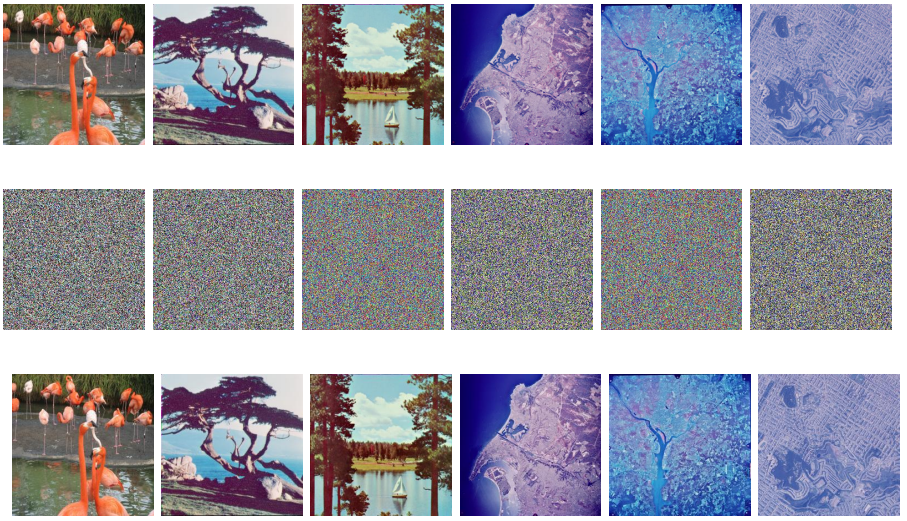


FIGURE 6. Original, encrypted and decrypted images

4.1. **Structure Similarity Index (SSI).** A statistical tool for calculating how similar two datasets or images are is the structural similarity index (SSI) [26]. The combination of the brightness, contrast, and structure comparison functions gives this index. Mathematically, it is calculated as:

$$SSI(P,Q) = \frac{(2\mu_P\mu_Q + C_1)(\sigma_{PQ} + C_2)}{(\mu_P^2 + \mu_Q^2 + C_1)(\sigma_P^2 + \sigma_Q^2 + C_2)}, \tag{2}$$

where P denotes the encrypted image, and Q denotes the original image. The variables μ_P and μ_Q calculate the average values of P and Q respectively. The parameters σ_P and σ_Q represent the variance of P and Q. Similarly, the parameter σ_{PQ} measures the covariance between the images P and Q. The result of SSI lies between -1 and 1. If two images are identical, then SSI is 1 otherwise it is close to 0. Table 1 shows the structure similarity index of six test images (component-wise). The SSI has been carried out between the original images and their corresponding cipherd images. It shows that the similarity for all the test is nearly equal to zero, making the presented algorithm a secure encryption method.

Test Images	Color components	SSIM
Flamingo	R	-0.0004
	G	-0.0027
	B	0.0003
Tree	R	0.0003
	G	-0.0036
	B	0.0009
Scene	R	-0.0004
	G	0.0011
	B	-0.0005
Satellite	R	-0.0033
	G	0.0034
	B	0.00007
Wash	R	-0.0021
	G	0.0051
	B	0.0012
View	R	0.0013
	G	0.0023
	B	0.0036

TABLE 1. Structure similarity index values

4.2. **Histogram Analysis.** A histogram is a graphical description of the frequency distribution of pixel intensities in an image [11]. For a grayscale image, the x-axis of the histogram represents pixel intensity values varying from 0 (black) to 255 (white). In contrast, the y-axis represents the frequency of occurrence of each intensity value [25]. Histograms provide insights into an image's overall brightness, contrast, and dispersal of pixel values.

Before performing histogram analysis for encryption, preprocessing steps may be applied to the image. Preprocessing involves converting the image to grayscale, resizing, or applying filters to enhance the quality of the encryption process. By analyzing the histograms of encrypted images and comparing them to histograms of the original images or plaintext, attackers may exploit weaknesses or patterns in the encryption algorithm. Hence, for reducing this type of attacks, the histogram of encrypted images must be uniform and having no peaks in the graph. Figure 7 represents the histogram analysis of six original images and the histogram of their corresponding encrypted images. In this figure, the first row shows the six original images and the second row shows their corresponding histograms, representing that the graph is not uniform. In contrast, the third row represents the encrypted images corresponding to above original images. Then, the fourth row is their corresponding histograms, which shows that the graph is uniform and, hence, the encryption is secure. The histogram of an encrypted image is uniformly distributed, meaning that all gray levels in the image have nearly the same frequency. This uniformity implies that all pixel values have an equal probability of occurrence. Consequently, the encrypted image exhibits strong randomness, as the absence of discernible patterns ensures resistance to statistical attacks. The histogram of the original image and the decrypted one is identical, implying that there is no data loss between the

encryption processes.

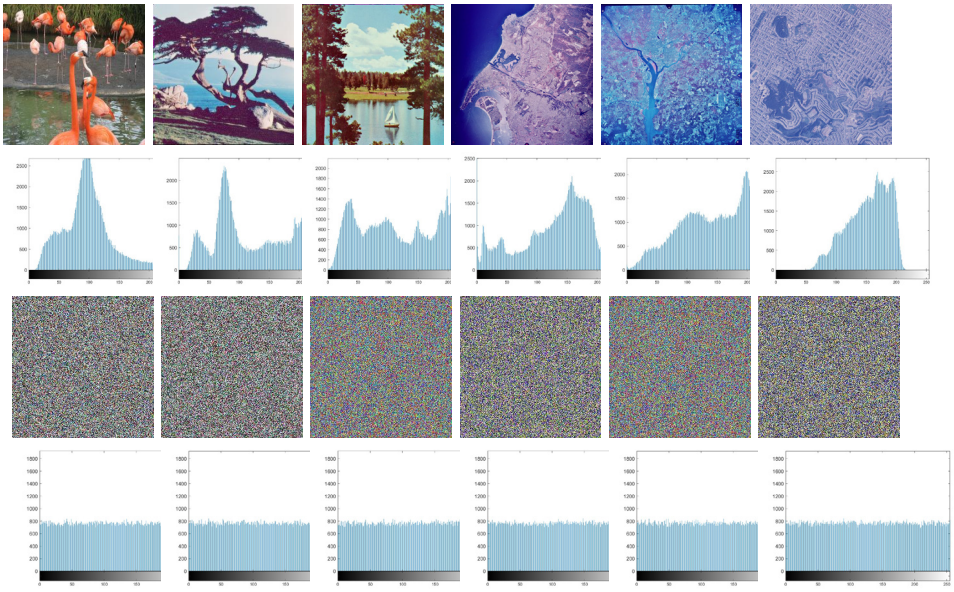


FIGURE 7. Row1 shows the original images, Row2 shows their corresponding histograms, Row3 shows the encrypted images, Row4 shows their corresponding histograms

4.3. **Chi-square Test.** Histogram analysis visually displays the dispersal of pixel intensities, while the chi-square test offers a quantitative assessment of the uniform distribution of the pixel in the encrypted image [44]. It is defined as

$$\chi^2 = \frac{\sum_{i=1}^{256}(I_i - E_i)^2}{E_i}. \tag{3}$$

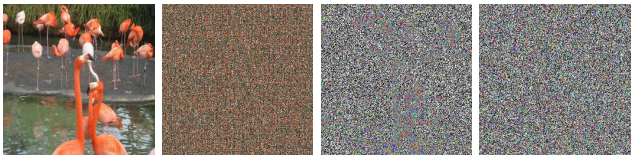
In this equation:
- χ^2 represents the chi-square value.
- I_i denotes the observed frequency for each intensity value i.
- E_i denotes the expected frequency for each intensity value i and $E_i = \frac{m \times n}{256}$

The analytical values for 256 degrees of freedom at 0.005 and 0.01 level of significance are $\chi^2_{0.01,255} = 310.4574$ and $\chi^2_{0.005,255} = 293.2478$. The χ^2-values for an efficient encryption scheme must be lower than the analytical values [26]. Table 2 shows the χ^2 values of the histogram analysis given in Figure 7. This table shows that all the Chi-square values are below 310.4574 and 316.9194. Hence, the test is verified, and the encryption is secure.

Test Images	R	G	B	Average
Flamingo	300.8125	280.2969	285.6172	288.9088
Tree	265.3359	245.9922	255.3125	255.5468
scenery	214.3828	254.9922	266.9688	245.4479
Satellite	242.4062	256.5469	258.7188	252.5573
Wash	256.7422	267.4531	263.4219	262.53
View	303.2344	248.2031	267.0156	272.8177

TABLE 2. Chi square test analysis: theoretical values are $\chi^2_{0.01,255} = 310.4574$ and $\chi^2_{0.005,255} = 293.2478$.

4.4. **Key Sensitivity.** To ensure effectiveness and robustness in encryption, it is crucial for the algorithm to be hypersensitive to the changes in the key. Even a small alteration in the key value or a random adjustment of key parameters should result in an incorrect image decryption [44]. It improves digital image encryption security by complicating decryption efforts. It prevent from brute-force attacks [22], where attackers methodically test various keys to decrypt the image, impractical. This is because of the multitude of potential keys and the unpredictability of how they influence the encrypted image [8]. For the proposed algorithm, results of the key sensitivity analysis are presented in Figure 8 and summarized below.



(A) (b) 12.0207 dB (c) 9.3237 dB (d) 9.3615 dB

FIGURE 8. Key Sensitivity analysis

Figure (8a) represents the decryption by considering correct secret keys and parameters.
Senstivity Analysis-I is carried out by changing initial value 'a' in the Gingerbreadman map during inverse confusion and keeping other values same. The obtained result is the image (b) of Figure 8, which shows that the original image one is not decrypted by changing the parameter 'a' only.

Senstivity Analysis-II is performed by changing a parameter in the two-dimensional piecewise smooth nonlinear chaotic map during inverse diffusion. The obtained result is the image (c) of Figure 8, which again shows that the original image 1 is not the same.

Senstivity Analysis-III is performed by changing a parameter in the 2D baker's chaotic map during inverse confusion. The obtained result is the image (d) of Figure 8.

Further, for the quantitative analysis of the quality of the images obtained after slight key changes, we calculated the PSNR between the original and the extracted images. The obtained PSNR values are provided in the captions of the corresponding images in the second row of Figure 8. From this, it is evident that all the calculated PSNR values are close to 10 dB, demonstrating that the extracted images, in the case of slight key changes, are completely different from the original images.

4.5. **Correlation Coefficient.** For every image, a definite degree of correlation exists between the neighboring pixels [25]. Therefore, a productive encryption technique should minimize the correlation as much as possible. In each image to calculate the correlation, adjacent pixels can be selected in three directions: horizontally (H), vertically (V), and diagonally (D) [1]. It is calculated as:

$$r_{xy} = \frac{mn \cdot E[(x - E_x)(y - E_y)]}{(\sum_{i=1}^{m}(x_i - E_x)^2) \times \left(\sum_{j=1}^{n}(y_j - E_y)^2\right)},$$

where

$$E_x = \frac{\sum_{i=1}^{m} x_i}{m}.$$

Table 3 shows proposed scheme's correlation analysis in which all the values are nearly equal to zero of encrypted images. Hence, there are highly uncorrelated pixel values in encryption images. This proves the argument of robustness. Further, the correlation of original and encrypted images are totally distinct, it implies that the original and encrypted images are highly uncorrelated, ensuring good quality of encryption and, hence, persistent to resist the attack.

Images		Original			Encrypted		
Flamingo	D	0.9174	0.8610	0.8583	0.0035	0.0072	0.0048
	V	0.9607	0.9208	0.9143	-0.0039	-0.0108	-0.0052
	H	0.9447	0.9094	0.9143	0.0060	0.0071	0.0054
Tree	D	0.9159	0.9318	0.9265	-0.0008	0.0031	-0.0003
	V	0.9361	0.9457	0.9406	0.0052	0.0051	0.0036
	H	0.9590	0.9687	0.9612	-0.0005	0.0033	0.0053
Scenery	D	0.9274	0.9225	0.9369	-0.0011	-0.0012	-0.0036
	V	0.9539	0.9527	0.9645	-0.0007	-0.0018	-0.0012
	H	0.9563	0.9558	0.9603	0.0009	-0.0046	-0.0011
Satellite	D	0.9246	0.9224	0.9149	-0.0019	0.0024	0.0005
	V	0.9484	0.9469	0.9412	-0.0024	-0.0020	-0.0040
	H	0.9517	0.9499	0.9443	0.0008	0.0023	-0.0023
Wash	D	0.7436	-0.0512	0.6570	-0.0066	-0.0025	0.0004
	V	0.8293	0.1360	0.7741	0.0011	0.0057	0.0058
	H	0.8229	0.1141	0.7772	0.0045	-0.0055	0.0011
View	D	0.5628	-0.0135	0.5258	0.0066	0.0034	-0.0057
	V	0.7244	0.1062	0.6971	0.0080	0.0070	0.0023
	H	0.6827	-0.0089	0.6484	0.0028	0.0083	0.0036

TABLE 3. Correlation analysis for plain and encrypted images

4.6. **Mean Square Error (MSE).** The collective error between two images is calculated using the mean squared error (MSE) [26]. The MSE between the input and cipher images should be more extensive, whereas it should be about zero between the decrypted and original images. A lower MSE value suggests higher similarity between the images, while a higher MSE value suggests greater dissimilarity. The MSE between two images of the same size p × q is calculated as:

$$MSE = \frac{1}{pq}\sum_{a=0}^{p-1}\sum_{b=0}^{q-1}[(O_1(a,b) - O_2(a,b))]^2,$$

where p and q represent the width and height of the images respectively. In the above equation, $O_1(a,b)$ and $O_2(a,b)$ denote the corresponding pixel values of the images at the position (a,b). The MSE is calculated between the original and the encrypted images and the original and the decrypted images. In Figure 4, the mean square error between the original and the encrypted images is high, which means that both the images are completely different and hence, it will be difficult to decrypt the image and data in it, whereas the mean square error between the original and the decrypted image is zero which shows that the image is decrypted successfully without any data loss.

Images	Layer	MSE (Original,Encrypted)	MSE (Original,Decrypted)
Flamingo	R	9.2086×10^3	0
	G	7.4811×10^3	0
	B	8.9425×10^3	0
Tree	R	8.7982×10^3	0
	G	1.1287×10^4	0
	B	9.6864×10^3	0
Scenery	R	7.2066×10^3	0
	G	1.1275×10^4	0
	B	1.1381×10^4	0
Satellite	R	9.7277×10^3	0
	G	9.7642×10^3	0
	B	7.3864×10^3	0
Wash	R	8.2786×10^3	0
	G	6.9062×10^3	0
	B	9.8328×10^3	0
View	R	6.6034×10^3	0
	G	6.1891×10^3	0
	B	9.1333×10^3	0

Table 4. The MSE Analysis

4.7. **Peak Signal to Noise Ratio (PSNR).** A statistic called peak signal-to-noise ratio (PSNR) compares the quality of an original, uncompressed signal to the corresponding reconstructed or compressed signal [26]. It measures the proportion of a signal's maximum possible power to the level of noise that interferes with the signal, reducing its precision.

Peak signal-to-noise ratio (PSNR) is a metric used to quantify the quality of a reconstructed or compressed signal, such as a digital image or audio file, relative to

the original, uncompressed signal. It measures the proportion of a signal's maximum potential power to the power of the noise that disrupts its accuracy. In simpler terms, the PSNR provides a numerical measure of how much the quality of the signal has degraded after compression or reconstruction. The PSNR is evaluated by [21]:

$$\mathrm{PSNR} = 10 \cdot \log_{10} \left(\frac{\mathrm{P}_v^2}{\mathrm{MSE}} \right),$$

where P_v denotes the highest pixel value in the image and the MSE is the mean squared error (please refer to Section 4.6). A greater PSNR value denotes less noise in the reconstructed image, almost identical to the original image. Decibels (dB) are commonly used to represent PSNR, with higher dB values denoting higher quality in the reconstruction. Further, the PSNR between the original and corresponding ciphered image must be smaller than 10 dB. Further, the PSNR between the original and corresponding ciphered image must be smaller than 10 dB. Table 5 demonstrates the PSNR results for the pair of plain and encrypted images and the pair of plain and deciphered images. Infinite PSNR for all reconstructed images shows that the decryption is done without any data loss. All the PSNR for original and encrypted images is less than 10 dB.

The calculated MSE values between the original and decrypted images are zero because the original and decrypted images are identical, resulting in zero pixel differences. Since MSE appears in the denominator of the PSNR calculation formula, a zero value for MSE leads to PSNR being infinite.

Images	Layer	PSNR(Original,Encrypted)	PSNR(Original,Decrypted)
Flamingo	R	8.5229	∞
	G	9.4251	∞
	B	8.6502	∞
Tree	R	8.7208	∞
	G	7.6392	∞
	B	8.3032	∞
Scenery	R	9.5875	∞
	G	7.6436	∞
	B	7.6031	∞
Satellite	R	8.2847	∞
	G	8.2684	∞
	B	9.4805	∞
Wash	R	8.9852	∞
	G	9.7724	∞
	B	8.2380	∞
View	R	9.9852	∞
	G	10.2485	∞
	B	8.5585	∞

TABLE 5. The PSNR analysis

4.8. **Differential Attack.** Differential cryptanalysis is a technique that enables attackers to decrypt an image by comparing two encrypted versions of the images

i.e., firstly, the image obtained by directly encrypting the original image and the other by encrypting the image after making a slight modification to it.

4.8.1. *Number of Pixels Change Rate (NPCR).* The N.P.C.R. stands for the number of pixels change rate, and it is determined as [8]:

$$NPCR = \frac{1}{q \times p} \sum_{a=0}^{q-1} \sum_{b=0}^{p-1} d(a,b) \times 100\%,$$

where q & p are the width & height of the encrypted image, respectively. The function d(a,b) is defined as:

$$d(a,b) = \begin{cases} 0, & \text{if } O_1(a,b) = O_2(a,b) \\ 1, & \text{if } O_1(a,b) \neq O_2(a,b) \end{cases},$$

where O_1 is the encrypted image corresponding to the original image, and O_2 is the encrypted image corresponding to a slight change in the original image. If slight changes in the original image lead to major changes in the encrypted images, the system is robust against differential attacks. A higher N.P.C.R. implies a large change in the pixel values during encryption, which generally implies stronger encryption [2]. It helps in evaluating the effectiveness and robustness of encryption algorithms, and hackers might not be able to detect the small changes in pixel values, which could be significant in certain applications. We change only one pixel value in the original image to analyze the robustness of the authentication-based image encryption scheme against differential attacks. Hence, O_1 is the encrypted image corresponding to the original images, whereas O_2 is the ciphered image obtained corresponding to a single pixel change in the original image. The N.P.C.R. values (component-wise) for all the test images are presented in Table 6. All the calculated N.P.C.R. values are greater than 99.5%, assuring that the proposed scheme is anti-differential and has a negligible probability for hackers to find the relationship between the original image and the corresponding ciphered image. Hence, the proposed scheme is efficient and fully secure against differential attacks.

Sample image	N.P.C.R test results (%)			Average
	R	G	B	
Flamingo	99.5972	99.5972	99.5972	99.5972
Tree	99.6231	99.6231	99.6231	99.6231
Scene	99.5850	99.5850	99.5850	99.5850
Satellite	99.6140	99.6140	99.6140	99.6140
Wash	99.6078	99.6078	99.6078	99.6078
View	99.6292	99.6292	99.6292	99.6292

Table 6. N.P.C.R Test Analysis

4.8.2. *Unified Average Changing Intensity (UACI).* The UACI quantifies the mean change in pixel intensity between corresponding pixels in the two encrypted images [8]. It gives useful information on the efficiency and accuracy of encryption techniques for securing digital images. Mathematically, the UACI is calculated as:

$$UACI = \frac{1}{q \times p} \sum_{a=0}^{q-1} \sum_{b=0}^{p-1} \frac{|P'_{ab} - P_{ab}|}{L-1}, \tag{4}$$

where L is the maximum possible intensity of pixel value in the image. In the above equation, P'_{ab} and P_{ab} are the pixel values of the encrypted image P' corresponding to the original image and the encrypted image P corresponding to a slight change in the original image. In terms of pixel intensity, a lower U.A.C.I value suggests poorer encryption as it shows that both the encrypted picture P and P' are more similar to each other and provide a loophole for hackers. The quality of the encrypted picture may be impacted by a higher U.A.C.I score, which denotes more notable differences between encrypted images P and P'. As in Section 4.8.1, only a slight change is made in the original image to analyze the N.P.C.R values. In Equation 4, P is the encrypted image corresponding to the original images, whereas P' is the ciphered image obtained corresponding to a single pixel change in the original image. The U.A.C.I values (component-wise) for all the test images are presented in Table 7. All the calculated U.A.C.I values are greater than 33%, which assures that the slight change in the original image has made a significant difference and hence, the proposed scheme is anti-differential.

Sample image	U.A.C.I. test results (%)			Average
	R	G	B	
Flamingo	33.5279	33.4928	33.4818	33.5008
Tree	33.3270	33.3158	33.2987	33.3138
Scene	33.4890	33.4711	33.5679	33.5093
Satellite	33.4985	33.5286	33.4748	33.5006
Wash	33.4940	33.4422	33.4586	33.4649
View	33.4987	33.4464	33.4530	33.4660

TABLE 7. U.A.C.I test analysis

4.9. **The Entropy Analysis.** The measurement of entropy is used to describe the randomness in the texture of a picture [19]. Shannon entropy is computed by analyzing the probability distribution of the pixel intensities present in the digital image. For a grayscale image, with L (=256), the possible pixel intensities, entropy H is calculated using the formula:

$$H = -\sum_{i=0}^{L-1} p_i \log_2(p_i),$$

where p_i is the probability of occurrence of intensity level i in the image. For color images, entropy can be calculated for each color channel separately or for the image as a whole. Measuring the amount of randomness present in the encrypted picture is a common way to show how well the encryption method randomizes the image's actual information. An image with high entropy and close to 8 in its encryption is more complex and less predictable, potentially increasing the difficulty for attackers attempting to decipher the original content.

Images	Original			Encrypted		
	R	G	B	R	G	B
Flamingo	7.4537	7.1761	7.1691	7.9967	7.9969	7.9969
Tree	7.2104	7.4136	6.9207	7.9971	7.9973	7.9972
scenery	7.2587	7.6143	7.1892	7.9976	7.9972	7.9971
Satellite	7.5978	7.2823	6.8053	7.9973	7.9972	7.9972
Wash	7.1582	7.1582	7.1974	7.9972	7.9971	7.9971
View	6.5585	7.0233	7.0233	7.9967	7.9973	7.9971

TABLE 8. Entropy analysis of different images

The above table shows the entropy of the original and the encrypted image corresponding to their color components. As it represents that the entropy for both the original and the encrypted images is near 8, which is substantially high, it implies that the randomness in both images is well-maintained.

4.10. **Noise Attack Analysis.** Noise in digital images pertains to undesired fluctuations in pixel values that can potentially deteriorate the overall quality of the image [13]. Common types of noise include Gaussian noise, salt and pepper noise, and speckle noise. Noise may distort an image's quality and clarity, introduce inconsistencies, and conceal minute details. Strategies for handling noise attacks:

(1) Preprocessing techniques: Noise reduction filters (e.g., Gaussian filter, median filter) can be used as preprocessing techniques to decrease or eliminate the effects of noise before encryption.
(2) Robust encryption algorithms: Integrating noise-resistant features or procedures into encryption algorithms to make them immune to noise attacks.

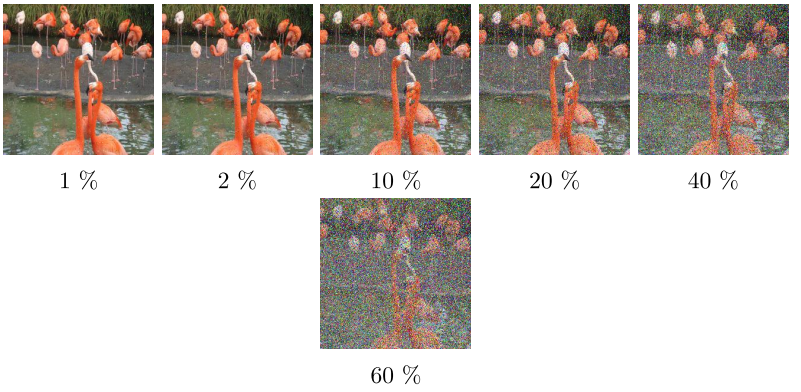


FIGURE 9. Noise attack analysis with different percentage

For the proposed scheme, different noise attack analyses have been carried out and results are presented in Figure 9. In the first image, the noise attack is 1%, which shows less impact on the image compared to the other images. The noise attack percentage varies from 1% to 60%, showing different impacts on each image. The image change has been increasing proportionally with the increase in attack percentage. 60% noise attack has the highest impact on the image. However, images are partially perceptible even in a larger presence of noise. Further, for the quantitative analysis of the quality of the extracted/decrypted images affected by noise, we calculated the PSNR between the original and the extracted images. The obtained PSNR results are presented in Table 9. From this table, it is evident that all the calculated PSNR values are greater than 10 dB, which demonstrates the clarity of the extracted images.

TABLE 9. Quantitative analysis of noise attack

Noise intensity	1%	2%	10%	20%	40%	60%
Calculated PSNR (dB)	28.6602	27.1206	21.2925	18.2156	15.0441	30.5496

4.11. **Cropping Attack.** Removing exterior portions of an image to enhance composition, concentrate on particular aspects, or frame is referred to as cropping [32]. A significant context or information from the original image may be lost during cropping. One may frequently hide or modify important information in an image using cropping techniques.

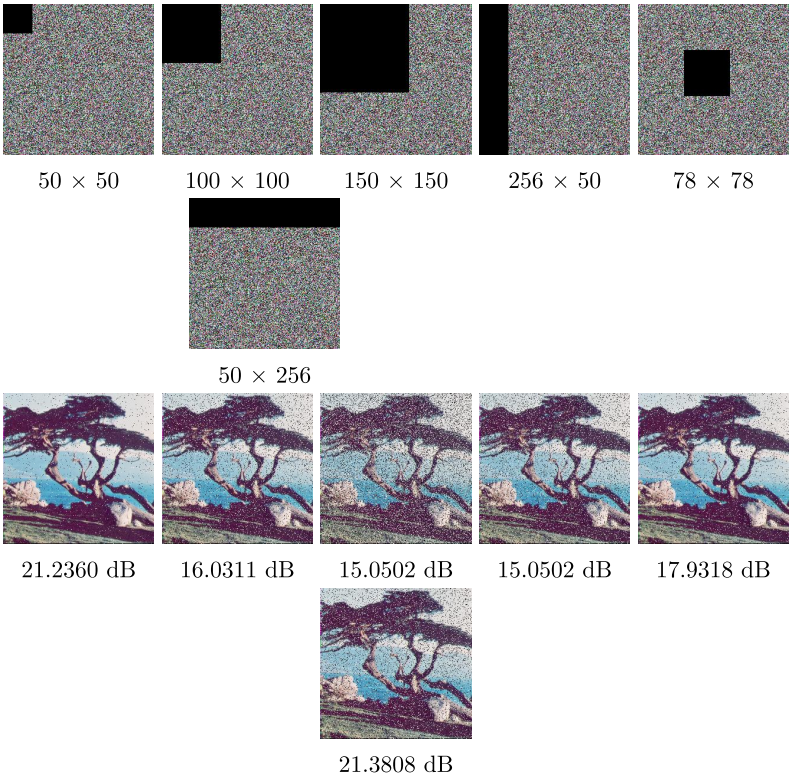


FIGURE 10. First row represents the crop attack on encrypted images whereas the second row represents the corresponding decrypted images

Cropping attack analysis shows that even after losing some part of the image, the rest of the figure can be rescued without any data loss. As in Figure 10, the first row represents the different cropping attacks on 256× 256 encrypted image. The second row shows the deciphered image of the cropped image, representing that even after a brute force attack on any part of the image from different positions, the data in the image can be restored, which makes the presented algorithm a good encryption scheme. Further, for the quantitative analysis of the quality of the extracted/decrypted images affected by cropping attack, we calculated the PSNR between the original and the extracted images. The obtained PSNR are provided in the caption of corresponding images in second row of Figure 10. From this, it is evident that all the calculated PSNR values are greater than 10 dB, which demonstrates the clarity of the extracted images.

4.12. **Computational efficiency analysis: complexity and encryption time.** The computational complexity analysis is important to implement a cipher scheme in real-world applications. The proposed scheme's computational complexity mainly depends on the following phases: generation of a digital signature using the RSA cryptosystem, confusion using Gingerbreadman map, diffusion using 2D-PSNCM

and permutation using Baker's map. The proposed scheme's execution time for all the RGB test images is demonstrated in Table 10. Where the encryption time is the combined time taken by the proposed scheme for the both stages encryption and digital signature generation. Computational complexity to implement the confusion over throughout the whole pixels of a $n \times n$ image by utilizing the Gingerbreadman map will be of order $O(n^2)$ because a chaotic sequence with n^2 elements is generated by the Gingerbreadman map during the confusion. Similarly computational complexity for the diffusion using 2D-PSNCM will be of order $O(n^2)$. The next phase is the permutation using Baker's map; the set of all pixel values in the image is partitioned, and the corresponding pixels are rearranged. Hence, the complexity of scrambling using Baker's map is of order $O(n^2)$. Further, during the digital signature generation, a hash value or message digest of length 'k' bits is generated, and the computational complexity for the RSA digital signature will be of order $O(k^2)$. Overall, the computational complexity for the proposed scheme is of order $O(3n^2+k^2)$. Since k is small as compared to n, the proposed scheme's computational complexity is approximated to $O(k^2)$.

Table 10. Proposed scheme's execution time (in Seconds)

Images	Encryption time (in seconds)	Decryption time (in seconds)
Flamingo	0.0791	0.0607
Tree	0.0778	0.0568
Scene	0.0816	0.0560
Satellite	0.0788	0.0545
Wash	0.0870	0.0541
View	0.0824	0.0565

4.13. **Protection Against Hacking and Security Threats.** The proposed approach protects against numerous hacking and security risks, including brute force, side-channel, and selected plaintext attacks. This robustness is primarily due to the usage of the SHA-256 hash function and the original image to generate the initial values employed in the encryption process. Since the proposed approach is plaintext-dependent, even a tiny change in the input plain image results in a completely different hash value, producing significant changes in the encrypted image. This sensitivity to plaintext ensures the encrypted output is unpredictable, making brute-force or chosen plaintext assaults infeasible. Furthermore, the multilayer encryption structure and the different chaotic maps applied add an extra layer of complexity, ensuring resilience against side-channel assaults.

4.14. **Comparative analysis.** This section extensively compares the proposed image authentication and ciphering scheme with some already developed approaches. The calculated results for the statistical protocols, including UACI, NPCR, entropy, SSIM, MSE, encryption time and PSNR, are used for the comparison. Corresponding results for the comparison are summarized in Table 11. The numerical simulation findings support the designed scheme's effectiveness and resilience against several current techniques.

TABLE 11. Comparative assessment of the proposed framework with existing techniques

Metrics	Enc time (s)	Entropy	DC	HC	VC	SSIM	NPCR	UACI
Ref. [12]	0.1300	7.9993	-0.0037	-0.0002	0.0006	-	99.7300	33.4500
Ref. [14]	3.0019	7.9968	-0.00151	0.00144	0.00795	-	99.6246	30.5681
Ref.[5]	2.5824	7.9970	-0.00132	0.002287	-0.00160	-	99.6287	30.3432
Ref.[6]	2.6371	7.9987	0.000013	0.00175	0.000024	-	99.6254	30.5681
Ref.[36]	25.3344	7.9580	0.0001	-0.0020	0.0001	0.0106	99.5865	28.6372
Ref.[39]	0.4598	7.9914	0.000627	-0.001627	0.000279	-	99.6060	33.4689
Ref. [43]	-	7.9958	0.0049	0.0054	0.0045	-	99.6205	33.4526
Proposed	0.0811	7.9970	0.0030	0.0045	0.0039	0.0018	99.6093	33.4592

5. Conclusion

The article presents encryption scheme by maintaining the level of confusion and diffusion using the Gingerbreadman map for confusion and the two-dimensional piecewise smooth non-linear chaotic map for diffusion. The obtained image is further confused by using Baker's map with suitable number of repetition. The RSA cryptosystem is used for the digital signature to verify the user's authenticity. Hence, the proposed scheme protects the image data from hackers as well as verify its authenticity. The proposed algorithm is shown step by step along with the flow chart. Then, the quality of the proposed work was tested by performing numerous tests, which showed the following results. Firstly, the histogram results shown in Figure 7 imply that the graph of the encrypted images is uniform, ensuring high randomness in the encrypted images. The histogram of an encrypted image is uniformly distributed, meaning that all gray levels in the image have nearly the same frequency. This uniformity implies that all pixel values have an equal probability of occurrence. Consequently, the encrypted image exhibits strong randomness, as the absence of discernible patterns ensures resistance to statistical attacks. Their corresponding Chi-square values are determined, and all Chi-square values are less than the critical values, which proves the randomness. Secondly, the proposed scheme has a high level of key sensitivity, which means that the process is highly sensitive to the key used, i.e., the decryption will not occur even if there is a slight change in the key at the time of decryption. Then, Table 3 shows that the original and encrypted images are highly uncorrelated, which makes it difficult for the attacker to find the relation between them. The mean square error (M.S.E.) for the original and decrypted images is 0, implying that the image is decrypted successfully without data loss. In contrast, their corresponding peak signal to noise ratio (P.S.N.R.) is ∞. Differential attacks, including N.P.C.R. and U.A.C.I analysis in Table 6 and Table 7. It shows that the difference between the encrypted image corresponding to the original one and the encrypted image corresponding to the single pixel value change in the original image are highly different. Figure 9 shows the variation of noise attack, which increases with the increasing percentage of the attack. However, extracted images are partially perceptible even in a larger presence of noise. Further, Figure 10 shows that the image data can be restored efficiently even after applying the cropping effects from different angles. Hence, the proposed authentication-based image encryption scheme can resist the different types of statistical attacks.

Limitations and Future Work

While the proposed approach successfully integrates RSA digital signature and multilayer chaotic encryption to secure both the confidentiality and authenticity of secret images, certain limitations remain. The computational cost/complexity or time complexity of RSA and multilayer chaotic encryption may pose issues for resource-constrained devices. Our further research could focus on refining the system for lightweight devices, extending it to video encryption, and enhancing resistance to modern cryptanalytic attacks while maintaining efficiency.

Declarations

Conflict of interest/Competing interest All authors declare that they have no conflict of interest.

Acknowledgement:

The authors are thankful to the DST, India, for support through grant no. SR/FST/MS-1/2021/104(C) under the DST-FIST project. We also thank the reviewers for their valuable comments, which greatly enhanced the quality of this manuscript.

Declarations

Conflict of interest/Competing interest All authors declare that they have no conflict of interest.

References

[1] Abd El-Latif, A. A., Li, L., Zhang, T., Wang, N., Song, X., and Niu, X. (2012). Digital image encryption scheme based on multiple chaotic systems. *Sensing and Imaging: An International Journal*, 13:67–88.

[2] Ahmad, J. and Ahmed, F. (2010). Efficiency analysis and security evaluation of image encryption schemes. *computing*, 23(4):25.

[3] Ahmad, M. and Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on computer science and engineering*, 2(1):46–50.

[4] Alam, S., Jamil, A., Saldhi, A., and Ahmad, M. (2015). Digital image authentication and encryption using digital signature. In *2015 International Conference on Advances in Computer Engineering and Applications*, pages 332–336. IEEE.

[5] Alexan, W., ElBeltagy, M., and Aboshousha, A. (2022). Rgb image encryption through cellular automata, s-box and the lorenz system. *Symmetry*, 14(3):443.

[6] Alexan, W., Elkandoz, M., Mashaly, M., Azab, E., and Aboshousha, A. (2023). Color image encryption through chaos and kaa map. *IEEE Access*, 11:11541–11554.

[7] Badawy, M. (2023). Security evaluation of different hashing functions with rsa for digital signature. *IJCI. International Journal of Computers and Information*, 10(2):99–116.

[8] Broumandnia, A. (2019). The 3d modular chaotic map to digital color image encryption. *Future Generation Computer Systems*, 99:489–499.

[9] Chen, J.-x., Zhu, Z.-l., Fu, C., Zhang, L.-b., and Zhang, Y. (2015). An efficient image encryption scheme using lookup table-based confusion and diffusion. *Nonlinear Dynamics*, 81:1151–1166.

[10] Coppersmith, D., Johnson, D. B., and Matyas, S. M. (1996). A proposed mode for triple-des encryption. *IBM Journal of Research and Development*, 40(2):253–262.

[11] Cristóbal, G., Schelkens, P., and Thienpont, H. (2013). *Optical and digital image processing: fundamentals and applications*. John Wiley & Sons.

[12] El Kaddouhi, S., Qobbi, Y., Abid, A., Jarjar, M., Zaaraoui, H., and Jarjar, A. (2024). A new image encryption approach that uses an improved hill-vigenère method and chaotic maps. *Multimedia Tools and Applications*, pages 1–29.

[13] Elghandour, A., Salah, A., and Karawia, A. (2022). A new cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal*, 13(1):101489.

[14] Elkandoz, M. T. and Alexan, W. (2022). Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications*, 81(18):25497–25518.

[15] Farajallah, M., El Assad, S., and Deforges, O. (2016). Fast and secure chaos-based cryptosystem for images. *International Journal of Bifurcation and Chaos*, 26(02):1650021.

[16] Gaffar, A., Joshi, A., and Kumar, D. (2020). Image encryption using gingerbreadman map and rc4a stream cipher. *Applications and Applied Mathematics: An International Journal (AAM)*, 15(2):30.

[17] Jaafar, A. M. and Samsudin, A. (2010). Visual digital signature scheme: a new approach. *IAENG International Journal of Computer Science*, 37(4):36–44.

[18] Jolfaei, A. and Mirghadri, A. (2010). An applied imagery encryption algorithm based on shuffling and baker's map. In *Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10), Florida, USA*, pages 279–285.

[19] Khan, M. and Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s 8 permutation. *Neural computing and applications*, 29:993–999.

[20] Luo, Y., Yu, J., Lai, W., and Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia tools and applications*, 78:22023–22043.

[21] Lyle, M., Sarosh, P., and Parah, S. A. (2022). Adaptive image encryption based on twin chaotic maps. *Multimedia Tools and Applications*, 81(6):8179–8198.

[22] Mali, K., Chakraborty, S., and Roy, M. (2015). A study on statistical analysis and security evaluation parameters in image encryption. *entropy*, 34:36.

[23] Mallouli, F., Hellal, A., Saeed, N. S., and Alzahrani, F. A. (2019). A survey on cryptography: comparative study between rsa vs ecc algorithms, and rsa vs elgamal algorithms. In *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pages 173–176. IEEE.

[24] Mandal, A. K., Parakash, C., and Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: Des and aes. In *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pages 1–5. IEEE.

[25] Mir, U. H., Lone, P. N., Singh, D., and Mishra, D. (2023). A public and private key image encryption by modified approach of vigener cipher and the chaotic maps. *The Imaging Science Journal*, 71(1):82–96.

[26] Mir, U. H., Singh, D., and Lone, P. N. (2022). Color image encryption using rsa cryptosystem with a chaotic map in hartley domain. *Information Security Journal: A Global Perspective*, 31(1):49–63.

[27] Mondal, B., Kumar, P., and Singh, S. (2018). A chaotic permutation and diffusion based image encryption algorithm for secure communications. *Multimedia Tools and Applications*, 77(23):31177–31198.

[28] Nguyen and Shparlinski (2002). The insecurity of the digital signature algorithm with partially known nonces. *Journal of Cryptology*, 15:151–176.

[29] Pareek, N. K., Patidar, V., and Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and vision computing*, 24(9):926–934.

[30] Prajwal, H. N. et al. (2023). Digital signature algorithm: A hybrid approach. *International Journal of Advanced Computer Science and Applications*, 14(3).

[31] Prajwalasimha, S., Kumar, A. V., Arpitha, C., Swathi, S., and Spoorthi, B. (2019). On the sanctuary of a combined confusion and diffusion based scheme for image encryption. *International Journal of Engineering and Advanced Technology*, 9(1):3258–3263.

[32] Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., and Rayappan, J. B. B. (2017). Fusion of confusion and diffusion: a novel image encryption approach. *Telecommunication Systems*, 65:65–78.

[33] Qadir, A. M. and Varol, N. (2019). A review paper on cryptography. In *2019 7th international symposium on digital forensics and security (ISDFS)*, pages 1–6. IEEE.

[34] Rahul, B., Kuppusamy, K., and Senthilrajan, A. (2023). Dynamic dna cryptography-based image encryption scheme using multiple chaotic maps and sha-256 hash function. *Optik*, 289:171253.

[35] Ranjan, R., Mukherjee, A., Rai, P., and Ahmad, K. (2019). Asymmetric cryptography. In *Emerging Security Algorithms and Techniques*, pages 119–137. Chapman and Hall/CRC.

[36] Sheela, S., Suresh, K., and Tandur, D. (2018). Image encryption based on modified henon map using hybrid chaotic shift transform. *Multimedia Tools and Applications*, 77:25223–25251.

[37] Singh, M., Kaur, H., and Kakkar, A. (2015). Digital signature verification scheme for image authentication. In *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, pages 1–5. IEEE.

[38] Sridevi, A., Sivaraman, R., Balasubramaniam, V., Sreenithi, Siva, J., Thanikaiselvan, V., and Rengarajan, A. (2022). On chaos based duo confusion duo diffusion for colour images. *Multimedia Tools and Applications*, 81(12):16987–17014.

[39] Teng, L., Wang, X., and Xian, Y. (2022). Image encryption algorithm based on a 2d-clss hyperchaotic map using simultaneous permutation and diffusion. *Information Sciences*, 605:71–85.

[40] Varshney, A., Routh, P., and Sujatha, G. (2024). Comparison of image encryption techniques using chaotic maps and conventional cryptographic techniques. In *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, pages 1–7. IEEE.

[41] Walia, A. G. N. K. (2014). Cryptography algorithms: A review. *International Journal of Engineering Development and Research*, 146.

[42] Yang, H., Wong, K.-W., Liao, X., Zhang, W., and Wei, P. (2010). A fast image encryption and authentication scheme based on chaotic maps. *Communications in*

Nonlinear Science and Numerical Simulation, 15(11):3507–3517.

[43] Ye, G., Jiao, K., and Huang, X. (2021). Quantum logistic image encryption algorithm based on sha-3 and rsa. *Nonlinear Dynamics*, 104:2807–2827.

[44] Yildirim, M. (2021). A color image encryption scheme reducing the correlations between r, g, b components. *Optik*, 237:166728.

[45] Yun-Peng, Z., Wei, L., Shui-Ping, C., Zheng-Jun, Z., Xuan, N., and Wei-Di, D. (2009). Digital image encryption algorithm based on chaos and improved des. In *2009 IEEE international conference on systems, man and cybernetics*, pages 474–479. IEEE.

Sandeep Kumar: 1. Department of Mathematics, Akal University, Talwandi Sabo, Bathinda (Punjab), 151302; 2. Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401

Email address: sandeepkumarsvr@gmail.com

Khushi: Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401

Email address: khushiwadhwa0207@gmail.com

Deep Singh: 1. School of Undergraduate Studies, Dr. B. R. Ambedkar University Delhi, Kashmere Gate, Delhi, 110006; 2. Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401

Email address: deepsinghspn@gmail.com