RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt2615

Multilayer Colour Image Encryption Scheme Based on Discrete Compound Chaotic Map and S-box

Deep Singh [a, b], Lalthazuala [b], Sandeep Kumar [c, b], Jatinder Kumar [d], Amit Paul [d, *]

[a] School of Undergraduate Studies, Dr. B. R. Ambedkar University Delhi, Delhi 110006, India
[b] Department of Mathematics and Statistics, Central University of Punjab, Bathinda, 151401, India
[c] Department of Mathematics, Akal University, Talwandi Sabo, Bathinda (Punjab), 151302, India
[d] Department of Mathematics, Guru Nanak Dev University, Chheharta, Road, Amritsar, 143005, India
* Corresponding Author Email: amitpaulcuj@gmail.com

DOI: https://doi.org/10.54392/irjmt2615
Received: 27-07-2024; Revised: 13-12-2025; Accepted: 25-12-2025; Published: 13-01-2026

Abstract: In today's technological age, ensuring the security of data transmitted across unsecured and open channels from one destination to another is an important issue. Strong techniques to protect images during transmission and storage are becoming more and more critical as the digital age advances. The main focus of the presented work is to enhance the protection of digital image data from unapproved sources over these open networks. It is possible that conventional encryption methods may not provide enough protection against contemporary cryptographic attacks. Thus, this study proposes an encryption method that combines the cryptographic properties of S-boxes and Baker's map together with the chaotic dynamics of the discrete compound chaotic (DCC) map. During encryption, the level of confusion and diffusion is well maintained. The confusion is achieved by employing the chaotic sequence obtained from the DCC map and through the use of Baker's map. The S-box and a DCC map are utilized for diffusion purposes. Further, to achieve a better scrambling effect, Baker's map is implemented multiple times (n_b k times). The innovation of the proposed scheme lies in its novel integration of the discrete compound chaotic map (DCC map) with the cryptographic properties of S-boxes and Baker's map, achieving an enhanced level of diffusion and confusion in encrypted images. Further, the hashSHA−256 utilized to derive initial conditions ensures the dependency of the proposed scheme on the original image, offering a robust defence against differential attacks and providing a more secure framework than traditional encryption techniques. The strong proposed scheme's capability was demonstrated via the following key results: average entropy value of 7.9971, low correlation coefficients in the encrypted images, high MSE values, average encryption time of 0.2599 seconds, UACI of 33.4765, NPCR of 99.6113, successful decryption without data loss. These statistical and simulation analysis results confirm the scheme's efficiency, high security, and robustness.

Keywords: S-Box, Discrete Compound Chaotic Map, Baker's Map, Confusion-Diffusion

1. Introduction

The rapid advancement in open communication networks and digital technologies has improved people's communication quality in their professional lives and working environments. In today's digital era, electronic storage and digital data sharing are increasing exponentially over unplugged and open channels. Parallely, cyber threats and data hacking are becoming more popular due to the increase in dependency on online open platforms for data storage, manipulation, and communication. The hackers can severely harm the interests of communication parties' attempts through the use of the network's openness and sharing characteristics to intercept sensitive information. Therefore, developing a highly efficient technology for secure information communication is necessary. Cryptography is a tool that ensures the security of such digital data over open networks by transforming it into meaningless forms of data. It has been used for many years, and its importance has increased to the maximum in today's present era. It is being used in ATM cards, computer passwords, online transactions, e-commerce, etc.

The digital image is the form of digital data that is utilized in almost every field, including defences, medical services, the education sector and law enforcement, and ensuring their security is crucial. For the security, integrity and confidentiality of sensitive digital photos, robust and efficient cryptosystems are needed [1]. A number of techniques have been developed for secure transmission of digital image data

based on chaos theory [2-5] RSA cryptosystem [6], DNA coding [7-9], elliptic curve cryptography [10, 11] and S-box [12-15]. As stated by Shannon [16], the principles of diffusion and confusion form the core stages of a strong image encryption scheme, ensuring high-level security for digital image data. Confusion refers to the permutation of pixels, where their positions are shuffled across the image without altering their actual values. The goal of confusion is to maximize the degree of complexity in the interaction between the plaintext and the cipher text. On the other hand, diffusion occurs if there is a direct change in the plaintext character to obtain corresponding ciphertext characters. In the context of encryption of digital images, the goal of diffusion is to change the pixel value of the original image to generate a significant corresponding pixel value for the cipher image.

Nowadays, chaotic maps are popularized in the field of image security because of their inherent properties, such as ergodicity, complex dynamic behaviour, and high sensitivity towards initial conditions, making them well-suited for designing robust encryption algorithms. Chaotic maps are the mathematical functions that produce a wildly random pattern corresponding to a given set of initial values and secret key parameters [17]. Chaotic maps are helpful in many branches of science, such as mathematics, biology, and physics, among many other fields. To in- duce confusion and diffusion in image pixel values, most encryption schemes make use of chaotic maps.

In [2], Fu *et al.* developed an image ciphering technique with enhanced security that uses the hyperchaotic Lorenz system for diffusion and permutation, whereas the chaotic Baker map is used for permutation purposes. In [3], Farah et al. proposed a novel hybrid chaotic map and an alternative method for enhancing the efficiency of ciphering algorithms utilizing optimization techniques. In [4], Belazi et al. introduced a novel chaos-based image cryptosystem that blends a hyper-chaotic, sensitive, and non-linear system with the mastery of grey codes. A new multiprocess digital data ciphering approach utilizing a hyperchaotic linked sine map was proposed by Shi *et al.* in [5]. Kumar *et al.* [18] presented an image encryption method that utilizes chaotic maps. In [20] [19], Kumar *et al*. introduced a method for multiple-image encryption (MIE) that combines DNA-based diffusion, dynamic permutation, and a unique exponent-sine- cosine (ESC) chaotic map. In [20], Yuqin et al. proposed a revolutionary double chaotic system- based image encrypting technique. In [21], Salleh et al. presented a parameter-varying Baker map (PVBM) with a non-stationary output signal. Tong *et al.* [12] introduced a novel image encryption technique based on the compound chaos theory. Similarly, Xiang *et al.* [22] developed a block cryptographic method that relies on the iteration of chaotic maps. In [23], Thomas *et al*. presented an image ciphering technique that uses the XOR operator combined with a chaotic function. In [24] Wang *et al.* used chaos theory to create a unique color image ciphering scheme. A novel multi-phase image encryption algorithm that combines the RSA cryptosystem with a MRMAC-(modified random matrix affine cipher) is introduced in [6]. In [25], Kumar *et al.* demonstrated an image security technique utilizing MSVD and DCST. In [26], Masood et al. introduced a creative privacy-preserving technique to safeguard private data contained in images.

In [27], D. Chatterjee et al. developed a chaos-based cryptosystem by employing a modified 2-D Baker's map is used for pixel permutation, while diffusion is achieved through a logistic map, which enable secure and efficient greyscale image encryption. In [28], A. Hussain et al. integrate three discrete chaotic maps, Arnold cat map, Logistic, and Baker's maps, in combination with the 3DES algorithm to build a strong and optimized scheme for image encryption. In [29], Sudevan et al. utilize Baker's map for efficient pixel scrambling and the 2D-LSCM (logistic sine coupling map) to enhance diffusion for telehealth data protection. In [30], E. Naeem *et al.* employ a combination of Henon map and Baker's map to achieve both diffusion and permutation in encrypting few-detail images. Further, XOR and permutation operations are integrated with high-detail images as a key to enhancing security.

The S-boxes are cryptographic components commonly used in ciphering techniques like AES (Advanced Encryption Standard). The S-boxes can contribute to image encryption by using non-linearity and enhance the level of diffusion by substituting key-dependent pixel values. In [12], Ding *et al.* introduces a productive method to create a static S-box by combining the cellular automata. In [13], Usama et al. presented a technique for building an effective key- dependent S-box that relies on the chaotic sine map's mixed characteristics. In [14], Khan et al. proposed an effective process for producing highly non-linear cryptographic S-box for algebraic and chaotic construction techniques. Authors in [15], presented a novel technique for creating a random bijective S-box utilizing discrete chaotic maps. Yi *et al.* [31] designed a novel S-box by employing the Baker map, sinusoidal chaotic map, compound chaotic map, and linear congruence generator. In [32], Liu et al. presented an innovative way of building a random S-box utilizing the spatiotemporal non-linear chaotic system. In [33], Ullah et al. proposed replacement boxes using the linear fractional transformation and chaotic system. Patidar *et al.* [34] introduced a well-known substitution-diffusion framework that incorporates chaotic standard and logistic maps. In a separate study, Yang *et al.* [35] proposed a color image encryption technique that employs a multi-objective optimized S-box along with a 2D sine-logistic-Gaussian (2D-SLG) coupled chaotic map

In [36], Ali *et al.* demonstrate digital photos ciphering scheme by introducing a novel generator that

integrates algebraic modelling with chaotic mapping, producing highly secure and diverse S-boxes with minimal computational overhead. Ustun *et al.* [37] introduced an image encryption method that integrates a novel S-box, designed using real-coded genetic algorithms, with a two- dimensional hyperchaotic Styblinski–Tang map. In another study, Ali *et al*. [38] enhanced the security and randomness of image encryption by combining a novel S-box with the CAST block cipher, along with 2D and 3D logistic chaotic maps. Additionally, Zheng *et al.* [39] developed a dynamic S-box based on chaotic maps to improve image security. Despite the advancements in encryption techniques and the increase in open network communication, many existing methods face challenges, including insufficient defense against statistical and brute-force attack methods and vulnerability to cryptanalytic attacks. Considering the critical need for safe transfer of digital images through public communication channels, this manuscript presents a multilayer color image encryption scheme that enhances image security against unauthorized access.

Authors in [40] developed a Arnold transform based quantum color image ciphering via storage to QRCI. Singh *et al.* [41] developed a RSA based grayscale, binary and color image ciphering technique. Authors in [42], developed an image encryption technique utilizing newly generated chaotic map. Singh *et al.* in [43], utilized the MHM and RSA for the partial ciphering before the embedding process. A block compressive sensing based image ciphering technique developed in [44].

The primary goal of the present manuscript is to develop a secure and robust ciphering scheme that prevents unauthorized access to digital image data. The color component images get extracted initially from a given RGB image. These component images are separately ciphered by employing the compound chaotic map, S-box and Baker's map. The whole encryption is based on multiple iteration of diffusion and confusion among the pixel values presented in the original image. The motivation to combine these specific encryption methods lies in their complementary strengths: Baker's map generates high scrambling effects due to its ergodic properties, while the DCC map and S-box provide robust confusion and diffusion capabilities, enhancing resistance against almost every cryptographic attack. This integration ensures an optimal balance of diffusion and confusion, crucial for protecting image ciphering in the face of evolving security threats.

The manuscript continues with the following section-wise breakdown: Basic theories related to chaotic maps along with the algorithm of designing the S-box by utilizing the polynomial mapping, are provided in Section 2. The decryption and encryption algorithms for the current scheme is demonstrated step by step in Section 3. Lastly, Section 4 and Section 5 provide the proposed scheme's security analysis and conclusion, respectively.

2. Basic Theory

2.1 Discrete sine map

The sine map is a trigonometry function based chaotic map and is defined as follows

$$\xi_{n+1} = \frac{\beta * \sin(\pi * \xi_n)}{4} \quad (1)$$

where ξ_{n+1} and ξ_n are the map's outputs in the range (0, 1) for $(n + 1)^{th}$ and n^{th} iterations, respectively, and β is the secret key parameter with range (3.5, 4) that describes the sine map's chaotic area [45].

2.2 Logistic Map

One of the most famous chaotic maps is the logistic map, and is defined as

$$\xi_{n+1} = r \times \xi_n \times (1 - \xi_n) \quad (2)$$

where ξn is the value of the variable at n^{th} iteration and lies in the range $0 \leq \xi_n \leq 1$. The parameter *r* controls how the map behaves.

2.3 Discrete compound chaotic (DCC) map

The DCC is a combined extension of sine map and logistic map [30]. Mathematical form for the discrete compound map is described as follows:

$$\xi_{n+1} = \frac{4\beta}{9} \times \xi_n \times (1 - \xi_n) + \frac{9-\beta}{9} \times sin(\pi \times \xi_n) \quad (3)$$

where β is the secret parameter. The DCC map has a chaotic nature for the range $0 \leq \beta \leq 9$. The map's outputs lies in the range (0, 1) for $(n + 1)^{th}$ and n^{th} iterations, are ξ_{n+1} and x_n respectively. The compound system generates the sine map for β = 0. The proposed scheme selects the DCC map for its complex, chaotic behavior, which provides higher sensitivity to initial conditions and extends the key space by maintaining the computational complexity and processing time. These properties are essential in real-world applications, as well as in preserving diffusion and resisting brute force and differential attacks.

2.4 Baker's map

According to the theory of dynamical systems, the Baker's map is a chaotic bijection that transforms a unit square into itself. It bijectivity maps a square matrix of dimensions N ×N onto the same space and is also known as a discrete two-dimensional Baker's map. By rearranging the pixel locations, this map is utilized in the field of digital two-dimensional data security to decrease the adjacent pixel's correlation [2]. Steps followed for Baker's map-based image ciphering for scrambling of the pixel values are as follows [46]:

1. In the beginning, an image with a size of N × N is divided into *l* vertical rectangles with dimensions {n_i × N }. The width numbers {n_i} satisfies the following conditions:

   a) Each n_i must divides N for all i,

   b) Width sum is N.

2. Each i[th] vertical rectangle is further divided into the n_i sub-rectangles containing N pixels and having dimension N

3. These sub-rectangles are stratched to form a row of N pixels and put rows one by one bottom to top for getting a scrambled image.

To demonstrate it mathematically, let us define N_0, N_1, ... N_l with the help of the width of the above vertical rectangles (i.e. n_0, n_1, n_2, ... $n_{(l-1)}$) as follows

$$N_i = \begin{cases} 0 & if\ i = 0 \\ n_0, n_1, n_2, \dots\ n_{(i-1)}) & if\ i = 1, 2, \dots\ l \end{cases} \#\qquad (4)$$

Let us consider the image's pixels having position (u, v). Corresponding to this position (u, v), there is some $i_1 \in \{0, 1, 2, \dots\ l - 1\}$ such that $N_i 1 \le u \le N_{(i1+1)}$. The new pixel position (α, β) after applying the Baker's map to the picture element at coordinates (u, v) is calculated as

$$(\alpha, \beta) = \left(\frac{N}{n_i}(u - n_i) + v mod\frac{N}{n_i}, \frac{n_i}{N}\left(v - v mod\frac{N}{n_i}\right) + N_i\right) \qquad (5)$$

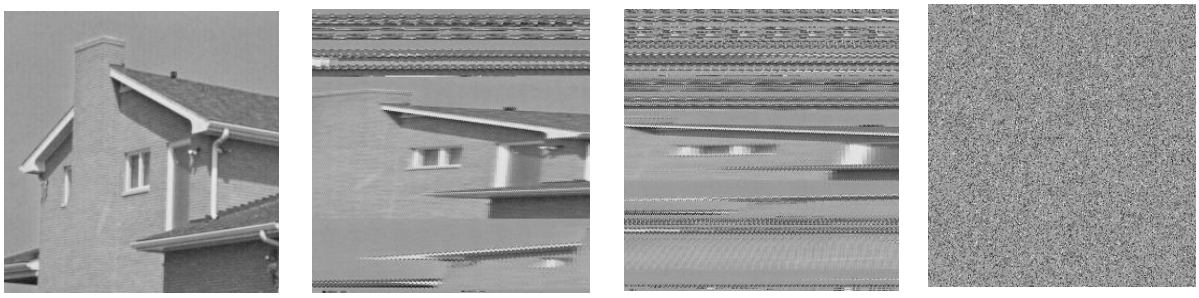
After repeating a few iterations, the discrete Baker maps produces efficient and highly encrypted image by improving pixel scrambling effect. Figure 1 demonstrates that how scrambling effect increases by increase in the iteration numbers of the Baker's map: (a) is test image and (b),

(c) & (d) are encrypted images with number of iteration r = 1 r = 2 & r = 10 respectively. Further, 1 presents the quantitative analysis of the scrambling effect based on the Peak Signal-to- Noise Ratio (OE_{PSNR}) and correlation metrics as the number of iterations (r) of the Baker map increases. Both OE_{PSNR} and correlation decrease with higher iterations, indicating enhanced scrambling and reduced similarity to the original image.

In the proposed scheme, Baker's map is chosen for its superior pixel scrambling capabilities, which are highly crucial in achieving a significant level of pixel permutation. Additionally, its ability to be iteratively applied allows for superior flexibility in optimizing the scrambling effect.

2.5 The S-box and its algebraic structure

The S-box is a fundamental component of a symmetric key cryptographic methods (like block ciphers). Its functioning is simply based on a table, and replacement of input values with matching output values from the table according to some specified algorithm. Mathematically, the S-box is a non-linear bijective function used in cryptographic algorithms to maintain the level of substitution. It maps the given input values from one finite set F_1 to another finite set F_1, defined as S: $F_1 \rightarrow F_2$, to achieve non-linearity. Its properties, including high non-linearity and avalanche effect, significantly enhance the diffusion process in the image encryption scheme.



(a) Original (r=0) (b) r =1 (c) r =2 (d) r =10

Figure 1. Result obtained by applying different iterations of the Baker's map

Table 1. Analysis of the dependency of scrambling effect on the number of iteration via PSNR and correlation

Metric	Number of iteration (r)			
	r = 0	r = 1	r = 2	r = 10
Cor_{Diag}	0.9126	0.7112	0.3972	-0.0020
Cor_{Ver}	0.9353	0.7049	0.3702	0.0018
Cor_{Hor}	0.9671	0.9124	0.6939	0.0031
OE_{PSNR}	inf	15.1497	14.9188	15.1088

For the proposed method, algebraic polynomial mapping [47] is utilized to generate the S-box is as follows:

Step 1. Consider a polynomial mapping $A: T \rightarrow T$ defined as

$$A(t) = \beta(t)^m + \gamma\big(mod(2^n + 1)\big), \beta, \gamma, t \in T \quad (6)$$

Where T is the set of 2^m elements

$$T = \{0,1,2,3, \ldots, 2^n - 1\}$$

And m is chooses from the set M,

$$M = \{2,\ 6,\ 10,\ 14,\ \ldots\ 254\}$$

Further, the parameters β and γ must satisfies the following conditions to create an $n \times n$ S-box

$$\gamma \in T - \{0\},\ \beta(t)^m + \gamma \neq 0.$$

Step 2. Choosing $n = 8$ and $m = 2$ to create a 8×8 matrix and for these values the above polynomial mapping becomes

$$A(t) = \beta(t)^2 + \gamma\big(mod(2^8 + 1)\big), \beta, \gamma, t \in T \quad (7)$$

Step 3. Now β, γ ∈ T, to understand the further generation of the S-box, let us consider as an example for the values of β and γ (viz., $\beta = 5$ and $\gamma = 2$), then the corresponding polynomial mapping becomes

$$A(t) = 5^2 + 2\big(mod(257)\big)\ t \in T. \quad (8)$$

Step 4. After solving the above equation under $mod\ 257$, the obtained elements forms a set $Z = \{z_1,\ z_2,\ \ldots\ z_n\}$.

Step 5. In order to restrict every element inside the range of 0-255, substitute $z_i - 1$ for each z_i.

Step 6. Construct a list of every missing components in the set *Z* and write in the descending order, say $\{t_1, t_2, \ldots\ldots, t_n\}$. Similarly, obtain a list of repeated elements by placing them in ascending order, say $\{u_1, u_2, , , , u_n\}$.

Step 7. In order to maintain the S-box's bijective, replace each t_j with u_j.

Step 8. After the above replacement of elements, rearrange the output into a square to produce the initial S-box [47].

Step 9. Initial S-box's elements are repositioned using permutations from the symmetric group S_{256}, which is employed to improve the initial S-box's randomness.

Step 10. After applying above multi-stage confusion in the initial S-box, the final S-box is obtained as presented in Table 2.

3. Proposed encryption algorithm

The proposed method utilizes Baker's map-based confusion, S-box-based substitution, and the discrete compound chaotic (DCC) map-based diffusion and confusion. In the proposed encryption scheme, Baker's map and the DCC map are selected for their distinct strengths in achieving image confusion and diffusion, respectively. Baker's map is used to introduce confusion by effectively scrambling pixel positions, which disrupts the spatial correlation among adjacent pixels, as demonstrated in Table 1. This scrambling ability makes Baker's map well-suited for the confusion stage. Further, the DCC map is applied for diffusion due to its complex, chaotic dynamics, which enable substantial pixel value alterations across the image, enhancing the encryption scheme's robustness against differential and statistical attacks. The step-by-step proposed algorithm is provided below, and the corresponding flow chart is picturized in Figure 2.

Table 2. Resultant S-box obtained from the polynomial mapping

217	144	246	56	208	50	154	148	30	22	59	251	95	123	4	199
152	104	249	160	52	105	216	85	17	169	86	159	161	178	222	227
188	231	225	96	162	136	124	138	224	116	245	143	127	204	228	132
33	37	11	248	57	82	133	238	164	113	115	66	77	130	71	198
76	201	155	112	168	234	49	68	226	250	16	220	141	190	88	81
180	40	21	53	102	94	209	183	252	117	147	108	146	48	2	1
75	13	173	156	63	47	7	25	189	167	125	34	145	192	128	55
5	65	103	93	41	29	12	137	43	171	153	58	212	175	149	92
186	214	78	89	60	223	131	107	135	197	174	31	244	203	97	213
42	51	185	111	36	184	241	170	134	27	179	177	70	99	80	110
229	44	90	100	219	87	206	24	242	254	176	79	129	210	32	23
8	236	150	18	255	121	62	28	19	139	172	163	215	247	193	6
196	67	38	194	83	243	232	101	151	165	202	120	0	84	142	46
211	200	158	26	54	221	64	20	72	114	207	157	218	195	98	69
240	205	235	237	91	191	45	126	122	61	253	109	181	118	230	9
106	187	73	233	166	10	74	140	239	15	14	182	35	3	119	39

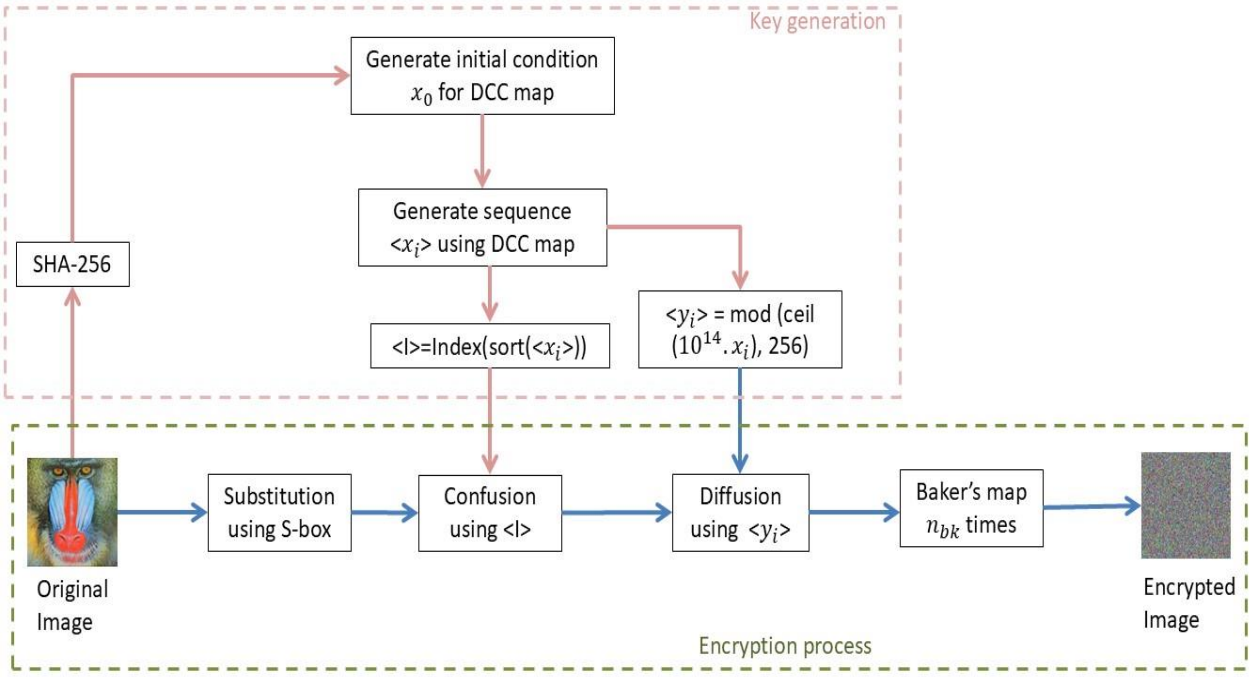


Figure 2. Flow chart of the proposed ciphering method

3.1 Initial condition generation

Step 1. Apply the $\mathrm{Hash}_{\mathrm{SHA-256}}$ to the test image (H) to obtain the hash value, say H_0.

Step 2. Convert the hash value H_0 to a decimal number in the range (0,1), and store it to x_0.

Pre-encryption process: generation of chaotic sequences

Step 3. Generate a S-box with the help of algebraic polynomial (please refer to Section 2.5), and store it to a matrix δ.

Step 4. Generating a sequence $< \mathrm{x_n} >$ by discrete compound chaotic and by utilizing initial condition $\mathrm{x_0}$ generated in Step 2 (please refer to Section 2.3).

Step 5. Sorting the elements of the sequence $< \mathrm{x_n} >$ and store corresponding indexes to the sequence $< \mathrm{I_1} >$ as

$$\mathrm{I_1} = \mathrm{index}\big(\mathrm{sort}(< \mathrm{x_n} >)\big) \qquad (9)$$

Step 6. Multiplying to each elements of the sequence $< \mathrm{x_n} >$ by 10^{14}, and reduce the numbers in the range 0 to 255 by taking *mod 256*. Storing the obtained sequence as $< \mathrm{y_n} >$

$$< \mathrm{y_n} \geq \mathrm{mod}(< \mathrm{x_n} > \times 10^{14}, 256).$$

Segregate the color components

Step 7. Take the original image H and segregate it into three color components, viz., $\mathrm{H_R}$, $\mathrm{H_G}$ and $\mathrm{H_B}$.

Step 8. Take the red component $\mathrm{H_R}$ of the original image.

Layer wise encryption:

Step 9. Apply S-box via matrix δ (obtained in Step 1) to the component image $\mathrm{H_R}$ for substitution of pixel values and modified component image $\mathrm{H_{R1}}$ is obtained.

Step 10. Apply confusion to $\mathrm{H_{R1}}$ with respect to the index sequence $< \mathrm{I_1} >$ obtained in Step 3, to produce partial encrypted image $\mathrm{H_{R2}}$.

Step 11. Create diffusion among pixel values by taking *bitXOR* to $\mathrm{H_{R2}}$ with the sequence $< \mathrm{y_n} >$ obtained in Step 4 to produce the ciphered image $\mathrm{H_{R3}}$.

Step 12 Apply $\mathrm{n_{bk}}$ times the Baker's map to $\mathrm{H_{R3}}$, that produces the final ciphered component image $\mathrm{C_r}$ (please refer to Section 2.4).

***Step 13*.** Repeat Step 8 to Step 12 for green and blue components (i.e. for $\mathrm{H_G}$ and $\mathrm{H_B}$) to gets the ciphered green component $\mathrm{C_g}$ and ciphered blue component $\mathrm{C_b}$, respectively.

Concatenating the components

Step 14. Combine $\mathrm{C_r}$, $\mathrm{C_g}$ and $\mathrm{C_b}$ to obtain the final coloured ciphered image $\mathrm{C_{rgb}}$

$$C_{rgb} = cat\big(3, C_r, C_g, C_b\big).$$

4 Result simulation and security analysis

A series of experimental and statistical analyses were carried out to establish the proposed scheme's efficiency and robustness. The output results, along with the detailed analysis are summarized throughout this section. Initially, all the test images (viz. Baboon $(Test_{im_1})$, House ($Test_{im_2}$), Aeroplane ($Test_{im_3}$), Capsicum ($Test_{im_4}$), Splash ($Test_{im_5}$) and Nature ($Test_{im_6}$)) over which the developed technique is employed are provided in Figure 3, and corresponding output ciphered pictures ($Teste_{im_i}$) are demonstrated in Figure 4. The resultant images for the decryption ($Testd_{im_i}$) are identical to the original images ($Test_{im_i}$) given in Figure 3. The potential of the developed technique is highlighted by the level of image reconstruction accuracy, which is an essential requirement for a secure and robust image ciphering scheme. In this section a deep analysis of the statistical experiments is presented.

4.1 Key space

The term 'key space' defines the complete range of available keys and secret parameters that are associated with a cryptographic algorithm [48]. The key space is often made to be sufficiently large to prevent an attempt to discover the key used to encrypt a message. The main goal of the cryptosystem is to eliminate the exhaustive key search attack by having a bigger key space (superior to 2^100). For the developed technique, parameters α, β and permutation from S_256 utilized to generate S-box; initial conditions x_0 and β1 are utilized in discrete compound chaotic map; width of rectangles { $n_0, n_1, n_2, \ldots n_{(l-1)}$} and number of iteration n_bk for the Baker's map are used secret keys and parameters. The initial condition x_0 and parameter β1 both having the precision of $10^{(-14)}$, and total contribution towards the key space is 10^28. As per the generation of the S-box in the developed technique it depends on some random permutation of order 256. Since, all the entries of the generated S-box are permutable, it contributes 256!. The width of l rectangles in the Baker's map { $n_0, n_1, n_2, \ldots n_{(l-1)}$} are selected from the Z_n, and it applies iteratively n_bk times, it contributes $n_bk \times n^l$. The total key space size for the proposed scheme is the product of the key spaces of each component, i.e. $10^{28} \times 256! \times n_{bk} \times n^l$. Which exceeds the required ideal key space size (2^{100}), and the developed technique having enough efficiency to defend key search attacks.

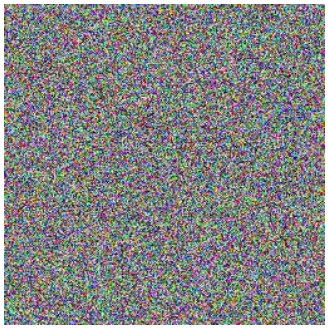
4.2 Key sensitivity

Key sensitivity (KS) concerns the way a slight change in the encryption (even a change in a single key by keeping the same algorithm and maintaining the rest of the keys) key affects the decrypted image.

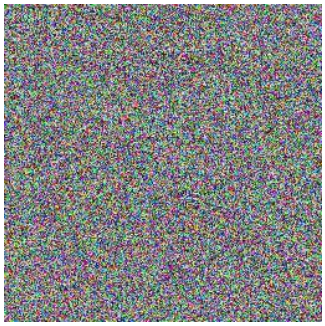
(a) Baboon **(b)** House **(c)** Aeroplane

(d) Capsicum **(e)** Splash **(f)** Nature

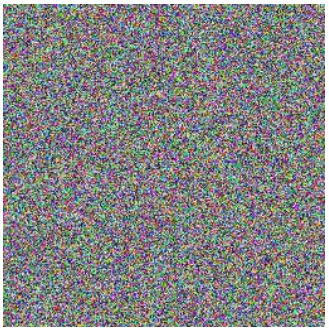
Figure 3. Set of color (RGB) secret test images, each of size 256×256 pixels



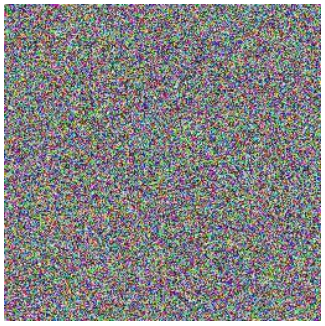
(a).Baboon: $PSNR = 8.98459, MSE = 8.46216 \times 10^3$



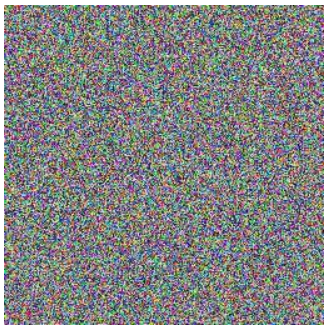
(b).House: $PSNR = 8.97840, MSE = 9.03173 \times 10^3$



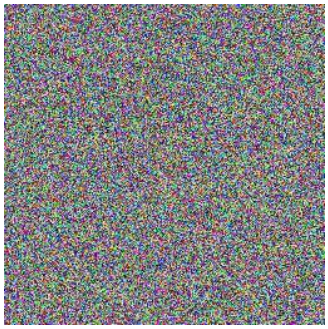
(c) Aeroplane: $PSNR = 8.01380, MSE = 9.66792 \times 10^3$



(d)Capsicum: $PSNR = 8.97840, MSE = 10.08708 \times 10^3$



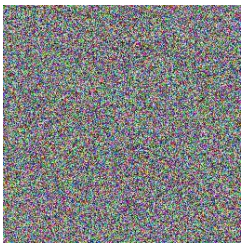
(e) Splash: $PSNR = 7.67335, MSE = 9.92048 \times 10^3$



(f) Nature: $PSNR = 8.20989, MSE = 10.33508 \times 10^3$

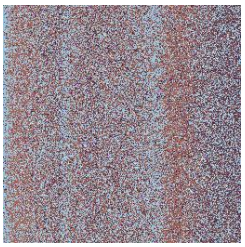
Figure 4. Set of ciphered images corresponding to plain test images given in Figure 3. The corresponding caption represents the calculated PSNR and MSE between original and encrypted images.

$(a)Test_{im_2}$

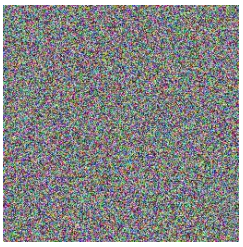


$(b)Teste_{im_2}$

$(c)Testd_{im_2}$



$(d)Testdks1_{im_2}$



$(e)Testdks2_{im_2}$

Figure 5. Resultant images for key sensitivity analysis.

High KS is one of the most essential characteristics of a secure ciphering algorithm and can provide additional complexity to the encryption scheme. For robust image encryption, the procedure should be highly susceptible to secret key variations. Consequently, a subtle modification to any individual secret key ought to yield a thoroughly scrambled and semantically meaningless output image. To demonstrate the proposed algorithm's robustness regarding secret keys, key sensitivity is analyzed for different used secret keys, and corresponding results are provided in Figure 5: (a) is the test ($Test_{im_2}$)), (b) is the ciphered ($Teste_{im_2}$), (c) is the deciphered image ($Testd_{im_2}$) by taking all the correct secret keys and parameters, (d) $Testdks1_{im_2}$ and (e) $Testdks2_{im_2}$ are deciphered images corresponding to slight modification (of order $10^{(-14)}$) in secret keys. This shows the proposed scheme's significant level of key sensitivity and ensures that corresponding minor changes in the deciphering key produce significantly different/meaningless decrypted images, thus preventing the scheme from unauthorized decryption.

4.4 Chi-square test analysis

Uniformity inside the encrypted visual data's pixel distribution is quantitatively examined through the Chi-square test, and mathematically, it is defined as:

$$\chi^2 = \sum_{k=0}^{2^n-1} \frac{(O_k - E_k)^2}{E_k} \quad (10)$$

where $E_k = mn/256$ is the expected pixel frequency for a m × n image, and O_k is the observed frequency of kth pixel intensity, respectively.

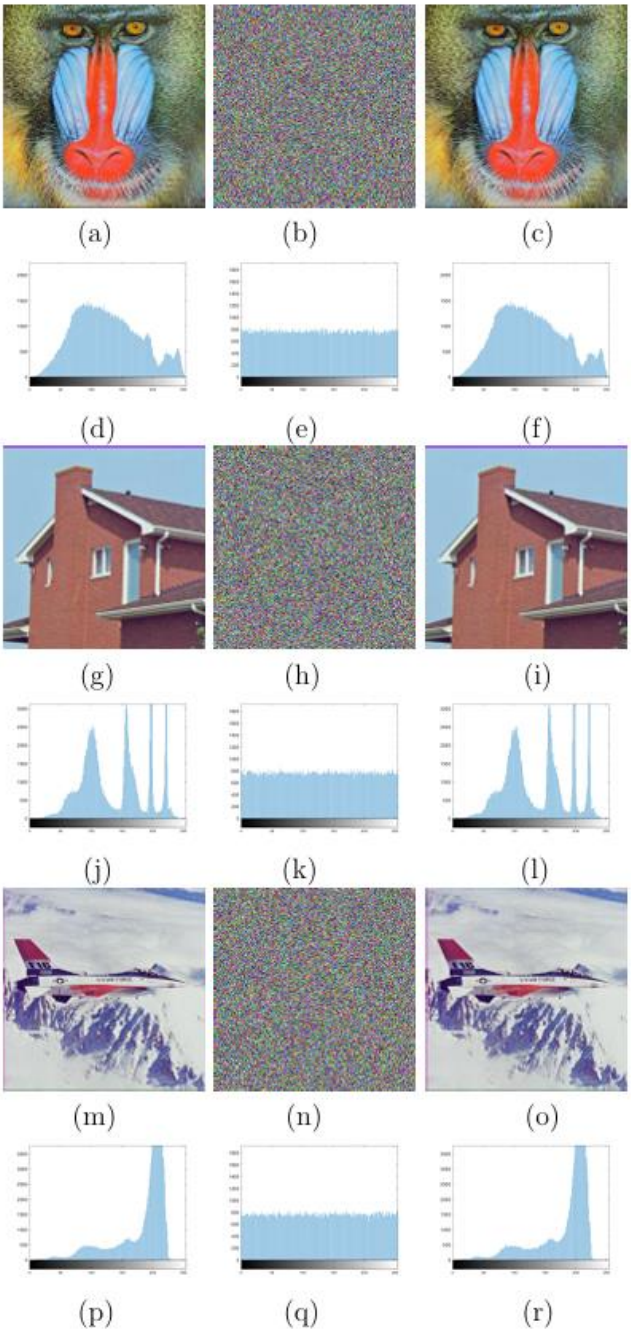


Figure 6. Histogram analysis: Images in first column are original test images and their histogram, second & third column's images represents the results for ciphered and deciphered images, respectively.

Table 3. Component wise χ^2 test's result

Ciphered Images	**χ^2 test values**				**H_0**
	R	**G**	**B**	**Average**	
Baboon	221.96875	207.67188	272.13281	233.92448	Pass
House	270.9375	261.34375	266.33594	266.20573	Pass
Aeroplane	258.26563	301.42188	301.44531	287.04427	Pass
Capsicum	234.86719	276.375	220.08594	243.77604	Pass
Splash	238.83594	271.10156	222.13281	244.02344	Pass
Nature	227.33594	288.17188	256.46094	257.32292	Pass

The Chi-square's ideal values are $\chi_{0.}05,255^2 = 293.2478$ and $\chi_{0.}01,255^2 = 310.4574$ for the significance level sig_α = 5% and sig_α = 1% with 255 degrees of freedom, respectively [49]. Table 3 represents the calculated Chi-square values for the developed technique and passes the hypothesis of uniformity at both levels of significance (viz. sig_α = 5% and sig_α = 1%). Since all the chi-square values are within the acceptable range, mathematically confirming the uniformity of picture element intensity distribution in the ciphered image's histogram and robustness against statistical attacks.

4.5 Entropy analysis

The measure the unpredictability within the image data is called entropy [50]. Since high unpredictability is necessary for the cipher images to enable a secure image encryption scheme [51]. Hence, entropy values of the well-ciphered images must be near the estimated value (i.e. 8). The entropy is denoted by $E_v$al and can be computed as follows

$$E_{val}(\mu) = \sum_{i=0}^{2^n-1} p(\mu_i) \log\left(\frac{1}{p(\mu_i)}\right) \quad (11)$$

where $p(\mu_i)$ is the occurrence probability of μ_i (ith gray value). The proposed method produces high-quality random encrypted images, as seen by the cipher image's entropy values near the critical value. Table 4 shows the $E_v$al values of plain (E_{val_o}) and corresponding ciphered (E_{val_e}) images, signifying that the proposed encryption method achieves near-perfect randomness and protects the encrypted images against information leakage.

4.6 Mean square error (MSE)

The MSE calculates the cumulative error to compare data of original and modified images [28]. It is one of the basic requirements to analyse the effectiveness and security of image ciphering scheme. MSE between the input and corresponding cipher images must be greater, whereas, between the input and corresponding decrypted images, it should be nearly zero. Table 5 shows the $MSE(Test_{im_i}, Teste_{im_i})$ values between the encrypted images ($Teste_{im_i}$) and plain images ($Test_{im_i}$). Very high evaluated MSE values confirm the significant differences and indicate the proposed scheme's robustness by emphasising the scrambling and diffusion of pixels in the ciphered images. Further, zero MSE values for all $Testd_{im_i}$ validate the argument of no data loss during the decryption of the proposed scheme.

4.7 PSNR analysis

The PSNR is a quality calculation parameter between two images [52]. A good encryption technique suggests a lower (less than 10 dB) encrypted image's PSNR value and greater as possible (nearer to infinity) deciphered image's PSNR values with reference to the plain image [46]. The formula to evaluate the $PSNR(Test_{im_i}, Teste_{im_i})$ is defined as

$$PSNR(Test_{im_i}, Teste_{im_i}) = \log_{10}\left(\frac{P_m^2}{E_\mu}\right) \quad (12)$$

The highest intensity of pixel values is denoted by P_m, and

$$E_\mu = \frac{1}{mn}\sum_{a=1}^{n}\sum_{b=1}^{m}(g'(a,b) - g(a,b)))^2$$

is the mean square error between. The plain and corresponding reconstructed images are de- noted by g and g′, respectively. The proposed algorithm's calculated $PSNR(Test_{im_i}, Teste_{im_i})$ for encrypted and decrypted images with reference to original images are provided in Table 5. Less than 10 dB $PSNR(Test_{im_i}, Teste_{im_i})$ values for all the encrypted images show the pro- posed scheme's robustness and efficiency. Further, infinite values for $PSNR(Test_{im_i}, Testd_{im_i})$, corresponding to all the deciphered images Testdimi indicate perfect reconstruction and show that the $Testd_{im_i}$ are identical to the $Test_{im_i}$.

4.8 Structure similarity index (SSIM)

To evaluate the image encryption's quality, the structure similarity between two images, the input and output ciphered images, is calculated [53]. If an encryption system functions well, the SSIM values ought to be nearly zero. The SSIM can be computed as

$$SSIM(a,b) = \frac{(2\mu_a\mu_b + c_0)(2\sigma_{ab} + c_1)}{(\mu_a^2 + \mu_b^2 + c_0)(\sigma_a^2 + \sigma_b^2 + c)} \quad (13)$$

where the covariance, mean, and standard deviation of the $Test_{im}$ and $Teste_{im}$ are $\sigma_a b$, (μ_a, μ_b), and (σ_a, σ_b), respectively. Moreover, the variables that need to be stabilized are c and c_0. Table 6 shows calculated SSIM values of encrypted ($Teste_{im_i}$) and decrypted ($Testd_{im_i}$) images with reference to original plain images for the proposed scheme viz., $SSIM(Test_{im_i}, Teste_{im_i})$ and $SIM(Test_{im_i}, Testd_{im_i})$. Approximately zero encrypted image's $SSIM(Test_{im_i}, Teste_{im_i})$ values for the proposed scheme suggest the higher dissimilarity among the plain and corresponding ciphered images. That creates difficulty for hackers in leaking the image information. Furthermore, the $SSIM(Test_{im_i}, Testd_{im_i})$ values of one for all the pairs of deciphered and plain images ensure that no image data is altered or lost during the decryption process. The quality of these images highlights their robustness and efficiency during the encryption and decryption process.

Table 4. Component-wise entropy analysis

Images		E_{val_o}			E_{val_e}	
	R	G	B	R	G	B
Baboon	7.60578	7.3581	7.66648	7.99755	7.99771	7.99701
House	6.43105	6.53893	6.23204	7.99703	7.99712	7.99705
Aeroplane	6.72543	6.82531	6.20785	7.99717	7.99667	7.99668
Capsicum	7.30091	7.55699	7.09288	7.99742	7.99696	7.99757
Splash	6.94171	6.90453	6.06012	7.99736	7.99700	7.99756
Nature	7.25873	7.61431	7.18921	7.99750	7.99683	7.99717

Table 5. *Calculated $PSNR(Test_{im_i}, Teste_{im_i})$ and $MSE(Test_{im_i}, Teste_{im_i})$ for ciphered images ($Teste_{im_i}$) in context to the plain images ($Test_{im_i}$)*

Images		PSNR			MSE	
	R	G	B	R	G	B
Baboon	8.91839	9.48895	8.54641	8.34144	7.31451	9.08739
House	9.80617	8.75593	8.37309	6.79929	8.65939	9.4574
Aeroplane	8.19844	7.85579	7.98718	9.84546	10.65373	10.33623
Capsicum	9.13327	7.68706	7.71397	7.93877	11.07577	11.00738
Splash	7.57035	7.2554	8.19428	11.37746	12.2332	9.8549
Nature	9.50428	7.58357	7.5418	7.28874	11.34287	11.45249
Decrypted images (all)	inf	inf	inf	0	0	0

Table 6. Structure similarity index (SSIM) analysis

Images	$SSIM(Test_{im_i}, Teste_{im_i})$	$SIM(Test_{im_i}, Testd_{im_i})$
Baboon	0.00855	1
House	0.01154	1
Aeroplane	0.00949	1
Capsicum	0.00827	1
Splash	0.00676	1
Nature	0.00775	1

4.9 Correlation coefficient

The correlation coefficient (C_r) between two sequences is used to determine the correlation between the relevant elements [50]. For the comprehensive analysis of security and to assess pixel relations in a digital image, three correlation coefficients (viz. horizontal (C_rh), vertical (C_rv) and diagonal (C_rd) directions) are evaluated for an image ciphering scheme. Generally, high correlation is deputed by the adjacent unencrypted image's pixel intensities. All three correlations C_rh, C_rv and C_rd should be significantly reduced in a ciphered image for a robust and secure image ciphering scheme. Mathematically, it is calculated as

$$C_r(A,B) = \frac{\sum_p \sum_q (A_{pq} - \bar{A})(B_{pq} - \bar{B})}{\sqrt{\sum_p \sum_q (A_{pq} - \bar{A})^2} \cdot \sqrt{\sum_p \sum_q (B_{pq} - \bar{B})^2}} \quad (14)$$

where A and B are two adjacent pixel sequences, $\bar{A}$ and B denote their mean values, respectively. The correlation coefficient C_r having a range $-1 \le C_r \le 1$. Whenever $C_r \rightarrow +1$ implies a strong positive link between neighbouring pixels, whereas $C_r \rightarrow -1$ indicates a significant negative link. Further, $C_r \approx 0$ indicates there is no relationship between neighbouring pixels [50]. Table 7 shows the proposed scheme's

correlation coefficient C_r of the original and corresponding ciphered images. This table ensures that the pixel values are randomized throughout ciphered images and that the pixel relationship is uniformly disturbed during the proposed encryption process and illustrating the effectiveness of the scheme in breaking pixel dependencies.

4.10 Differential attack analysis

A differential attack is a common security analysis technique for ciphering schemes. This attack slightly adjusts the original image's pixel intensities and tries to determine the difference among the corresponding encrypted image [54]. From this study, a hacker can attempt to see how the unencrypted image and its scrambled version relate to one another [55]. Two estimations can help us stop such attacks by analyzing them mathematically, viz., NPCR and UACI. The formula to compute the NPCR and UACI are as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{mn} \times 100\% \quad (15)$$

$$UACI = \frac{1}{mn}\sum_{i,j}\left|\frac{\Phi_1(i,j)-\Phi_2(i,j)}{255}\right| \times 100\% \quad (16)$$

Computed proposed scheme's UACI and NPCR values indicated in Table 8 and Table 9. During these calculations, Φ_2 is the ciphered image associated with a change in a single bit of the first pixel of red channel only (i.e. only a single bit is changed) in the $Test_{im_i}$. All the obtained values are approximately similar to corresponding theoretical values, i.e. 31.9622 for UACI and 99.6 for NPCR. This indicates the suggested approach is capable of resisting the differential attacks, ensuring that slight variations within the unencrypted images result in significant alterations in the cipher images.

Further, this proposed scheme's resistance is also verified theoretically as the initial conditions of the DCC map are derived with the help of the original image and SHA-256 hash function. This incorporates the high sensitivity towards the original image, and corresponding to any slight changes in the original image renders a wholly distinct encrypted output image due to the significant alternation of chaotic sequence obtained from the DCC map. This sensitivity ensures that even minor differences in plaintext produce vastly different ciphertexts.

For the error analysis in NPCR and UACI values, we conduct a null hypothesis with different levels of significance. In Table 8, $U^{*+}_{0.05}$, $U^{*+}_{0.01}$ and $U^{*+}_{0.001}$ represents the right value for the critical values of rejecting the null hypothesis at the α = 0.05, α = 0.01 and α = 0.001 significance level, respectively [54]. Whereas, $U^{*-}_{0.05}$, $U^{*-}_{0.01}$ and $U^{*-}_{0.001}$ represents the left value for the corresponding critical values. It is apparent from this table that all the calculated UACI values lie in the range (viz., U^{*-}_{α} to U^{*+}_{α}) of the critical values at all three level of significance, validate the argument of random-like. Further, in Table 9, $N^{*}_{0,05}, N^{*}_{0,01}$ and $N^{*}_{0,001}$ represents the critical values of rejecting the null hypothesis at the α = 0.05, α = 0.01 and α = 0.001 significance level respectively. It is apparent from this table that, it is clear that all the calculated NPCR values are greater than the critical values at all three levels of significance; hence, corresponding all the pairs of ciphertext images are randomlike.

4.11 Noise attack analysis

Noise signals may impact the digital data during the transmission over the open network channels. To test the resistance against noise attacks to the ciphered images, noise with varying intensity is added, and corresponding obtained deciphered images are analyzed [55]. Here, in the proposed algorithm to test noise attack analysis, the *Salt & Pepper* noise is added to the ciphered images. The noise affected decrypted images ($Testd_{im_2}$) using the proposed technique are shown in Figure 7. The fact that all of the noise-affected images in this figure are clearly visible shows that the suggested method of encryption works well and is robust to noise attacks, preserving image visibility even under various levels of noise interference.

Table 7. Correlation coefficient (C_r) analysis for the proposed scheme

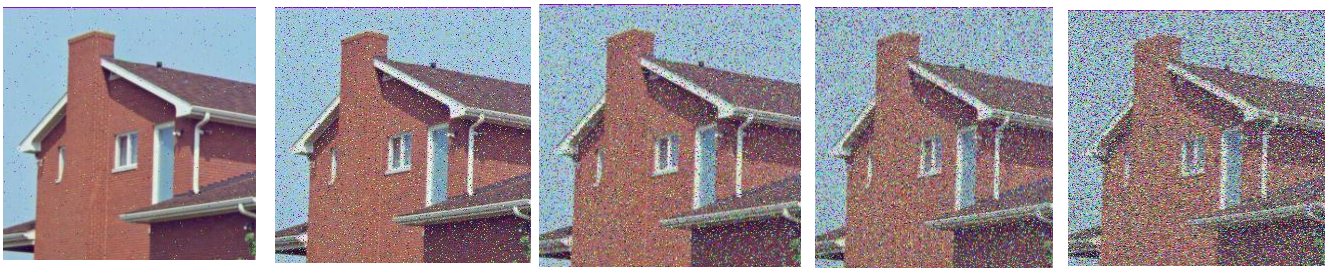
Images	Test			Encrypted		
	Horz (C_{rh})	Verti (C_{rv})	Diag (C_{rd})	Horz (C_{rh})	Verti (C_{rv})	Diag (C_{rd})
Baboon	0.92207	0.90238	0.86986	-0.00161	-0.00098	0.00154
House	0.97980	0.95971	0.94142	-0.0017	-0.00206	0.00465
Aeroplane	0.93833	0.92752	0.87657	0.00062	0.0037	-0.00495
Capsicum	0.97532	0.97905	0.95299	0.00361	0.0005	0.0023
Splash	0.98631	0.9896	0.97755	-0.00084	0.00181	0.00076
Nature	0.95822	0.95832	0.92797	-0.00055	-0.00086	0.00083

Table 8. Component wise UACI test analysis

Images	Calculated UACI values				Theoretical UACI critical values		
	R	G	B	Average	0.05-level $U^{*+}_{0.05}$=33.2824% $U^{*-}_{0.05}$=33.6447%	0.01-level $U^{*+}_{0.01}$=33.2255% $U^{*-}_{0.01}$=33.7016%	0.001-level $U^{*+}_{0.001}$=33.1594% $U^{*-}_{0.001}$=33.7677%
Baboon	33.44808	33.52864	33.53994	33.50555			
House	33.67408	33.3742	33.38736	33.47855			
Aeroplane	33.42632	33.42999	33.45644	33.43758	pass	pass	pass
Capsicum	33.40644	33.5453	33.48169	33.47781			
Splash	33.2736	33.4469	33.53005	33.41685			
Nature	33.5945	33.49378	33.54049	33.54292			

Table 9. Component wise NPCR test analysis

Images	Calculated NPCR values				Theoretical NPCR critical values		
	R	G	B	Average	0.05-level $N^{*}_{0,05}$=99.5693%	0.05-level $N^{*}_{0,01}$=99.5527%	0.05-level $N^{*}_{0,001}$=99.5341%
Baboon	99.60022	99.60327	99.59869	99.60073			
House	99.59869	99.60785	99.59564	99.60073			
Aeroplane	99.61548	99.55139	99.67651	99.61446	pass	pass	pass
Capsicum	99.6048	99.6109	99.61548	99.61039			
Splash	99.64142	99.61243	99.58344	99.61243			
Nature	99.65973	99.62463	99.60327	99.62921			



(a) 0.1% (b) 1% (c) 10% (d) 20% (e) 40%

Figure 7. Noise attack analysis: deciphered images corresponding to given intensity of Salt & Pepper noise.

4.12 Occlusion attack

In addition to data congestion and deliberate data destruction, occlusion attacks threaten or lose image data during transmission [56]. Occlusion attacks can examine the recovery rate of the destroyed encrypted image. To determine the proposed scheme's resiliency against this attack, the ciphered image of the house is cropped of various sizes and from different locations. It is presented in the first row of Figure 8. The high quality retained by the extracted images (please refer to images in the second row of Figure 8), shows the efficiency and ability of the proposed technique towards reconstructing image data even in case of incomplete or tempered data and highlighting the robustness of the encryption process in protecting data integrity.

4.13 Encryption time and computational complexity analysis

Good computation speed is the essential requirement for the real-life implementation of an encryption scheme, and for this, it should be as minimal as possible. The proposed algorithm's encryption and decryption process is performed over different test images to analyze the corresponding speed rate on *MATLAB2021b* and using an HP laptop with

specifications *12th Gen, 16GB RAM, 1.30 GHz, i5-1235U and 512GB SSD*. The Execution from the perspective of ciphering time and decryption time for the proposed algorithm is provided in Table 10.

Further, the system's complexity is vital in maintaining efficiency and speed. In the present technique, it is divided into the following levels: substitution S-box, confusion-diffusion using a discrete compound chaotic (DCC) map, and iterative scrambling using Baker's map. For an image of size n by n, the computational complexity for the implementation of the S-box is O(n^2) since each pixel is substituted once. For the confusion-diffusion using the DCC map, the chaotic sequence is generated with n^2 elements, and each pixel is permuted and passed through the bitXOR operation, and the combined complexity is O(2*n^2). During the partition and rearrangement, Baker's map operated on the coordinates of each pixel value. Further, Baker's map is iterated $n_b k$ times, and the complexity for the overall scrambling is O($n_b k * n^2$). Hence, proposed scheme's total complexity is O($n^2 + 2n^2 + n_{bk} \times n^2$), which is approximated to O(n^2).

4.14 Comparison of developed technique with some existing methods

This section discusses the detailed comparison of the developed scheme compared with a num- ber of established approaches. The calculated encryption time and statistical analysis results, including entropy, MSE, PSNR, SSIM, NPCR and UACI, are compared as presented in Table 11 and Table 12 respectively. The simulation results favour the proposed scheme's efficiency and robustness when compared with some existing schemes.

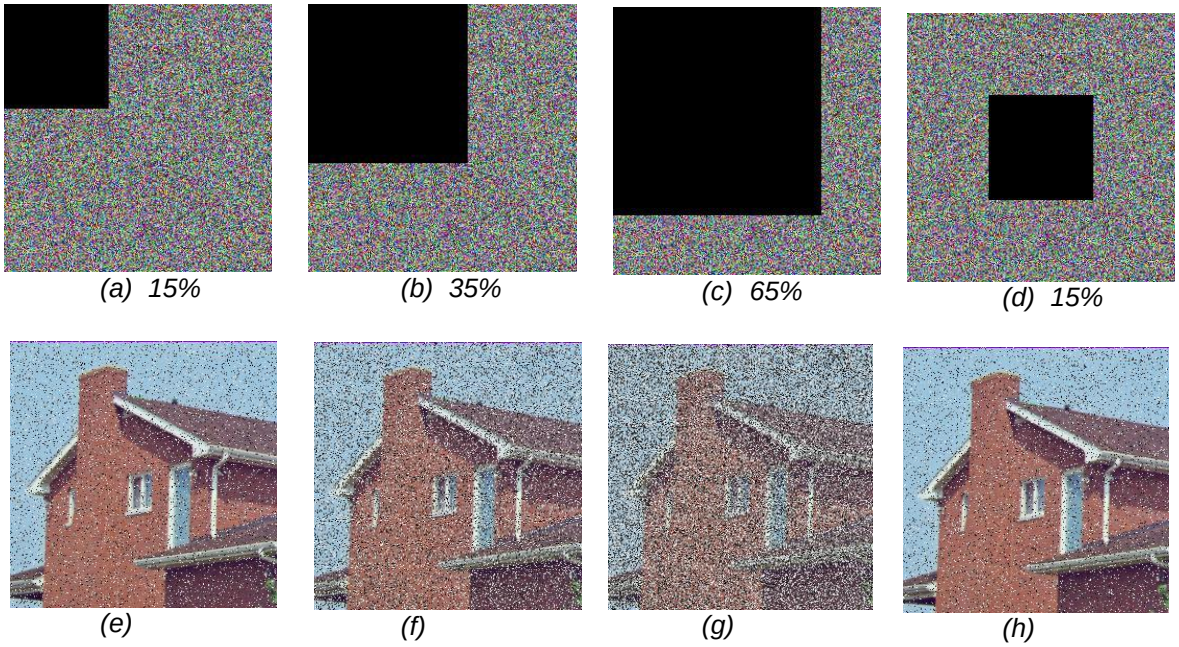


Figure 8. Occlusion attack analysis: images in first row are different sized occluded images, and second row represents the corresponding deciphered images.

Table 10. Execution time of the proposed scheme

Images	Encryption time (in seconds)	Decryption time (in seconds)
Baboon	0.2800111	0.8281262
House	0.2481881	0.7795507
Aeroplane	0.2583081	0.8595164
Capsicum	0.2596622	0.8448122
Splash	0.2602812	0.8748994
Nature	0.2531385	0.804225

Table 11. Execution time's comparison

References	Image size	Encryption time (s)
Ref.[57]	256×256	2.6371
Ref. [58]	256×256	2.5824
Ref. [59]	256×256	3.0019
Ref. [60]	256×256	25.3344
Ref. [61]	256×256	0.4598
Proposed	256×256	0.2599

Table 12. Proposed technique's comparative analysis

Metrics	DC	VC	HC	SSIM	Entropy	NPCR	UACI
Ref. [59]	-0.00151	0.00795	0.00144	-	7.9968	99.6246	30.5681
Ref. [60]	0.0001	0.0001	-0.002	0.0106	7.958	99.5865	28.6372
Ref. [61]	0.000627	0.000279	-0.00162	-	7.9914	99.6060	33.4689
Ref. [58]	-0.00132	-0.0016	0.002287	-	7.997	99.6287	30.3432
Ref. [62]	0.0049	0.0045	0.0054	-	7.9958	99.6205	33.4526
Ref. [57]	0.000013	0.000024	0.00175	-	7.9987	99.6254	30.5681
Proposed	0.002502	0.00165	0.001488	0.0087	7.9971	99.6113	33.4765

5. Conclusion

This study introduces a new image encryption method that integrates the use of an S-box, Baker's map, and discrete compound chaotic (DCC) map. Our approach addresses the critical requirement of an effective and strong encryption technique to protect the confidential image data. With the chaotic and unpredictable nature, the DCC map provides high security by offering a strong foundation for generating encryption key sequences utilized for diffusion and confusion. The S-box enhances the encryption process's diffusion strength, whereas the multiple iterations of the Baker's map contributes towards the effective scrambling of image pixels. The results of the experiments on a range of benchmark images demonstrate how well proposed is the encryption approach against various common cryptographic attacks. The proposed method achieves high security and compatibility by facilitating seamless integration into practical systems. The proposed scheme's robustness, efficiency and reliability are highlighted through the quality of ciphered and deciphered image, and makes a perfect choice for application in the area of data integrity with high level of security.

5.1 Directions for further study

In the present digital era, with digital communication advancement, simultaneously, multiple images or video content is conveyed via unsecured channels. Security seems crucial in these situations, and for future endeavours, we wish to extend the proposed technique to enhance the security of videos and multiple images.

References

[1] M. Kumar, S. Agrawal, Color image encoding in DOST domain using DWT and SVD. Optics and Laser Technology, 75, (2015) 138–145. https://doi.org/10.1016/j.optlastec.2015.06.022

[2] C. Fu, Z.-K. Wen, Z.-L. Zhu, H. Yu, A security improved image encryption scheme based on chaotic baker map and hyperchaotic Lorenz system. International Journal of Computational Science and Engineering, 12(2–3), (2016) 113–123. https://doi.org/10.1504/IJCSE.2016.076212

[3] M.B. Farah, A. Farah, T. Farah, An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4), (2020) 3041–3064. https://doi.org/10.1007/s11071-019-05413-8

[4] A.A.A. El-Latif, B. Abd-El-Atty, A. Belazi, A.M. Iliyasu, Efficient chaos-based substitution-box and its application to image encryption. Electronics, 10(12), (2021) 1392. https://doi.org/10.3390/electronics10121392

[5] H. Shi, M. Ji'e, C. Li, D. Yan, S. Duan, L. Wang, A novel image encryption algorithm based on 2D self-coupling sine map. International Journal of

Bifurcation and Chaos, 32(15), (2022) 2250233. https://doi.org/10.1142/S0218127422502339

[6] D. Singh, S. Kumar, A multiphase encryption scheme using RSS, modified RMAC and Chen's hyperchaotic map. Multimedia Tools and Applications, 83(19), (2024) 57059–5708.

[7] Q. He, P. Li, Y. Wang, A color image encryption algorithm based on compressive sensing and block-based DNA coding. IEEE Access, IEEE, 12 (2024) 77621-77638. https://doi.org/10.1109/ACCESS.2024.3406766

[8] Y.M. Afify, N.H. Sharkawy, W. Gad, N. Badr, A new dynamic DNA-coding model for gray-scale image encryption. Complex & Intelligent Systems, 10(1), (2024) 745–761. https://doi.org/10.1007/s40747-023-01187-0

[9] X. Yan, Q. Hu, L. Teng, A novel color image encryption method based on new three-dimensional chaotic mapping and DNA coding. Nonlinear Dynamics, 113 (2024) 1799-1826. https://doi.org/10.1007/s11071-024-10277-8

[10] S. Kumar, D. Sharma, A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artificial Intelligece Review, 57(4), (2024) 87. https://doi.org/10.1007/s10462-024-10719-0

[11] M.M. Deep, M.N.D. Praveen, P.S. Deekshith, P.V. Teja, S.K. Kannaiah, K. Prasad, (2024) A survey on image encryption using elliptic curve cryptography. Proceedings of the International Conference on Inventive Computation Technologies (ICICT), IEEE, Lalitpur, Nepal, 1460–1464. https://doi.org/10.1109/ICICT60155.2024.10544776

[12] X. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. Signal Processing, 89(4), (2009) 480–491. https://doi.org/10.1016/j.sigpro.2008.09.011

[13] M. Usama, O. Rehman, I. Memon, S. Rizvi, An efficient construction of key-dependent substitution box based on chaotic sine map. International Journal of Distributed Sensor Networks, 15(12), (2019) 1550147719895957. https://doi.org/10.1177/1550147719895957

[14] L.S. Khan, M.M. Hazzazi, M. Khan, S.S. Jamal, A novel image encryption based on Rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. Chinese Journal of Physics, 72, (2021) 558–574. https://doi.org/10.1016/j.cjph.2021.03.029

[15] D. Lambić, A novel method of S-box design based on discrete chaotic map. Nonlinear Dynamics, 87, (2017) 2407–2413. https://doi.org/10.1007/s11071-016-3199-x

[16] C.E. Shannon, Communication theory of secrecy systems. The Bell System Technical Journal, Nokia Bell Labs, 28(4), (1949) 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[17] A. Vaish, An error free and key sensitive color image encryption-using sine powered map and Arnold transform in Stockwell domain. Multimedia Tools and Applications, 83 (2023) 1–19. https://doi.org/10.1007/s11042-023-16277-x

[18] S. Kumar, S. Srivastava, Image encryption using simplified data encryption standard (S-DES). International Journal of Computer Applications, 104(2), (2014) 38-42. https://doi.org/10.5120/18178-9070

[19] A. Kumar, M. Dua, A novel exponent–sine–cosine chaos map-based multiple-image encryption technique. Multimedia Systems, 30(3), (2024) 141. https://doi.org/10.1007/s00530-024-01334-8

[20] Y. Luo, J. Yu, W. Lai, L. Liu, A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications, 78, (2019) 22023–22043. https://doi.org/10.1007/s11042-019-7453-3

[21] M. Salleh, S. Ibrahim, I.F. Isnin, (2003) Enhanced chaotic image encryption algorithm based on baker's map. Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03, IEEE, Bangkok, Thailand. https://doi.org/10.1109/ISCAS.2003.1206022

[22] T. Xiang, X. Liao, G. Tang, Y. Chen, K.-W. Wong, A novel block cryptosystem based on iterating a chaotic map. Physics Letters A, 349(1–4), (2006) 109–115. https://doi.org/10.1016/j.physleta.2005.02.083

[23] M. François, T. Grosges, D. Barchiesi, R. Erra, A new image encryption scheme based on a chaotic function. Signal Processing: Image Communication, 27(3), (2012) 249–259. https://doi.org/10.1016/j.image.2011.11.003

[24] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos. Signal Processing, 92(4), (2012) 1101–1108. https://doi.org/10.1016/j.sigpro.2011.10.023

[25] M. Kumar, A. Vaish, Encryption of color images using mSVD in DCST domain. Optics and Lasers in Engineering, 88, (2017) 51–59. https://doi.org/10.1016/j.optlaseng.2016.07.009

[26] F. Masood, J. Masood, L. Zhang, S.S. Jamal, W. Boulila, S.U. Rehman, F.A. Khan, J. Ahmad, A new color image encryption technique using DNA computing and Chaos-based substitution box. Soft Computing, 26(16), (2022) 7461-7477.

[27] D. Chatterjee, B.G. Banik, A. Banik, Attack resistant chaos-based cryptosystem by modified baker map and logistic map. International Journal of Information and Computer Security, 20(1–2), (2023) 48–83.

[28] .Z. Hussain, M.A.A.A. Khodher, Medical image encryption using multi chaotic maps. TELKOMNIKA (Telecommunication Computing Electronics and Control), 21(3), (2023) 556–565. http://doi.org/10.12928/telkomnika.v21i3.24324

[29] S. Sudevan, K. Jain, (2023) A lightweight medical image encryption scheme using chaotic maps and image scrambling. Proceedings of the International Symposium on Digital Forensics and Security (ISDFS), IEEE, Chattanooga, USA

[30] E.A. Naeem, A.B. Joshi, D. Kumar, F.E.A. El-Samie, Few-detail image encryption algorithm based on diffusion and confusion using Henon and Baker chaotic maps. Soft Computing, 28(4), (2024) 2851–2861. https://doi.org/10.1007/s00500-023-09333-z

[31] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, J. Liu, A novel block encryption algorithm based on chaotic S-box for wireless sensor network. IEEE Access, IEEE, 7, (2019) 53079–53090. https://doi.org/10.1109/ACCESS.2019.2911395

[32] L. Liu, Y. Zhang, X. Wang, A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Applied Sciences, 8(12), (2018) 2650. https://doi.org/10.3390/app8122650

[33] A. Ullah, S.S. Jamal, T. Shah, A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. Nonlinear Dynamics, 88, (2017) 2757–2769. https://doi.org/10.1007/s11071-017-3409-1

[34] V. Patidar, N. Pareek, K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 14(7), (2009) 3056–3075. https://doi.org/10.1016/j.cnsns.2008.11.005

[35] S. Yang, X. Tong, Z. Wang, M. Zhang, Efficient color image encryption algorithm based on 2D coupled chaos and multi-objective optimized S-box. Physica Scripta, 97(4), (2022) 045204. https://doi.org/10.1088/1402-4896/ac59fa

[36] R. Ali, J. Ali, P. Ping, M.K. Jamil, A novel S-box generator using Frobenius automorphism and its applications in image encryption. Nonlinear Dynamics, 112(21), (2024) 19463–19486. https://doi.org/10.1007/s11071-024-10003-4

[37] D. Ustun, S. Sahinkaya, N. Atli, Developing a secure image encryption technique using a novel S-box constructed through real-coded genetic algorithm's crossover and mutation operators. Expert Systems with Applications, 256, (2024) 124904. https://doi.org/10.1016/j.eswa.2024.124904

[38] R.S. Ali, O.Z. Akif, S.A. Jassim, A.K. Farhan, E.-S.M. El-Kenawy, A. Ibrahim, M.E. Ghoneim, A.A. Abdelhamid, Enhancement of the CAST block algorithm based on novel S-box for image encryption. Sensors, 22(21), (2022) 8527. https://doi.org/10.3390/s22218527

[39] J. Zheng, Q. Zeng, An image encryption algorithm using a dynamic S-box and chaotic maps. Applied Intelligence, 52(13), (2022) 15703–15717. https://doi.org/10.1007/s10489-022-03174-3

[40] L. Wang, Q. Ran, J. Ding, Quantum color image encryption scheme based on 3D non-equilateral Arnold transform and 3D logistic chaotic map. International Journal of Theoretical Physics, 62(2), (2023) 36. https://doi.org/10.1007/s10773-023-05295-y

[41] D. Singh, S. Kumar, Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps. Expert Systems with Applications, 274, (2025) 126883. https://doi.org/10.1016/j.eswa.2025.126883

[42] L. Li, A novel chaotic map application in image encryption algorithm. Expert Systems with Applications, 252, (2024) 124316. https://doi.org/10.1016/j.eswa.2024.124316

[43] D. Singh, S. Kumar, C. Verma, Z. Illes, N. Kumar, Visually meaningful image encryption for secure and authenticated data transmission using chaotic maps. Journal of King Saud University – Computer and Information Sciences, 36(10), (2024) 102235. https://doi.org/10.1016/j.jksuci.2024.102235

[44] L.L. Hu, M.X. Chen, M.M. Wang, N.R. Zhou, A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion. Chaos, Solitons & Fractals, 188, (2024) 115521. https://doi.org/10.1016/j.chaos.2024.115521

[45] Q. Lu, C. Zhu, X. Deng, An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, IEEE, 8, (2020) 25664–25678. https://doi.org/10.1109/ACCESS.2020.2970806

[46] U.H. Mir, P.N. Lone, D. Singh, D. Mishra, A public and private key image encryption by modified approach of Vigenère cipher and the chaotic maps. The Imaging Science Journal, 71(1), (2023) 82–96. https://doi.org/10.1080/13682199.2023.2175436

[47] A. Mahboob, M. Asif, I. Siddique, A. Saleem, M. Nadeem, D. Grzelczyk, J. Awrejcewicz, A novel construction of substitution box based on polynomial mapped and finite field with image encryption application. IEEE Access, 10, (2022) 119244–119258. https://doi.org/10.1109/ACCESS.2022.3218643

[48] P. Ayubi, S. Setayeshi, A.M. Rahmani, Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application. Journal of Information

Security and Applications, 52, (2020) 102472. https://doi.org/10.1016/j.jisa.2020.102472

[49] D. Ravichandran, P. Praveenkumar, J.B.B. Rayappan, R. Amirtharajan, DNA chaos blend to secure medical privacy. IEEE Transactions on Nanobioscience, IEEE, 16(8), (2017) 850–858. https://doi.org/10.1109/TNB.2017.2780881

[50] U.H. Mir, D. Singh, D. Mishra, P.N. Lone, Multilayer security of RGB image in discrete Hartley domain. Applications and Applied Mathematics: An International Journal, 15(2), (2020) 29.

[51] M. Diwakar, M. Kumar, CT image denoising using NLM and correlation-based wavelet packet thresholding. IET Image Processing, 12(5), (2018) 708–715. https://doi.org/10.1049/iet-ipr.2017.0639

[52] S. Agrawal, M. Kumar, Mean value based reversible data hiding in encrypted images. Optik, 130 (2017) 922–934. https://doi.org/10.1016/j.ijleo.2016.11.059

[53] X.Y. Wang, P. Li, Y.Q. Zhang, L.Y. Liu, H. Zhang, X. Wang, A novel color image encryption scheme using DNA permutation based on the Lorenz system. Multimedia Tools and Applications, 77, (2018) 6243–6265. https://doi.org/10.1007/s11042-017-4534-z

[54] Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology – Journal of Selected Areas in Telecommunications, (2011) 31–38.

[55] P.N. Lone, D. Singh, U.H. Mir, Image encryption using DNA coding and three-dimensional chaotic systems. Multimedia Tools and Applications, 81(4), (2022) 5669–5693. https://doi.org/10.1007/s11042-021-11802-2

[56] P.N. Lone, D. Singh, U.H. Mir, A novel image encryption using random matrix affine cipher and the chaotic maps. Journal of Modern Optics, 68(10), (2021) 507–521. https://doi.org/10.1080/09500340.2021.1924885

[57] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, A. Aboshousha, Color image encryption through chaos and KAA map. IEEE Access, 11, (2023) 11541–11554. https://doi.org/10.1109/ACCESS.2023.3242311

[58] W. Alexan, M. ElBeltagy, A. Aboshousha, RGB image encryption through cellular automata, S-box and the Lorenz system. Symmetry, 14(3), (2022) 443. https://doi.org/10.3390/sym14030443

[59] M.T. Elkandoz, W. Alexan, Image encryption based on a combination of multiple chaotic maps. Multimedia Tools and Applications, 81(18), (2022) 25497–25518. https://doi.org/10.1007/s11042-022-12595-8

[60] S. Sheela, K. Suresh, D. Tandur, Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimedia Tools and Applications, 77, (2018) 25223–25251. https://doi.org/10.1007/s11042-018-5782-2

[61] L. Teng, X. Wang, Y. Xian, Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Information Sciences, 605, (2022) 71–85. https://doi.org/10.1016/j.ins.2022.05.032

[62] G. Ye, K. Jiao, X. Huang, Quantum logistic image encryption algorithm based on SHA-3 and RSA. Nonlinear Dynamics, 104, (2021) 2807–2827. https://doi.org/10.1007/s11071-021-06422-2

Acknowledgement

The first author is thankful to DST, India for support through grant no.: SR/FST/MS- 1/2021/104(C) under DST-FIST project.

Authors Contribution Statement

Deep Singh: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Data Curation, Writing - Review & Editing, Visualization, Supervision, Project administration. Lalthazuala: Conceptualization, Methodology, Software, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Visualization. Sandeep Kumar: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data Curation, Writing - Original Draft, Visualization. Jatinder Kumar: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing - Review & Editing, Visualization, Funding acquisition. Amit Paul: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing - Review & Editing, Visualization, Supervision, Funding acquisition. All the authors read and approved the final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes