IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 July 2022, accepted 15 August 2022, date of publication 18 August 2022, date of current version 26 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3199738

RESEARCH ARTICLE

Encrypting Multiple Images With an Enhanced Chaotic Map

LAIPHRAKPAM DOLENDRO SINGH[1], (Member, IEEE), ROHIT THINGBAIJAM[1], KHOIROM MOTILAL SINGH[2], AND MOATSUM AL AWIDA[3]

[1]Department of Computer Science and Engineering, National Institute of Technology Silchar, Silchar, Assam 788010, India
[2]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522302, India
[3]Department of Computer Sciences and Information Technology, Abu Dhabi University, Abu Dhabi 59911, United Arab Emirates

Corresponding author: Laiphrakpam Dolendro Singh (ldsingh.cse@gmail.com)

This research is funded by the Office of Research & Sponsored Programs of Abu Dhabi University, United Arab Emirates and this work has been partially supported by Abu Dhabi University under Grant No 19300635.

ABSTRACT A multiple-image encryption scheme based on an enhanced chaotic map is proposed. This scheme combines multiple grayscale images into three planes. An amplified sine map is used to generate a dynamic permutation table and a chaotic sequence. The initial parameters of the amplified sine map are obtained from an elliptic curve coordinate, computing using elliptic curve point multiplication between the input image hash value and the seed value of an elliptic curve. The dynamic permutation table performs cyclic shift transformation on the input image, diffusing it horizontally and vertically. The diffused image is converted to a cipher image through an XOR operation with the chaotic sequence generated by the amplified sine map. Using an amplified sine map provides larger key space, more extensive chaotic range, more extensive control parameters, better sensitive initial values and enhanced security against cryptanalysis. The experiment results indicate that the proposed scheme is fast, secure, efficient and can resist certain cryptographic attacks. Compared to other recent schemes, the proposed scheme is shown to be secure and efficient.

INDEX TERMS Multiple image encryption, cyclic shift transformation, amplified sine map, elliptic curve cryptography.

I. INTRODUCTION

With the rapid advancement of multimedia technology, developers and researchers have made it extremely simple to transfer multiple data sets simultaneously. As a result, there is a greater need for high-security and faster data communication methods. Image, video, and other multimedia data have high data redundancy and capacity, as well as a high correlation between adjacent pixels. Traditional encryption schemes like Data Encryption Standard (DES), Advanced Encryption Standard (AES), and others are not always efficient enough to encrypt these data. Researchers developed various encryption techniques by using concepts on DNA encoding [1], wavelet transform [2], [3], compressed sensing [4], ElGamal cryptosystem [5], visual secret sharing [6], etc. On the other hand, because of the ergodicity, unpredictability, non-convergence, and high sensitivity to the initial conditions, encryption schemes that are based on chaos-based [7] have piqued the attention of a large number of developers and researchers.

In chaos-based cryptography, two main issues arise (i) one-dimensional (1D) chaotic maps which do not satisfy the unpredictability property, and (ii) high-dimensional (HD) chaotic maps, despite exhibiting complex and chaotic behavior, it requires more computational complexity [8], [9]. This led to the state-of-the-art 1D chaotic map with a simple structure, more extensive chaotic range, better sensitive initial values with low computational complexity.

Mansouri *et al.* [10] proposed a new sine powered chaotic system. The chaotic map is then used in a new encryption scheme based on row-by-row and column-by-column confusion and diffusion operations. The chaotic system exhibits high randomness and sensitivity, solving the correlation of adjacent pixels. Later, they also proposed a new amplified

The associate editor coordinating the review of this manuscript and approving it for publication was Sathish Kumar.

1-D chaotic map generator [11], which amplifies the existing 1-D maps. The amplified chaotic map is then used for the generation of initial parameters for the index representation operation. Finally, a bit-level operation is carried out to generate the cipher image.

During the process of encryption using Latin squares [12], the three channels of colour images are encrypted one by one, which results in many redundant operations and low efficiency. Hua *et al.* [13] developed a colour image encryption scheme using orthogonal Latin squares and a 2D chaotic system that overcomes the weakness of the Latin squares. Further, Hua *et al.* [14], [15] and proposed a 2D parametric polynomial chaotic system and n-dimensional polynomial chaotic system that possess robust chaos, late chaos degradation and desired dynamic properties with customized parameters for desired Lyapunov exponents for better dynamic properties.

Zhang *et al.* [16] use DNA encoding and a chaotic system to develop a multiple-image encryption technique. Multiple k images are combined and a combined big image is generated and $SHA256$ is used on the big image to determine the initial parameter of the chaotic map. The big image is further decomposed into k encrypted images after pixel shuffling with the Piece-wise Linear Chaotic Maps (PWLCM) and DNA decoding. Concerning the encryption process's speed, Enayatifar *et al.* [17] developed a multiple-image encryption method based on Index-based permutation-diffusion and DNA sequences. A single big image is created using multiple images, and then converted into a one-dimension array. DNA sequence and cellular automata are employed to make permutation more secure in a quick and effective combined index based permutation and diffusion system.

Zarebnia *et al.* [18] created a hybrid chaotic systems-based multiple image encryption. In their method, the smaller blocks of plain-images are shuffled using the chaotic system, and permutation is performed. Using the Arnold cat map and cyclic shift operation, the cipher image is obtained using XoR operation. Another PWLCM based multiple-image encryption scheme was proposed by Patro *et al.* [19]. In their method, multiple grayscale images were combined to create a bigger 2D-image. Row-wise and column-wise permutation is performed to scramble the big image and produce the cipher image through the cross-coupled PWLCM technique. By combining the theory of chaotic system and elliptic curve cryptography (ECC), Singh *et al.* [20] use hyper-chaotic system with 3D scrambling to develop multiple image encryption. They combine n-images to produce a 3D image and the hyper-chaotic system's initial parameters are generated using $SHA512$. The permutation and substitution operations in carried out using the hyper-chaotic system. Finally, the cipher 3D image is formed by conducting a bit-wise XoR operation between the scrambled 3D image and the chaotic 3D image.

Many methods have been proposed to improve 1D chaotic maps' security levels so they can be used in cryptography applications. The fundamental problem that 1D classical chaotic maps suffer when realized on a digital computer is dynamical degradation. The enhanced methods can be divided into nine categories, cascading multiple chaotic maps [21], perturbing the chaotic states [22], switching between multiple chaotic maps [23], error compensation [24], combining chaotic maps using modular operation [25], coupling chaotic maps [26], introducing delays [27], bit reversal chaotic map [28], and finite state machine [29].

These enhanced methods make use of additional external sources, including multiple chaotic maps, another chaotic map, and pseudo-random numbers, which makes the chaotic map's structure complex and boosts computational complexity. Our chaotic map can create chaotic points seamlessly without the need for additional mathematical operations. Additionally, our chaotic map can produce high-quality behaviour like security and randomness without the support of an additional external source like a classical chaotic map.

The chaotic image encryption structure's augmented chaotic maps were applied in various recent proposed image encryption algorithms. In a 1D chaotic map, which is used as a source of entropy, chaotic points are leveraged to encrypt image pixels using the diffusion and confusion fundamental processes. Because initial conditions and control parameters are so sensitive to even tiny changes, the majority of proposed algorithms employ them as secure keys. A chaotic image encryption-based chaotic Jaya optimization technique was developed by the authors of [30] to produce S-boxes. The proposed algorithm employed two encryption operations to accomplish Shannon's confusion/diffusion characteristics.

A new, improved 1D sinusoidal chaotic system (I1DS), which is the core part of the proposed image encryption, was introduced in [31]. The authors presented new image encryption based on dynamic bit-shifting recombination operation and a non-linear diffusion technique. A novel signcryption system for medical images was proposed by the authors of [32] based on a new chaotic map and a combination strategy of hybrid cryptography techniques. The medical images were encrypted using elliptic curve cryptography. The authors improved the 1D classical chaotic map (Tent map) using a finite state machine, and they then utilized the enhanced chaotic map to create a novel image encryption algorithm. The proposed chaotic map's security is a prerequisite for the proposed algorithm [33].

The proposed method can encrypt twelve secret images with more than the those given in [16], [18], [19], [20], [34], and [36] except for [17], [35], and [37] with any i numbers of images. Theoretically, in [17], [35], and [37], i numbers of images can be given as input. However, a bottleneck can occur with respect to resource constraints in the computing device during actual implementation. Unlike other proposed methods where multiple chaotic systems are used as in [16], [18], [19], and [35] to provide the discrete dynamics of chaos, or that of hyper-chaotic system [20], [37], the proposed method only uses Amplified Sine Map (ASM) to fulfill the discrete dynamics of chaos. With the use of ECC [38], [39] for key exchange, the proposed method is secure, efficient and robust against various statistical attacks.

The overall contribution of the proposed encryption scheme can be summarized as follows:

1) A multiple grayscale image encryption based on enhanced chaotic map is proposed.
2) To avoid known plain-text attacks and chosen plain-text attacks, *SHA*384 is adopted to generate the initial conditions of the amplified chaotic system.
3) An amplified Sine map is used, which exhibits complex chaotic behaviour with low computational complexity.
4) A cyclic shift transformation (CST) is introduced where random byte shifts along the horizontal and vertical axes are carried out.
5) The iteration involved in the computation of random sequence used for encryption is reduced by a factor of four using base conversion operation.

The rest of the paper is structured as follows. Section II describes the preliminaries. Section III describes the proposed multiple image encryption method. Section IV displays the simulation. Section V presents the security analysis of the algorithm, followed by the Conclusion in Section VI.

II. PRELIMINARIES

A. CHAOTIC MAP

Initial values and control parameters are extremely important in chaotic maps. Any small variation in the initial conditions results in a significant difference. One-dimensional (1D) and high-dimensional chaotic maps are the two types of chaotic maps. One-dimensional maps usually feature only one or a few variables, as well as a limited output range.

1) SINE MAP

The 1D Sine Map (SM) is define as:

$$x_{n+1} = \gamma sin(\pi x_n) \tag{1}$$

where $\gamma \in [0, 1]$ is the control parameter and when $\gamma \in [0.87, 1]$, it manifests chaotic behavior.

2) AMPLIFIED SINE MAP

Unlike the traditional Sine Map, the Amplified Sine Map (ASM) [11] possesses a simple structure, larger chaotic range, bigger control parameters and better sensitive initial values. The Amplified Sine Map is defined as:

$$x_{n+1} = |cos(\gamma \delta \pi sin(\pi x_n))| / Log(3 - \gamma sin(\pi x_n)) \tag{2}$$

where $\gamma > 0$, $\delta \in [0, 1]$ and $x_n \in [0, 1]$ is the chaotic system parameter.

The bifurcation diagram of SM and ASM is shown in Fig. 1. The bifurcation diagram is used to visually analyse the chaotic behaviour of a dynamic system. Fig. 1 shows that the ASM exhibit chaotic behaviour over the whole control parameter range, with a wider output range than the SM. The Lyaponov Exponent in Fig. 2 also shows that the ASM exhibit good chaotic behaviour. NIST randomness test is performed and tabulated in Table 1 to test the randomness of the pseudo-random sequence (PRS) generated from ASM.

B. CYCLIC SHIFT TRANSFORMATION (CST)

Cyclic shift transformation (CST) is a method for scrambling image pixels in order to reduce pixel correlation. A dynamic permutation table is generated using a multi chaotic map which helps in performing random byte circular shifts along horizontal and vertical axes. The step size of the shift is based on the index of the permutation table. The structure of CST in the proposed method are as follows:

Step 1: An *ASM* sequence is generated using Equation 2. The sequence is sorted in ascending order and duplicate elements are removed.

Step 2: A permutation table (*P_table*) is generated using the values from step 1 whose length is equal $(M_1 + N_1)$, where M_1 and N_1 are the row and column dimension of the combined input image.

Step 3: $Row\_P - table$ and $Column\_P - table$ are assigned to the combined input image using the values from step 2.

Step 4: If the particular $Row\_P - table$ is i, the corresponding row is circular right shifted to i positions.The Circular right shift is performed for all the rows with respect to its $Row\_P - table$ value. Similarly, if the particular $Column\_P - table$ value is j, the corresponding columns is circular down shifted to j positions.The Circular down shift is performed for all the column with respect to its $Column\_P - table$ value.

The above CST process is illustrated in Fig. 3 and Fig. 4 for shift row and shift column respectively. Algorithm 1 represents the pseudo code generated for CST.

C. ELLIPTIC CURVE OPERATIONS

Given an elliptic curve $E_p : y^2 \equiv x^3 + ax + b \bmod p$ and the seed point $S(x_s, y_s)$. The elliptic curve point $h.S(x_{hS}, y_{hS}) = S + S + S + \ldots h$ times, where h is an integer. $hS(x_{hS}, y_{hS})$ can be computed using Algorithm 2.

The algorithm to compute point addition $(P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2))$ when $P_1 \neq P_2$ or $P_1 == P_2$ is shown in Algorithm 3. Point subtraction $(P_3(x_3, y_3) = P_1(x_1, y_1) - P_2(x_2, y_2))$ is converted to point addition by converting the y_2 coordinate to negative as $(P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, -y_2))$.

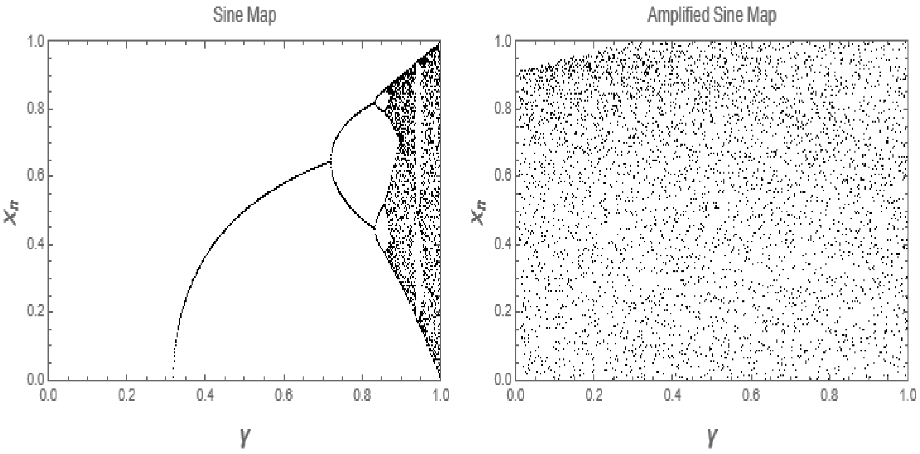
III. PROPOSED MULTIPLE IMAGE ENCRYPTION

The proposed multiple image encryption is as follows-

A. KEY GENERATION

The key generation of the proposed method is as follows:

Step 1: Combine all the input grayscale images into three planes of equal size and obtain a colour image I_1.



(a) (b)

FIGURE 1. Bifurcation diagram of (a) Sine map (b) Amplified Sine Map.

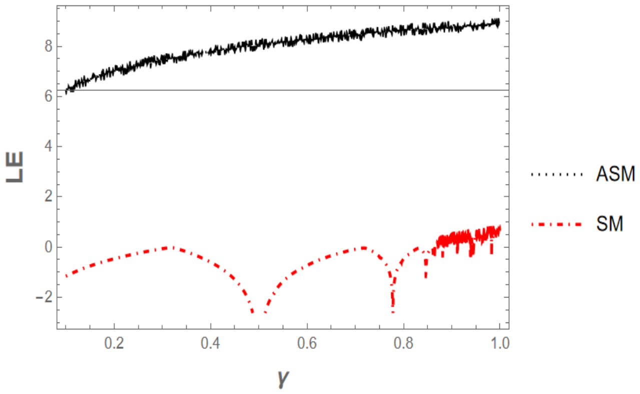


FIGURE 2. Lyaponov exponent of Sine map and Amplified Sine Map.

Step 2: Compute SHA-348 on I_1 to generate a 384-bit hash value (h).

Step 3: Compute $hS(x_{hS}, y_{hS})$ by performing an elliptic curve point multiplication between (h) and elliptic curve seed $S(x_s, y_s)$.

Step 4: Binarize x_{hS} and y_{hS} into 384 bits each and store as bin_x and bin_y respectively.

Step 5: Divide the 384-bits in bin_x and bin_y into three groups each of 128 bits and denote as hS_1, hS_2, hS_3, hS_4, hS_5 and hS_6.

Step 6: Generate the keys as:

$$x_{n1} = \frac{BaseConvert[hS_1, 2]}{2^{128}} \tag{3}$$

$$\delta_1 = \frac{BaseConvert[hS_2, 2]}{2^{128}} \tag{4}$$

$$\gamma_1 = 2200 + \frac{BaseConvert[hS_3, 2]}{2^{116}} \tag{5}$$

$$x_{n2} = \frac{BaseConvert[hS_4, 2]}{2^{128}} \tag{6}$$

$$\delta_2 = \frac{BaseConvert[hS_5, 2]}{2^{128}} \tag{7}$$

$$\gamma_2 = 2200 + \frac{BaseConvert[hS_6, 2]}{2^{116}} \tag{8}$$

where, x_{n1}, γ_1 and δ_1 will be used as the keys for the permutation table of the CST. x_{n2}, γ_2 and δ_2 will be used as the keys for generating a pseudorandom sequence PRS. $BaseConvert[list, b]$ converts the value of the list with respect to base b.

B. ENCRYPTION PROCESS

The encryption process is carried out as shown in the algorithm 4 and discussed below.

Step 1: Combine all the input grayscale images into three planes of equal size and obtain a colour image I_1.

Step 2: Perform CST on all the three planes of I_1 using algorithm 1 and the keys x_{n1}, γ_1 and δ_1.

Step 3: Using Equation 2 along with the keys x_{n2}, γ_2 and δ_2 generate a pseudo-random sequence PRS of length $(M_1 \times N_1 \times 3/4)$, where $(M_1 \times N_1)$ is the dimension of I_1.

Step 4: Compute $|ASM[i] \times 10^{16}|$ and base convert it using 256 as base upto eight terms and pick the elements at position three to six and store in PSR.

Step 5: Perform XoR operation between the values of Step 2 and PRS.

Step 6: Generate the cipher image.

C. KEY SHARING

The initial parameters $x_{n1}, \gamma_1, \delta_1, x_{n2}, \gamma_2$ and δ_2 are all generated from $h.S(x_{hS}, y_{hS})$. In order to decrypt the images exactly as the original images, the same set of initial parameters are required in the receiver side. $h.S(x_{hS}, y_{hS})$ is secretly shared as $h.S'(x'_{hS}, y'_{hS})$ to the communicating party. $h.S'(x'_{hS}, y'_{hS})$ is computed as:

$$h.S' = \{r.S, (h.S + r.R)\} \tag{9}$$

TABLE 1. Randomness Test on sequence generated from ASM.

	p-value			
Test	PRS_1	PRS_2	PRS_3	PRS_4
$\mathbb{P}_{Monobit\_Test}$	0.114023	0.165318	0.729901	0.680752
$\mathbb{P}_{Frequency\_within\_Block}$	0.072604	0.866317	0.360072	0.078637
$\mathbb{P}_{The\_Runs\_test}$	0.483461	0.277409	0.684825	0.635841
$\mathbb{P}_{Longest\_Run\_of\_Ones\_in\_a\_Block}$	0.876549	0.665436	0.978973	0.330148
$\mathbb{P}_{Binary\_Matrix\_Rank}$	0.769933	0.843884	0.211151	0.685974
$\mathbb{P}_{DFT}$	0.027444	0.166032	0.060573	0.674394
$\mathbb{P}_{Non\_Overlapping\_Template\_Matching}$	0.902773	0.748860	0.184214	0.632401
$\mathbb{P}_{Overlapping\_Template\_Matching}$	0.113538	0.729445	0.816368	0.533173
$\mathbb{P}_{Maurer's\_Test}$	0.340917	0.341394	0.341477	0.341314
$\mathbb{P}_{The\_Linear\_Complexity}$	0.963107	0.715299	0.654654	0.783117
$\mathbb{P}_{The\_Serial\_test}$				
p_{value1}	0.054239	0.045848	0.848333	0.557577
p_{value2}	0.311345	0.568182	0.787199	0.413601
$\mathbb{P}_{Approximate\_Entropy}$	0.325687	0.302375	0.952809	0.826108
$\mathbb{P}_{Cumulative\_Sums\_Test}$	0.136799	0.292317	0.805319	0.584062
$\mathbb{P}_{Random\_excursions\_(RE)}$				
μ=-4	0.456022	0.635523	0.334503	0.535901
μ=-3	0.025380	0.277903	0.643218	0.991606
μ=-2	0.040800	0.698853	0.996621	0.964991
μ=-1	0.451399	0.857202	0.989789	0.277537
μ=1	0.276993	0.037735	0.247846	0.618558
μ=2	0.997331	0.401898	0.448515	0.700175
μ=3	0.820459	0.915280	0.562327	0.770051
μ=4	0.909431	0.578684	0.920603	0.889179
$\mathbb{P}_{RE\_variant}$				
μ=-9	0.530572	0.814737	0.253302	0.988135
μ=-8	0.654857	0.796726	0.319525	0.790877
μ=-7	0.866288	0.935004	0.485979	0.680060
μ=-6	0.908247	0.879202	0.666247	0.454028
μ=-5	0.764333	0.969285	0.633487	0.248195
μ=-4	0.598262	0.793350	0.472330	0.378518
μ=-3	0.594076	0.598895	0.522350	0.880124
μ=-2	0.640260	0.636278	0.816809	0.894392
μ=-1	0.752924	0.682135	0.958262	0.951109
μ=1	0.322504	0.933048	0.807055	0.747530
μ=2	0.845610	0.662451	0.991964	0.703540
μ=3	0.680139	0.679403	0.906842	0.768170
μ=4	0.905293	0.895790	0.721803	0.981511
μ=5	0.685680	0.820013	0.429042	0.906449
μ=6	0.472378	0.884199	0.595252	0.728871
μ=7	0.508593	0.722342	0.857924	0.652246
μ=8	0.478775	0.477459	0.978439	0.936909
μ=9	0.376998	0.486857	0.996624	0.820595

where,

r is a random integer

R public of the receiver.

$R = key.S$

key is the private key of the receiver.

The receiver gets $(h.S(x_{hS}, y_{hS})$ from $h.S'(x'_{hS}, y_{hS})'$ by using Equation 10

$$h.S = (h.S + r.R) - key.r.S \tag{10}$$

D. DECRYPTION PROCESS

Using Equation 10, the receiver computes $(h.S(x_{hS}, y_{hS})$ from $h.S'(x'_{hS}, y_{hS})'$ using his/her private key key. The initial parameters x_{n1}, γ_1, δ_1, x_{n2}, γ_2 and δ_2 are generated from the shared key $(h.S(x_{hS}, y_{hS})$ using Step 4 to Step 6 given in III-A. The decryption process of the proposed method is as follows:

Step 1: Using Equation 2 along with the keys x_{n2}, γ_2 and δ_2 generate a pseudorandom sequence PRS of length $(M_1 \times N_1 \times 3)$, where $(M_1 \times N_1)$ is the dimension of C_1.

Step 2: Perform XoR operation between PRS and the three planes of C_1.

Step 3: Perform reverse CST on the three planes of step 2 using the permutation table the keys x_{n1}, γ_1, δ_1.

Step 4: Separate the three planes of Step 3.

Step 5: Extract all the plain images from Step 4.

IV. SIMULATIONS

The proposed multiple grayscale image encryption is simulated using Wolfram Mathematica 13 on a Fujitsu Celsius Workstation with Intel Xeon(R) W-2133 @ 3.60 GHz and

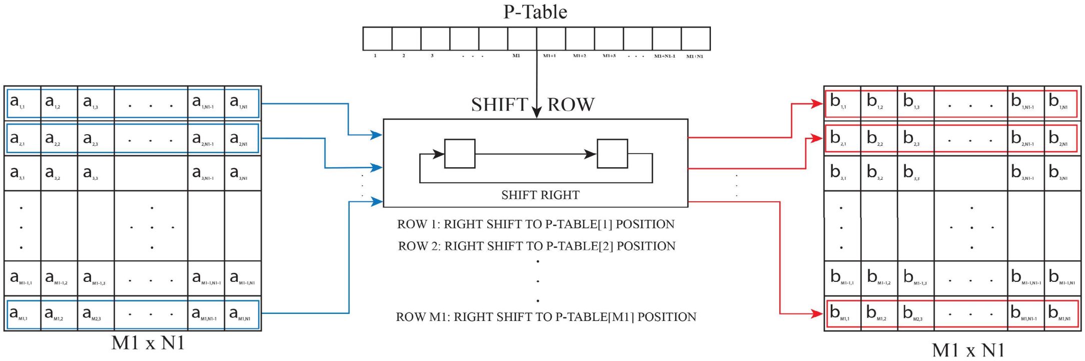

P-Table
1
2
3
M1
M1+1
M1+2
M1+3
M1+N1-1
M1+N1
SHIFT ROW
SHIFT RIGHT
ROW 1: RIGHT SHIFT TO P-TABLE[1] POSITION
ROW 2: RIGHT SHIFT TO P-TABLE[2] POSITION
ROW M1: RIGHT SHIFT TO P-TABLE[M1] POSITION
M1 x N1
M1 x N1

FIGURE 3. Shift Row Operation.

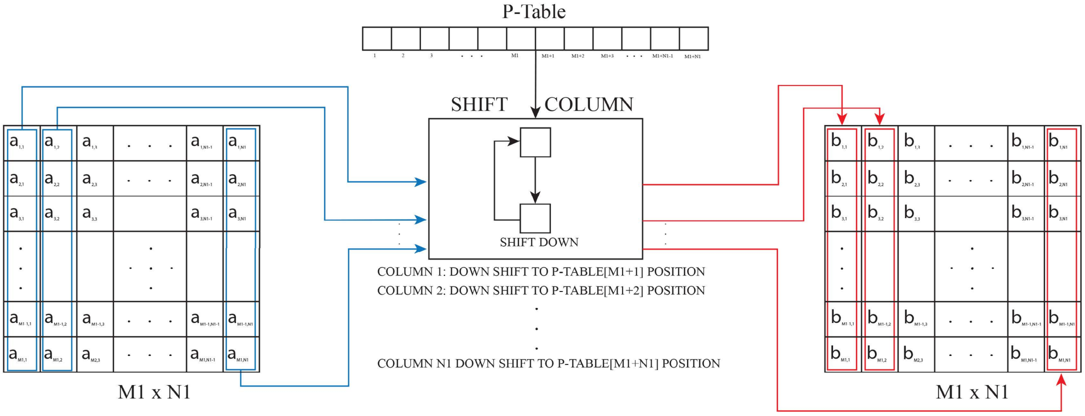

P-Table
1
2
3
M1
M1+1
M1+2
M1+3
M1+N1-1
M1+N1
SHIFT COLUMN
SHIFT DOWN
COLUMN 1: DOWN SHIFT TO P-TABLE[M1+1] POSITION
COLUMN 2: DOWN SHIFT TO P-TABLE[M1+2] POSITION
COLUMN N1 DOWN SHIFT TO P-TABLE[M1+N1] POSITION
M1 x N1
M1 x N1

FIGURE 4. Shift Column Operation.

a ram of 32GB. The experimental images were downloaded from the USC-SIPI database [40]. In this paper, due to space limitations, we used 12 (twelve) images to form a single combined RGB image (C_I). Each plane of the RGB is composed of 4 (four) grayscale images. Experimental analysis are carried out on four combine images- C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4}. The image representation of C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4} are shown in the Fig. (6a, 6c, 6e and 6g) respectively. The images used in combine images- C_{I-1}, C_{I-2}, C_{I-3}, C_{I-4} and its respective planes are shown in Table 2. The proposed method can encrypt and decrypt the multiple grayscale images successfully.

V. SECURITY ANALYSIS

A. PSNR AND SSIM

The peak-signal-to-noise-ratio (PSNR) and structural-similarity-index (SSIM) are used to ascertain the accuracy of the image after the decryption. The computed values are shown in Table 3. The PSNR and SSIM are calculated using the below formula:

$$\mathrm{PSNR} = 20 \times \log_{10} \frac{Max^m_{p_{\mathrm{value}}}}{Mean_{s_{\mathrm{error}}}} \tag{11}$$

$$Mean_{s_{\mathrm{error}}} = \frac{1}{M_1 \times N_1} \sum_{i=0}^{M_1-1} \sum_{j=0}^{N_1-1} [\mathrm{O_{Img}}(i,j) - D_{img}(i,j)]^2 \tag{12}$$

where $Max^m_{p_{value}}$: maximum supported pixel value. $Mean_{s_{\mathrm{error}}}$: mean squared error. $M_1 \times N_1$: dimension of the image. $O_{Img}(i,j)$: original image pixel value at index (i,j).$D_{Img}(i,j)$: decrypted image pixel value at index (i,j).

$$\mathrm{SSIM}(x,y) = \frac{\left(2M_v^x M_v^y + c_v\right)\left(2Co_v^{xy} + c'_v\right)}{\left((M_v^x)^2 + (M_v^y)^2 + c_v\right)\left((S_v^x)^2 + (S_v^y)^2 + c'_v\right)} \tag{13}$$

where M_v^x = mean value of $x.M_v^y$ = mean value of $y.S_v^x$ = standard deviation value of $x.S_v^x$ = standard deviation value of $y.Co_v^{xy}$ = covariance value of x and y. $c_v = (k_v L_v)^2 \cdot c'_v = \left(k'_v L_v\right)^2 .k_v = 0.01$ and $k'_v = 0.03.L_v = 2^{\mathrm{count}} - 1$. *count*= no. of bit per pixel.

B. KEY SPACE

A key space is the total number of all the possible keys for a given encryption scheme. The key space in an ideal encryption technique should be large enough to resist a brute force attack. The keys used in the proposed method are

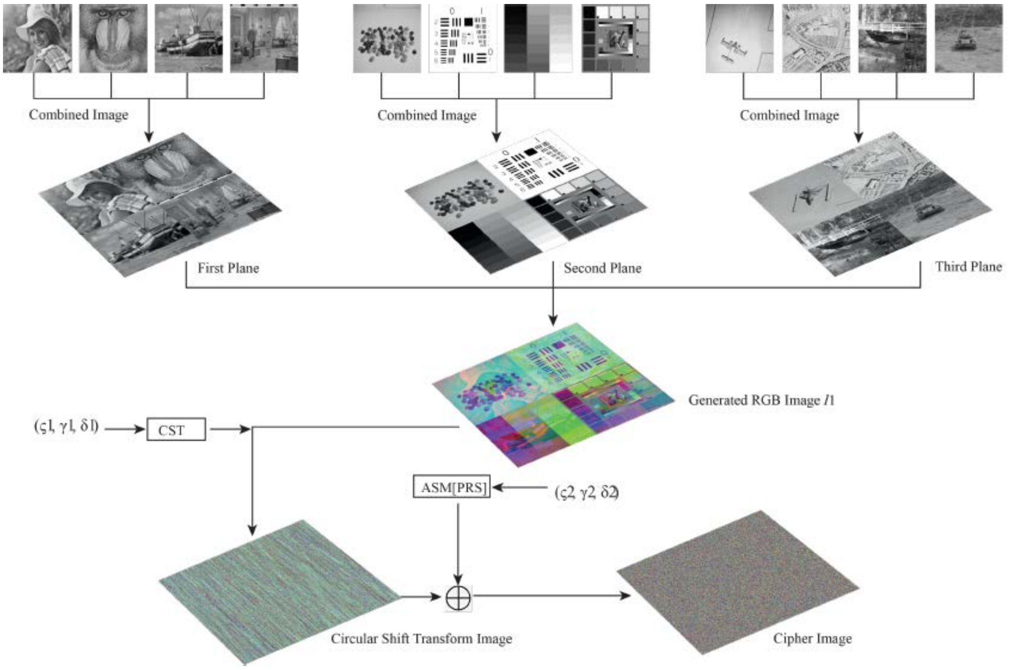


FIGURE 5. The process of encryption using ASM and CST for multiple images.

$(x_{n1}, \gamma_1, \delta_1, x_{n2}, \gamma_2, \delta_2)$. As a result, the suggested enhanced encryption scheme's total key space is 2^{332} (approx). The value is sufficiently big to overcome any type of brute force attack.

C. HISTOGRAM ANALYSIS

An image histogram is an analysis of the statistical attack which is shown graphically by plotting the frequency. The frequency is the plot on every pixel value across all the pixel values possible. The histogram of a plain image shows uneven pixel frequency distribution while the histogram of a well decrypted image shows equal pixel frequency distribution. Fig. (6a, 6b, 6c, 6d) and (6e, 6f, 6g, 6h) shows the plane images and the cipher images. Fig. (7a, 7b, 7c, 7d) and (7e, 7f, 7g, 7h) represents the histogram of the plane images and histogram of the cipher images.

D. COMPLEXITY OF THE PROPOSED METHOD

The computational complexity of the proposed method can be summarised as:

1) The time complexity of generating the ASM sequence for the permutation table is $O(3 \times (M_1 + N_1))$.
2) The time complexity of performing the CST operation on the three planes is $O(3 \times (M_1 + N_1))$.
3) The time complexity of generating the chaotic sequence PSR is $O(3 \times M_1 \times N_1)$.
4) The time complexity of performing a bit-XOR operation on two n-bit value is O(n) and each values are represented by 8-bits. So, the time complexity of performing bit-XOR operation in between CST$[T_1]$ and PSR is $O(8 \times 3 \times M_1 \times N_1)$

The overall time complexity to execute the encryption procedure is $O(3 \times (M_1 + N_1)) + O(3 \times (M_1 + N_1) + O(3 \times M_1 \times N_1) + O(8 \times 3 \times M_1 \times N_1) = O(27M_1N_1) + O(6(M_1 + N_1)$

E. INFORMATION ENTROPY ANALYSIS

The information entropy analyses how the image has randomness in it by computing:

$$E_p(\chi) = -\sum_{i=1}^{n} P_b(\chi_i) \log_\beta P_b(\chi_i) \tag{14}$$

where $E_p(\chi)$: entropy. $P_b(\chi_i)$: probability mass function. $\beta = 2$. The entropy value is shown in Table 4 which is computed using equation 14 on the cipher images.A Comparison of the entropy with the other state of the art methods is tabulated in Table 10.

F. AVALANCHE EFFECT

The Avalanche effect is an idea related to the specific behaviour of the arithmetic function used in encryption. It states that "a minor variation in plain text can impact a substantial variation in the cipher text". As a result, it's one of the processes to check for desirable qualities of the cipher image. An effective encryption technique is predicted to be good if the value of the avalanche is very near to 50 *percent*. For the suggested approach, the avalanche value for the cipher image Fig. (8b, 8e, 8h, 8k) generated by the plain image Fig. (8a, 8d, 8g, 8j) and the cipher image Fig. (8c, 8f, 8i, 8l) derived by some minor variation in the pixel value of plain image Fig. (8a, 8d, 8g, 8j) is shown in the Table 5.

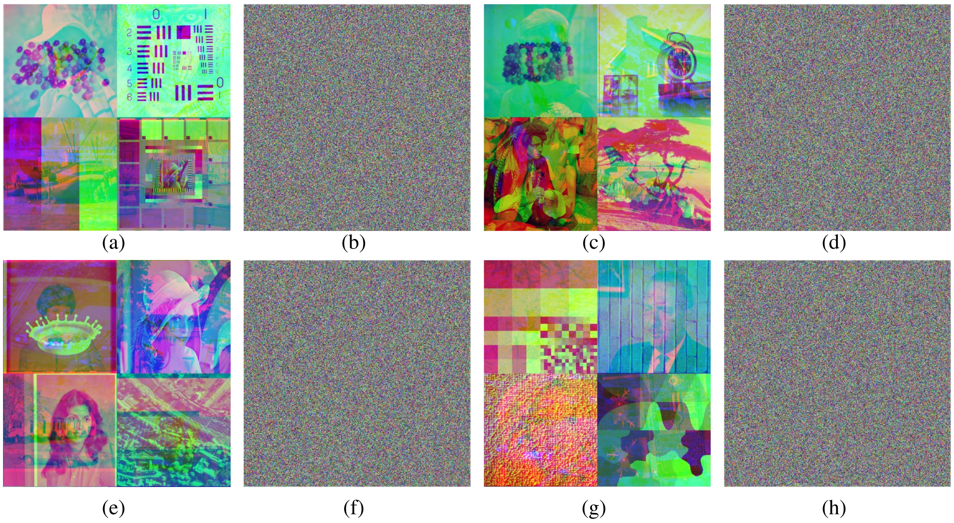

(a) (b) (c) (d) (e) (f) (g) (h)

FIGURE 6. **(a, c, e, g) Combined images C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4}. (b, d, f, h) Cipher image of C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4}.**

```
Algorithm 1: The Process of CST
  Input: INPUT IMAGE $I_1$, image size $M_1 \times N_1$, ASM
         initial parameters $(x_{n1}, \gamma_1, \delta_1)$
  Output: CST IMAGE, image size $M_1 \times N_1$
  for $i \leftarrow 1$ to $M_1 + N_1$ do
      Generate $ASM[i]$
      $i++$
  end for
  $Seq_x = ASM[[1; ; M_1]]$
  $Seq_y = ASM[[M_1 + 1; ; N_1]]$
  $Sort_x = Sort\ (Seq_x)$
  $Sort_y = Sort\ (Seq_y)$
  for $i \leftarrow 1$ to $Length[Seq_x]$ do
      $Row\_P - table[i]$ = Position of $Sort_x$[i] in $Seq_x$
      $i++$
  end for
  for $i \leftarrow 1$ to $Length[Seq_y]$ do
      $Column\_P - table[i]$ = Position of $Sort_y$[i] in $Seq_y$
      $i++$
  end for
  for $i \leftarrow 1$ to $Row\_P - table[i]$ do
      RotateRight, $Row[i]$ of $I_1$ by $Row\_P - table[i]$
        position
      $i++$
  end for
  for $i \leftarrow 1$ to $Column\_P - table[i]$ do
      RotateDown, $Column[i]$ of $I_1$ by
        $Column\_P - table[i]$ position
      $i++$
  end for
```

```
Algorithm 2: Elliptic Curve Point multiplication(.)
  Input: $a, b, p, S(x_s, y_s), h$
  Output: $h.S(x_{hS}, y_{hS})$
  Start with $n = h$, $P_1 = \infty$, $P_2 = S$
  while $(n \neq 0)$ do
      if $(n \bmod 2 == 0)$ then
          $n = n/2$
          $P_1 = P_1$
          update $P_2 = P_2 + P_2$
      end if
      else
          $n = n - 1$
          update $P_1 = P_1 + P_2$
          $P_2 = P_2$
      end if
  end while
  if $(n == 0)$ then
      $P_1 = hS(x_{hS}, y_{hS})$
  end if
```

```
Algorithm 3: Elliptic Curve Point addition(+)
  Input: $a, b, p, P_1(x_1, y_1), P_2(x_2, y_2)$
  Output: $P_3(x_3, y_3)$
  if $(P_1(x_1, y_1) \neq P_2(x_2, y_2))$ then
      $\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$
      $x_3 = \lambda^2 - x_1 - x_2 \bmod p$
      $y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$
  end if
  else if $(P_1(x_1, y_1) == P_2(x_2, y_2))$ then
      $\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p$
      $x_3 = \lambda^2 - 2\,x_1 \bmod p$
      $y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$
  end if
```

G. OCCLUSION ATTACK

Occluded data occurs because of the lack of security in the channel while transferring the encrypted image to the receiver. In our analysis the cipher image generated were occluded 6.5%,12.5%, 25% and 50%. The occluded cipher images were performed decryption process. The results of

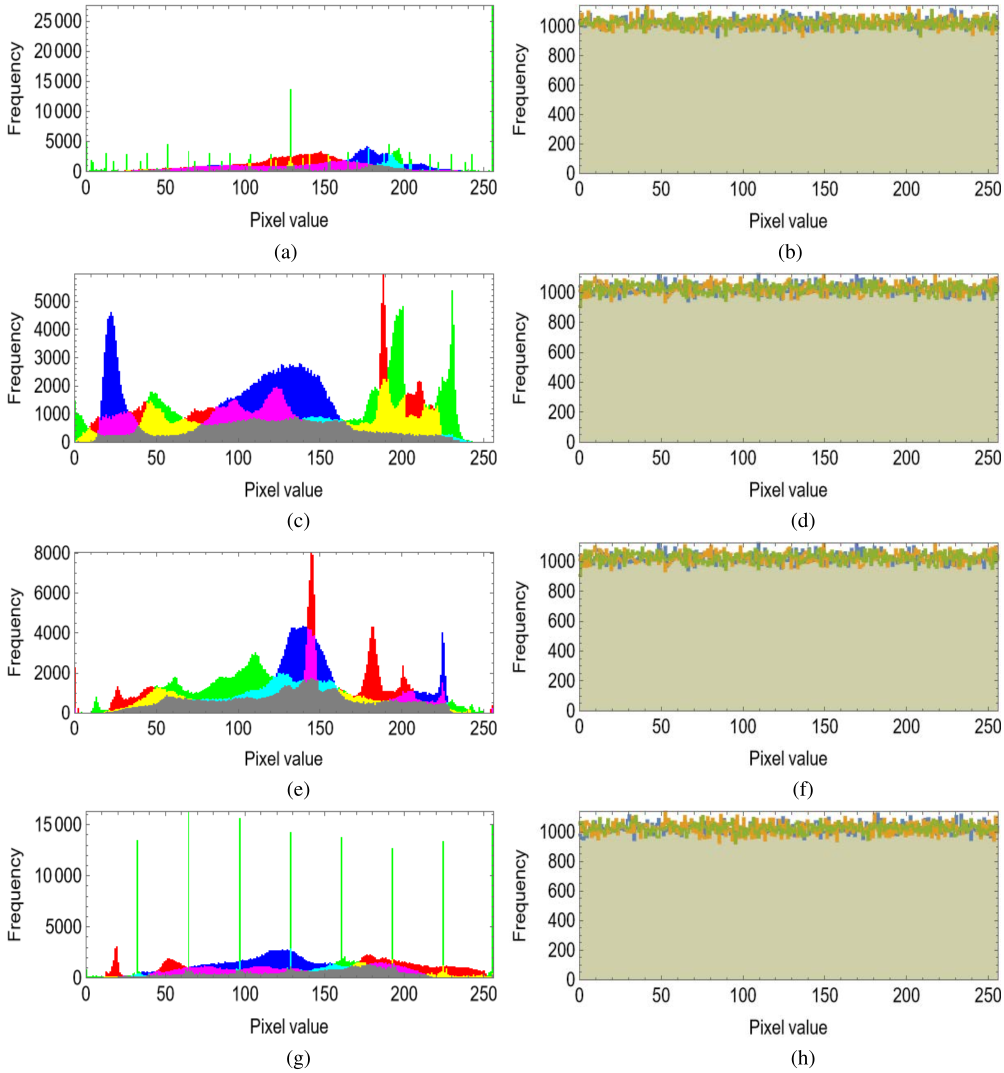


FIGURE 7. (a, c, e, g) Histogram of Combined images, C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4}. (b, d, f, h) Histogram of Cipher image, C_{I-1}, C_{I-2}, C_{I-3} and C_{I-4}.

Algorithm 4: The Encryption Process

```
Input: INPUT IMAGE $I_1$, image size $M_1 \times N_1$, $x_{n1}$, $\gamma 1$,
       $\delta 1$, $x_{n2}$, $\gamma 2$ and $\delta 2$
Output: CIPHER IMAGE $C_1$, image size $M_1 \times N_1$
CST[$I_1$] $\leftarrow I_1, \gamma_1, \delta_1, x_{n1}$.
for $i \leftarrow 1$ to $M_1 \times N_1 \times 3/4$ do
    Generate $ASM[i] \leftarrow \gamma_2, \delta_2, x_{n2}$
    $i{+}{+}$
end for
$PSR \leftarrow$ BaseConvert[|$ASM[i] \times 10^{15}$|,256,8][[3;;6]]
$C_1$=$PSR$ XoR CST[$I_1$]
```

the occlusion attack are represented in Fig. 8, which is identifiable with some pixels lost. The PSNR value of the occluded images was calculated with the original image and the decrypted image. The values were tabulated in the Table 6.

H. KEY SENSITIVITY

An ideal cryptographic scheme should have good key sensitivity. A slight change in the key should completely alter the output of the cryptographic scheme. Fig. 8 shows the output using the original key and by altering one bit of data in the original key.

I. DIFFERENTIAL ATTACKS

In order to prevent the differential attack, the cipher image C_{img1} and the cipher image C_{img2} derived by some minor variation in the pixel value of the plain image. They both should be random enough that the pixel index should not be similar. Two methods to estimate the intensity of a differential attack are the Number of Pixel Changes (NPCR) and the Unified Averaged Changed Intensity (UACI). The theoretically ideal value of NPCR and UACI should be closed to 100% and 33.3% [42] respectively. The rate of pixel change of the cipher

TABLE 2. Image file used in C_{I-1}, C_{I-2}, C_{I-3}, C_{I-4} and its respective planes.

	Plane-1	Plane-2	Plane-3
C_{I-1}	Elaine	Jelly beans	Airplane
	Mandrill	Resolution chart	Aerial
	Boat	21 level step wedge	Stream and bridge
	Couple	Testpat.1k	Tank
C_{I-2}	Female	Jelly beans	Moon surface
	House	Clock	Aerial
	Peppers	Male	Airplane (U-2)
	Airplane (F-16)	Tree	Car and APCs
C_{I-3}	Female	Splash	Chemical plant
	Sailboat on lake	Lena	Airplane
	House	Female	APC
	Tile roof	Aerial	Tank
C_{I-4}	San Francisco and Oakland	USC texture mosaic #2	Truck
	Walter Cronkite, frame 7	Brodatz - Brick wall (D94)	San Diego (Downtown)
	Tiffany	Brodatz - Raffia (D84 H.E.)	Chemical Plant (close view), frame 12
	Airport	USC texture mosaic #3 (info)	Truck and APCs

TABLE 3. PSNR and SSIM values of encrypted and decrypted image.

Image ID	ENCRYPTED			
	PSNR			
	Plane-1	Plane-2	Plane-3	RGB Generated Image
C_{I-1}	9.48398	7.10247	8.94423	8.38622
C_{I-2}	8.56415	7.96293	8.60384	8.36692
C_{I-3}	9.05205	9.13934	9.78612	9.31371
C_{I-4}	8.09153	8.17246	9.35814	8.50339
	SSIM			
C_{I-1}	0.004886	0.008521	0.007757	0.007121
C_{I-2}	0.004446	0.004854	0.005617	0.005047
C_{I-3}	0.008361	0.009821	0.009357	0.007624
C_{I-4}	0.004222	0.006217	0.006978	0.005562
	DECRYPTED			
	PSNR			
C_{I-1}	∞	∞	∞	∞
C_{I-2}	∞	∞	∞	∞
C_{I-3}	∞	∞	∞	∞
C_{I-4}	∞	∞	∞	∞
	SSIM			
C_{I-1}	1	1	1	1
C_{I-2}	1	1	1	1
C_{I-3}	1	1	1	1
C_{I-4}	1	1	1	1

TABLE 4. Entropy values for plane image and encrypted images.

Image ID	ENTROPY ANALYSIS			
	PLANE IMAGE			
	Plane-1	Plane-2	Plane-3	RGB Generated Image
C_{I-1}	7.4114	6.0631	7.4520	7.3769
C_{I-2}	7.66142	7.5632	7.2816	7.7757
C_{I-3}	7.4292	7.6193	7.2586	7.5964
C_{I-4}	7.7714	6.5995	7.4751	7.6119
	ENCRYPTED IMAGE			
C_{I-1}	7.9993	7.99913	7.9993	7.9997
C_{I-2}	7.9992	7.9992	7.9993	7.9998
C_{I-3}	7.9992	7.9993	7.9993	7.9998
C_{I-4}	7.9993	7.9992	7.9994	7.9997

TABLE 5. Avalanche value for cipher image on 1 bit changed in plain image.

AVALANCHE EFFECT			
Input Image	Cipher Image	1 bit changed Cipher Image	Avalanche value
Fig. 8a	Fig. 8b	Fig. 8c	50.0051
Fig. 8d	Fig. 8e	Fig. 8f	50.0452
Fig. 8g	Fig. 8h	Fig. 8i	50.0052
Fig. 8j	Fig. 8k	Fig. 8l	50.0060

images C_{img1} and C_{img2} is measured by NPCR:

$$NPCR_1 = \frac{1}{M_1 \times N_1} \times \sum_{i,j} D_1(i,j) \times 100 \tag{15}$$

The average variation of the intensity between original image and cipher image is measured by UACI using the below expression.

$$UACI_1 = \frac{1}{M_1 \times N_1}\left[\sum_{i,j} \frac{\left|C_{img1}(i,j) - C_{img2}(i,j)\right|}{L_1}\right] \tag{16}$$

where,$NPCR_1$ represents the NPCR and $UACI_1$ represents UACI of the 512-grayscale image. The size of the images is represented by $M_1 \times N_1$, L_1 represents the largest pixel that can be supported and $D_1(i,j)$ is represented by the below expression.

$$D_1(i,j) = \begin{cases} 0 & \text{if } \mathrm{C}_{img1}(i,j) = C_{img2}(i,j) \\ 1 & \text{if } \mathrm{C}_{img1}(i,j) \neq \mathrm{C}_{img2}(i,j) \end{cases} \tag{17}$$

The value for NPCR and UACI on four different images i.e in the Fig. (6a, 6c, 6e, 6g) is shown in the Table 7. The NPCR and

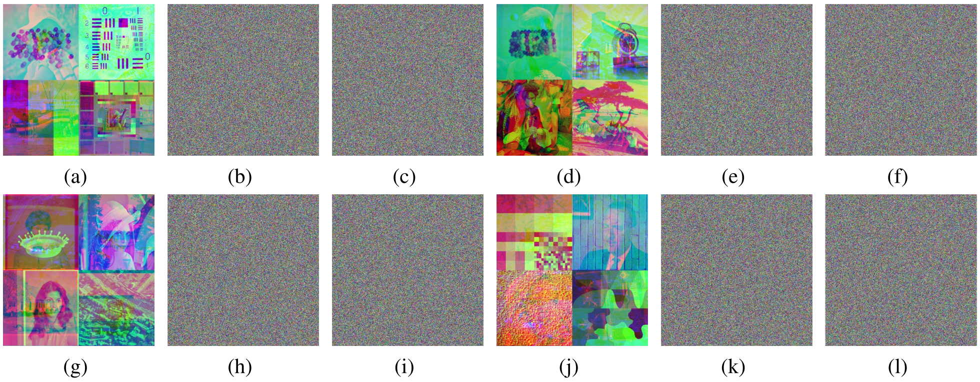


FIGURE 8. (a, d, g, j) plain images with the (b, e, h, k) cipher images and (c, f, i, l) is cipher image obtained with some minor variation in pixel value of (a, d, g, j) plain images.

TABLE 6. PSNR and SSIM values of occluded image.

Occluded	DECRYPTED			
	PSNR			
	Plane-1	Plane-2	Plane-3	RGB Generated Image
6.5%	21.5367	19.2475	21.0487	20.4953
12.5%	18.5321	16.1732	17.9929	17.4446
25%	15.5407	13.1602	15.0030	14.4440
50%	12.5158	10.1017	11.9643	11.4000
	SSIM			
6.5%	0.883532	0.937480	0.898828	0.921827
12.5%	0.780136	0.873636	0.804373	0.845148
25%	0.605407	0.749855	0.641571	0.702832
50%	0.339607	0.501377	0.376721	0.441476

TABLE 7. Result of the proposed approach for NPCR and UACI taken on four sets of images.

Image ID	NPCR and UACI			
	NPCR			
	Plane-1	Plane-2	Plane-3	RGB Generated Image
C_{I-1}	99.6235	99.5987	99.6037	99.6086
C_{I-2}	99.6098	99.6223	99.6040	99.6120
C_{I-3}	99.5945	99.6052	99.6067	99.6021
C_{I-4}	99.5964	99.5983	99.5918	99.5955
	UACI			
C_{I-1}	33.4265	33.5271	33.4461	33.4666
C_{I-2}	33.4741	33.5335	33.4141	33.4739
C_{I-3}	33.4452	33.4745	33.4832	33.4676
C_{I-4}	33.4748	33.4283	33.4428	33.4486

UACI comparison with other proposed methods are tabulated in Table 10.

J. CORRELATION ANALYSIS

The correlation of an image is computed as:

$$\text{Correlation}\,[vec_1, vec_2] = \frac{\text{Co}_{\text{variance}}\,[vec_1, vec_2]}{\rho\ [vec_1] \times\ \rho\ [vec_2]} \tag{18}$$

Here, $\text{Co}_{variance}$ is the covariance. ρ is the standard deviation. vec_1 and vec_2 are the input vectors.

The orientation of the horizontal, vertical and diagonal which is denoted by H_{tal},V_{cal} and D_{nal} of Plane-1, Plane-2, Plane-3 and the generated RGB image correlation coefficient is shown in the Table 8. The correlation coefficient along the H_{tal},V_{cal} and D_{nal} direction of RGB generated plain image and cipher image is plotted by computing with 10000 random pixel values as shown in Fig. 10.

K. RANDOMNESS ANALYSIS FOR ENCRYPTED IMAGES

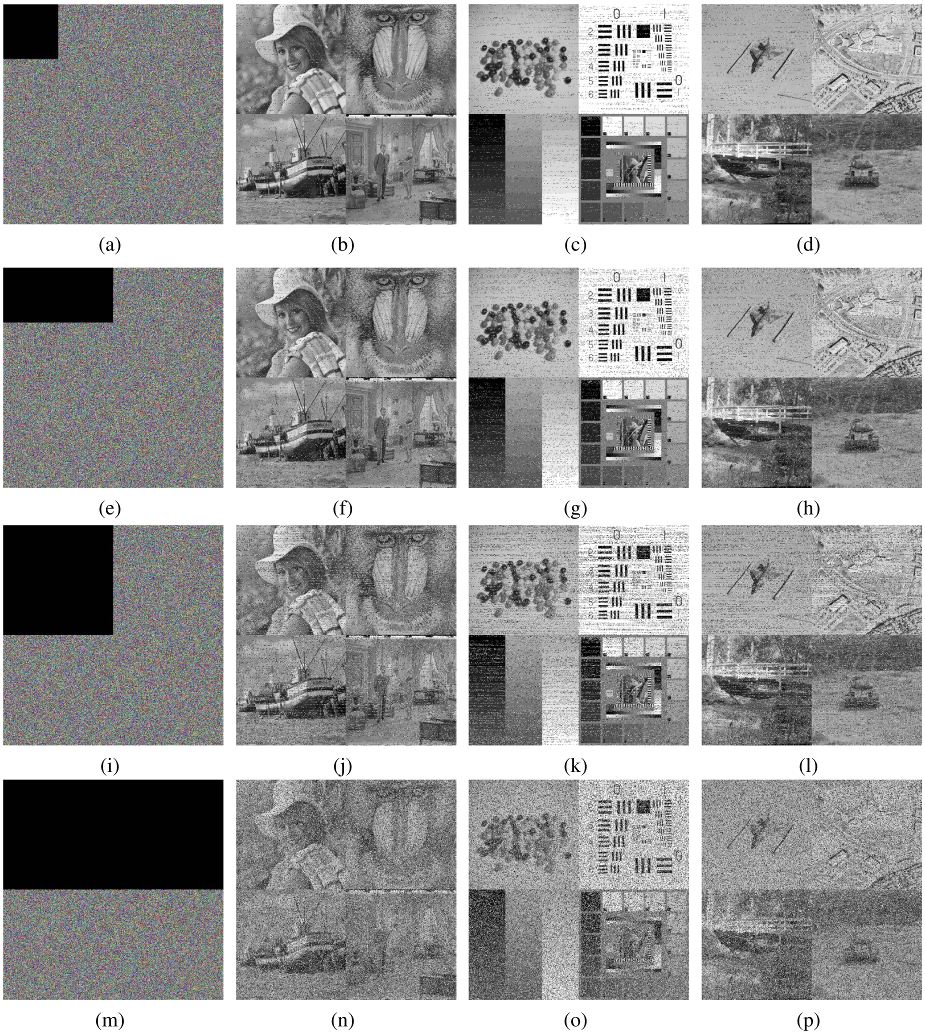
The randomness of the cipher is checked by performing the NIST test on the cipher image. The proposed approach uses the NIST test to analyze the randomness of the generated cipher image. The NIST test is proposed by Andrew *et al.* [41] and it consists of 15 different tests. For each and every test p-value are calculated. A cipher image is considered to be random if the p-value is more than 0.01. The NIST test is performed on the cipher images shown in Fig. (8b, 8e, 8h, 8k) using the proposed encryption method and Table 9 shows the result of the test.

L. ATTACK ANALYSIS

The proposed method has got a vast keyspace. So, when an adversary has only cipher-text information, the proposed method will withstand the exhaustive key attack. The proposed method can also withstand Known plain-text attacks. The initial keys for the enhanced chaotic map are derived from the Secure Hash Algorithm's hash value. So every different image that may differ just by one bit also generates a different hash value leading to different initial values for the enhanced chaotic map.

M. COMPARISON AND DISCUSSION

The proposed multiple image encryption scheme is compared with some of the recent related works [16], [17], [18], [19], [20], [34], [35], [36], [37] that encrypts multiple images where each image is of image dimension 512 × 512. The comparison is made with respect to correlation, NPCR, UACI, Entropy, Key-space, Number of images encrypted per execution and execution time of encryption per image as tabulated in Table 10.



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

FIGURE 9. **(a, e, i, m) Occluded cipher images with 6.25%, 12.5%, 25% and 50% occlusion. (b, f, j, n) Decrypted Plane-1, (c, g, k, o) Decrypted Plane-2 and (d, h, l, p) Decrypted Plane-3 of occluded cipher images.**

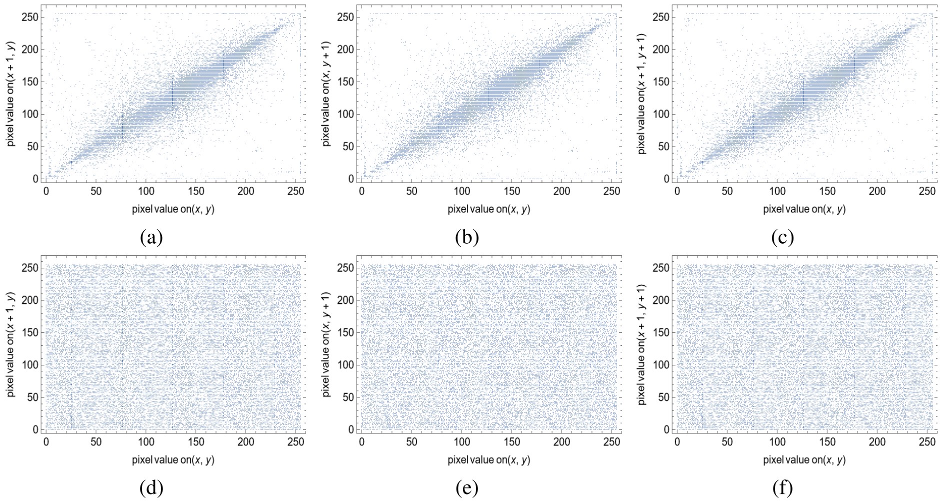
TABLE 8. **Correlation coefficient for plane image and encrypted images.**

Image ID	CORRELATION ANALYSIS								
		PLANE IMAGE				ENCRYPTED IMAGE			
	Orientation	Plane-1	Plane-2	Plane-3	RGB Generated Image	Plane-1	Plane-2	Plane-3	RGB Generated Image
C_{I-1}	H_{tal}	0.909781	0.936636	0.930746	0.934057	-0.012985	0.008586	-0.001810	0.002425
	V_{cal}	0.889481	0.937112	0.902513	0.934057	0.000438	0.012843	0.006502	0.005525
	D_{nal}	0.835325	0.885604	0.865775	0.884037	-0.019161	0.002223	-0.006094	-0.002245
C_{I-2}	H_{tal}	0.972168	0.965771	0.964949	0.969488	-0.003857	-0.001560	0.000335	0.000320
	V_{cal}	0.971038	0.962514	0.953313	0.967228	-0.011751	-0.008611	-0.006261	-0.007152
	D_{nal}	0.948791	0.935795	0.925495	0.943163	0.003872	-0.003285	0.008805	0.001648
C_{I-3}	H_{tal}	0.954617	0.937343	0.955608	0.956955	-0.003945	0.006344	0.010601	0.001667
	V_{cal}	0.929687	0.950617	0.953111	0.947382	-0.004951	0.002170	-0.005767	-0.002069
	D_{nal}	0.902684	0.898827	0.925674	0.919395	-0.012216	0.015475	-0.000344	-0.005128
C_{I-4}	H_{tal}	0.973644	0.871123	0.948498	0.930578	0.001790	-0.000889	-0.015010	0.012250
	V_{cal}	0.980236	0.845536	0.931035	0.919622	-0.016426	-0.002640	0.006814	-0.004834
	D_{nal}	0.962030	0.774278	0.899960	0.878867	-0.005515	0.001313	0.000736	-0.004180

TABLE 9. Randomness Test.

	p-value			
Test	C_{I-1}	C_{I-2}	C_{I-3}	C_{I-4}
$\mathbb{P}_{Monobit\_Test}$	0.228584	0.258872	0.631787	0.734702
$\mathbb{P}_{Frequency\_within\_Block}$	0.069345	0.029659	0.195985	0.903805
$\mathbb{P}_{The\_Runs\_test}$	0.446026	0.966441	0.895422	0.609479
$\mathbb{P}_{Longest\_Run\_of\_Ones\_in\_a\_Block}$	0.292414	0.329523	0.158241	0.117309
$\mathbb{P}_{Binary\_Matrix\_Rank}$	0.762835	0.238650	0.955868	0.817738
$\mathbb{P}_{DFT}$	0.027444	0.040120	0.060573	0.011204
$\mathbb{P}_{Non\_Overlapping\_Template\_Matching}$	0.361925	0.317796	0.255528	0.780320
$\mathbb{P}_{Overlapping\_Template\_Matching}$	0.231136	0.535481	0.698407	0.401081
$\mathbb{P}_{Maurer's\_Test}$	0.341355	0.341364	0.341577	0.341612
$\mathbb{P}_{The\_Linear\_Complexity}$	0.565642	0.751541	0.710082	0.483984
$\mathbb{P}_{The\_Serial\_test}$				
p_{value1}	0.219754	0.161922	0.662197	0.844905
p_{value2}	0.774005	0.136057	0.391674	0.940593
$\mathbb{P}_{Approximate\_Entropy}$	0.580378	0.425981	0.878009	0.039330
$\mathbb{P}_{Cumulative\_Sums\_Test}$	0.289672	0.126155	0.635901	0.381256
$\mathbb{P}_{Random\_excursions\_(RE)}$				
μ=-4	0.672276	0.897589	0.786081	0.255167
μ=-3	0.161120	0.845869	0.667460	0.604759
μ=-2	0.207747	0.933182	0.534978	0.454643
μ=-1	0.893072	0.154353	0.457261	0.993085
μ=1	0.522128	0.633477	0.442125	0.342124
μ=2	0.225867	0.931063	0.122214	0.161002
μ=3	0.529444	0.309192	0.894601	0.184282
μ=4	0.469220	0.515440	0.401039	0.110656
$\mathbb{P}_{RE\_variant}$				
μ=-9	0.730301	0.465181	0.529296	0.985735
μ=-8	0.926899	0.330500	0.440656	0.746249
μ=-7	0.874706	0.203675	0.539358	0.735840
μ=-6	0.780585	0.137631	0.693129	0.755658
μ=-5	0.831170	0.078185	0.790453	0.863425
μ=-4	0.747203	0.067949	0.982061	0.966661
μ=-3	0.726637	0.203922	0.906812	0.960558
μ=-2	0.869635	0.314435	0.757231	0.915259
μ=-1	0.669815	0.363316	0.905291	0.911948
μ=1	0.319767	0.460141	0.086654	0.285090
μ=2	0.267938	0.463802	0.540955	0.067219
μ=3	0.171741	0.952723	0.741476	0.092681
μ=4	0.107039	0.528745	0.418248	0.443523
μ=5	0.169454	0.874596	0.512860	0.658253
μ=6	0.415505	0.643699	0.513818	0.449804
μ=7	0.594601	0.717026	0.376492	0.283073
μ=8	0.474222	0.988295	0.223782	0.215993
μ=9	0.408044	0.807659	0.126161	0.321033

With respect to statistical analyses such as correlation (horizontal, vertical, diagonal), NPCR, UACI and entropy, all the compared related works in [16], [17], [18], [19], [20], [34], [35], [36], and [37] show a comparable result. For a good cipher image, the correlation coefficients are expected to have a value close to zero, indicating a weak correlation between the pixels in the cipher image. The proposed and compared methods can generate a low correlated cipher image. The NPCR and UACI data indicate that the proposed and compared methods can resist differential attacks. With eight bits representing each pixel of the cipher image, the maximum entropy value is eight. The proposed and compared methods can generate an entropy value of nearly eight. The key space for all the compared related work is large enough to resist Brute force attack with [18] having the maximum of 2^{648} and [17] having the maximum of 2^{128}. The proposed method has a moderate key space of 2^{332}. The claimed key space of [34] is 2^{628}, which consists of eight initial parameters derived from the hash value of SHA-256 applied on the input images with a precision of 10^{14} and a set of fixed eight external parameters $(c_1, c_2, \ldots, c_8)$. As the external parameters are fixed and the initial parameters of the chaotic system are derived from the hash value of SHA-256, the actual key-space is 2^{256}. The proposed method can encipher twelve secret images which is more than the those given in [16], [18], [19], [20], [34], and [36] except for [17], [35], and [37] with any i numbers of images. Theoretically, in [17], [35], and [37], i numbers of images can be given as input. However,



(a) (b) (c)

(d) (e) (f)

FIGURE 10. **(a, b, c) H_{tal},V_{cal} and D_{nal} correlation graphs of generated RGB plane image. (d, e, f) H_{tal},V_{cal} and D_{nal} correlation graphs of encrypted image.**

TABLE 10. **Comparison.**

Scheme	Horizontal Correlation	Vertical Correlation	Diagonal Correlation	NPCR	UACI	Entropy	Key-space	Number of image(s)	Encryption time/image (sec.)
Ref. [16]	-0.0019	-0.0066	0.0031	99.61 %	33.45 %	7.9993	2^{286}	4	43
Ref. [17]	0.0016	0.0022	0.0007	99.61 %	33.57 %	7.9992	2^{128}	$i^2, i \in \mathbb{Z}$	0.04
Ref. [18]	-0.0036	0.0026	0.0012	99.59 %	33.48 %	7.9995	2^{648}	4	0.24
Ref. [19]	0.0020	-0.0047	0.0028	99.61 %	33.47 %	7.9993	1.24×2^{237}	4	0.32
Ref. [20]	-0.0036	0.0016	-0.0058	99.61 %	33.48 %	7.9999	2^{512}	8	0.07
Ref. [34]	-0.0003	0.0011	0.0013	99.60 %	33.51 %	7.9998	2^{628}	4	0.42
Ref. [35]	0.0023	0.0052	0.0024	99.61 %	33.47 %	7.9996	1.15×2^{674}	$i^2, i \in \mathbb{Z}$	2.46
Ref. [36]	0.0015	-0.0002	-.0004	99.60 %	33.48 %	7.9998	2^{128}	9	0.55
Ref. [37]	0.0013	-0.0009	-0.0023	99.62 %	33.46 %	7.9999	2^{478}	$i, i \in \mathbb{Z}$	2.42
Proposed	0.0024	0.0055	-0.0022	99.62 %	33.42%	7.9998	2^{332}	12	0.25

a bottleneck can occur with respect to resource constraints in the computing device during actual implementation. The proposed method has a decent execution speed, faster than most of the compared methods. The proposed method can decipher the exact original images from the cipher images, while the method given in [36] provides visually similar images but not the exact original images. For the proposed method, the PSNR and SSIM value are ∞ and one, respectively, while for [36], the PSNR is in the range of 25 to 33 and SSIM is in the range of 0.89 to 0.97. The proposed method has the edge over other methods in reducing the iteration of a chaotic system. If $M1 \times N1$ is the size of the image, the proposed method reduces the iteration in the chaotic system by a factor of four by employing a base conversion operation. In contrast, the compared methods iterate for $M1 \times N1$ to generate the chaotic sequence. The keys used for the proposed method is securely shared as an elliptic curve point as given in Section III-C. The keys are safe from the adversary as the elliptic curve discrete logarithmic problem is one of the complicated problems that cannot be solved in a feasible time as of now.

VI. CONCLUSION

This paper proposed a multiple images encryption scheme based on an amplified Sine map. The ASM exhibits complex chaotic behaviour with a more extensive chaotic range and low computational cost. Two different key sets of the ASM is generated by using $SHA384$. A dynamic permutation table is generated for the CST using the first key set of ASM. The CST then performs random byte circular shifts along the horizontal and vertical axes of the combined input image. Again, using the second key set of ASM, a chaotic image is generated whose dimension is equal to that of the input combined image. Bitwise XoR is performed between the CST image and chaotic image to get the cipher image. The experimental analysis and results show the effectiveness of the proposed method against various cryptographic attacks. The performance analysis shows that the proposed algorithm is superior or on par with the other methods under consideration.

REFERENCES

[1] Y. Qobbi, A. Jarjar, M. Essaid, and A. Benazzi, "Image encryption algorithm based on genetic operations and chaotic DNA encoding," *Soft Comput.*, vol. 26, no. 12, pp. 5823–5832, Jun. 2022, doi: 10.1007/S00500-021-06567-7.

[2] S. Huang, L. Huang, S. Cai, X. Xiong, and Y. Liu, "Novel and secure plaintext-related image encryption algorithm based on compressive sensing and tent-sine system," *IET Image Process.*, vol. 16, no. 6, pp. 1544–1557, May 2022, doi: 10.1049/ipr2.12429.

[3] W. H. Alshoura, Z. Zainol, J. S. Teh, M. Alawida, and A. Alabdulatif, "Hybrid SVD-based image watermarking schemes: A review," *IEEE Access*, vol. 9, pp. 32931–32968, 2021, doi: 10.1109/ACCESS.2021.3060861.

[4] X. Wang and Y. Su, "Image encryption based on compressed sensing and DNA encoding," *Signal Process., Image Commun.*, vol. 95, Jul. 2021, Art. no. 116246.

[5] K. M. Singh, L. D. Singh, and T. Tuithung, "Text encryption based on Huffman coding and ElGamal cryptosystem," *Recent Patents Eng.*, vol. 14, pp. 3–8, Sep. 2020.

[6] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7397–7407, Dec. 2018.

[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[8] M. Alawida, A. Samsudin, N. Alajarmeh, J. S. Teh, M. Ahmad, and W. H. Alshoura, "A novel hash function based on a chaotic sponge and DNA sequence," *IEEE Access*, vol. 9, pp. 17882–17897, 2021, doi: 10.1109/ACCESS.2021.3049881.

[9] M. Alawida, J. S. Teh, D. P. Oyinloye, M. Ahmad, and R. S. Alkhawaldeh, "A new hash function based on chaotic maps and deterministic finite state automata," *IEEE Access*, vol. 8, pp. 113163–113174, 2020, doi: 10.1109/ACCESS.2020.3002763.

[10] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Inf. Sci.*, vol. 520, pp. 46–62, May 2020.

[11] A. Mansouri and X. Wang, "A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme," *Inf. Sci.*, vol. 563, pp. 91–110, Jul. 2021.

[12] M. Xu and Z. Tian, "A novel image cipher based on 3D bit matrix and Latin cubes," *Inf. Sci.*, vol. 478, pp. 1–14, Apr. 2018.

[13] Z. Hua, Z. Zhu, Y. Chen, and Y. Li, "Color image encryption using orthogonal Latin squares and a new 2D chaotic system," *Nonlinear Dyn.*, vol. 104, no. 4, pp. 4505–4522, May 2021.

[14] Z. Hua, Y. Chen, H. Bao, and Y. Zhou, "Two-dimensional parametric polynomial chaotic system," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4402–4414, Jul. 2022, doi: 10.1109/TSMC.2021.3096967.

[15] Z. Hua, Y. Zhang, H. Bao, H. Huang, and Y. Zhou, "*n*-dimensional polynomial chaotic system with applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 784–797, Feb. 2022, doi: 10.1109/TCSI.2021.3117865.

[16] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, 2019.

[17] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, no. 3, pp. 131–140, 2019.

[18] M. Zarebnia, H. Pakmanesh, and R. Parvaz, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for grayscale images," *Optik-Int. J. Light Electron. Opt.*, vol. 179, pp. 761–773, Jan. 2019.

[19] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102470.

[20] A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," *Inf. Sci.*, vol. 550, pp. 252–267, Mar. 2021, doi: 10.1016/j.ins.2020.10.031.

[21] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015, doi: 10.1109/TCYB.2014.2363168.

[22] L. Liu, J. Lin, S. Miao, and B. Liu, "A double perturbation method for reducing dynamical degradation of the digital baker map," *Int. J. Bifurcation Chaos*, vol. 27, no. 7, Jun. 2017, Art. no. 1750103.

[23] Y. Wu, Y. Zhou, and L. Bao, "Discrete wheel-switching chaotic system and applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 12, pp. 3469–3477, Dec. 2014.

[24] Y. Deng, H. Hu, and L. Liu, "Feedback control of digital chaotic systems with application to pseudorandom number generator," *Int. J. Mod. Phys. C*, vol. 26, no. 2, Feb. 2015, Art. no. 1550022.

[25] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, Apr. 2014.

[26] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008.

[27] L. Liu and S. Miao, "Delay-introducing method to improve the dynamical degradation of a digital chaotic map," *Inf. Sci.*, vol. 396, pp. 1–13, Aug. 2017.

[28] M. Alawida, A. Samsudin, and J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," *Inf. Sci.*, vol. 512, pp. 1155–1169, Feb. 2020.

[29] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Deterministic chaotic finite-state automata," *Nonlinear Dyn.*, vol. 98, no. 3, pp. 2403–2421, Nov. 2019.

[30] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, Mar. 2020.

[31] X. Wang, Y. Li, and J. Jin, "A new one-dimensional chaotic system with applications in image encryption," *Chaos, Solitons Fractals*, vol. 139, Oct. 2020, Art. no. 110102.

[32] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020.

[33] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.

[34] X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Opt. Laser Technol.*, vol. 141, Sep. 2021, Art. no. 107073, doi: 10.1016/j.optlastec.2021.107073.

[35] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal, "A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations," *IEEE Access*, vol. 8, pp. 123536–123555, 2020, doi: 10.1109/ACCESS.2020.3004536.

[36] A. Gaffar, A. B. Joshi, S. Singh, V. N. Mishra, H. G. Rosales, L. Zhou, A. Dhaka, and L. N. Mishra, "A technique for securing multiple digital images based on 2D linear congruential generator, silver ratio, and Galois field," *IEEE Access*, vol. 9, pp. 96125–96150, 2021, doi: 10.1109/ACCESS.2021.3094129.

[37] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, and X. Chen, "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1535–1551, Apr. 2022, doi: 10.1016/j.jksuci.2022.01.017.

[38] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[39] M. Miller, "Uses of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer-Verlag, 1986, pp. 417–426.

[40] *The USC-SIPI Image Database*. Accessed: May 19, 2020. [Online]. Available: http://sipi.usc.edu/database/

[41] R. Andrew, S. Juan, N. James, S. Miles, and B. Elaine, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MA, USA, Tech. Rep., 2010.

[42] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu.*, vol. 1, pp. 31–38, Apr. 2011.

LAIPHRAKPAM DOLENDRO SINGH (Member, IEEE) received the master's degree from the National Institute of Technology Agartala, India, and the Ph.D. degree from the National Institute of Technology Manipur, India. He is currently an Assistant Professor with the Department of Computer Science and Engineering, National Institute of Technology Silchar, Assam, India. He has published several research papers in reputed journals. He has published two patents. His research interests include cryptography and cryptanalysis. He is a Life Member of Cryptography Research Society of India. URL: http://cs.nits.ac.in/dolendro/.

ROHIT THINGBAIJAM received the B.Tech. degree from the Department of Computer Science and Engineering, National Institute of Technology Manipur, India, in 2019, and the M.Tech. degree from the Department of Computer Science and Engineering, National Institute of Technology Silchar, Assam, India.

KHOIROM MOTILAL SINGH received the B.Tech. and M.Tech. degrees from the Department of Computer Science and Engineering, National Institute of Technology Manipur, India, in 2014 and 2016, respectively, and the Ph.D. degree from the National Institute of Technology Nagaland, India, in 2022. He is currently an Assistant Professor with the Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. He has published one patent.

MOATSUM AL AWIDA received the Ph.D. degree in computer science/cybersecurity (cryptography) from the School of Computer Sciences, Universiti Sains Malaysia, in 2020. He is an Assistant Professor of cybersecurity with Abu Dhabi University. He published more than 25 articles in high impact factor journals. In 2021, he was ranked among the top 2% of all scientists in the world. His research interests include chaotic systems, chaos-based applications, multimedia security, blockchain, cybersecurity, quantum-based cryptography, and cryptography. He has served as a Referee for some renowned journals, such as IEEE TRANSACTIONS ON CYBERNETICS, *Signal Processing*, *Information Sciences*, *Journal of Information Security and Applications*, IEEE ACCESS, *Wireless Personal Communications*, the *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, *Optik*, *Optics and Laser Technology*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Chaos, Solitons and Fractals*, *Physica A: Statistical Mechanics and its Applications*, and *Signal Processing: Image Communication*.