A Novel Image Encryption using Memetic Differential Expansion based Modified Logistic Chaotic Map

Anvita Gupta[1], Dilbag Singh[2], Manjit Kaur[3]
Computer Science and Engineering,
Apex Institute of Technology
Chandigarh University
Gharuan, Punjab, India

***Abstract*—Under this paper, the primary conditions of a modified logistic chaotic map are created with the help of memetic differential expansion. In the beginning, the color image is broken down into different channels like red, blue and green. Then the modified logistic chaotic map essential variables are enhanced with the execution of memetic differential expansion. The strength operation is employed by the association coefficient and Entropy function. The private keys are produced by the modified logistic chaotic map. The encoded image is acquired with a combination of different encoded color channels. The memetic differential expansion builds on image encryption and the previous image encryption techniques build with the different standard images play a vital role in carrying out the larger experiments. The evaluation of the outcome of the proposed technique gives better security and efficiency in contrast to all the previously implemented image encryption techniques.**

Keywords*—Image encryption; modified logistic chaotic map; memetic differential expansion

I. Introduction

The reliability of contents which is available on the digital platform is becoming the most exigent point with the development of many software applications and latest technologies [1]. In several operations like military, remote sensing, imaging in medical, etc. images plays the major part [2].

Hongjun et al. implement the stream-encoded approach that consists of single way keys and vigorous chaotic maps. This approach ensures a high level of security and upgraded the active breakdown. The piecing chaotic map is used to create the artificial random key stream series [3].

Yaobin et al. implement the image encryption scheme based on the baker map in three dimensional that results in high security with speedy image encryption technique [4], [5].

To have preferable image encryption outcomes, Chaotic maps are considerably used [6]. Usama et al. utilized several chaotic maps. Some of them are Sine, Tent, Logistic, Cubic, etc. to encode the images [7].

Guodong et al. proposed an encryption technique with the help of Arnold map that consists of two divisions, i.e., arrangement and distribution. Initially, an entire circular operation is utilized in the arrangement division that considerably minimizes the association linking the adjoining pixels. Afterward, at the distribution stage dual diffusion operations that include constructive and contradictory module are used along with novel production of keystream [8], [9].

Ruisong et al. proposed an approach of image encryption that has inbuilt features of arrangement and distribution technique. Initially, for the arrangement of image pixel place, an un-specialized Arnold map in the arrangement phase is used to create a single chaotic path to receive dual index sequences. While in the distribution phase, un-specialized Arnold map along with un-specialized Bernoulli fetch map are engaged to capitulate dual imitation random gray points order for a dual-process distribution of gray points [10], [11].

Kwok et al. implement the high potential propagation technique that uses elementary list lookup along with exchange approach as a thin-mass substitute of one-dimensional chaotic map repetition [12].

Chong et al. proposed an approach that is built on a bit size arrangement technique to have reliable and well-organized image encryption. This approach launch the remarkable diffusion consequences in the arrangement process along with dual division bit-size jumble algorithm that perceives by both chaotic order organized algorithm and Arnold cat map [13].
Yong et al. implement the quick image cipher technique which is the combination of arrangement and distribution algorithm. In this approach, the initial image is broken down into the number of pixels. Afterward, fourth dimension chaos is used to rearrange the pieces and also to alter the pixel worth [14].

Fabian et al. implement a method to encode-decode the color effective occurrence with the help of the original optical substitute. Then the three fundamental chromatic medium which creates the initial parameter gets split. Afterward, the individual medium is executed with the help of 4f encryption procedure and theta moderation pertain to every encoded frame in each medium [15].

Sahar et al. implement an approach named Coupled Nonlinear Chaotic Map (CNCM) and image encryption scheme build in chaos to encode the color images with the help of the implemented approach [16], [17].

Madhusudan et al. implement the technique for color image encryption with the help of fractional Fourier transform [18].

Chong et al. proposed an improved version of the distribution plan to encourage the effectiveness of the extensively scrutinize arrangement-distribution kind image encryption [19].

Licheng et al. proposed the memetic approach which proves more powerful in contrast with the dual state of the technique image section approach that further consist of effective graph build technique and spectral group build algorithm and also defeat its hereditary type, fuzzy c-mean technique and also the k-mean approach is dividing many of the problems [20].

Kumar et al. implement the elliptic curve cryptography along with DNA to encode the images [21].

There are several image encryption approaches which are meta-heuristic in nature such as Genetic Algorithm (GA) [22], [23], [24], Many Objective Non-Dominated Sorting Genetic Algorithm build on Reinforcement learning (MNSGA-RL) [25], Ant Colony Optimization (ACO) [26], differential evolution [27] and Dynamic Harmony Search(DHS) [28]. Although these all are having bad computational speed.

Chunyan et al. proposed a modified logistic chaotic map to improve the security in the case of a single logistic map [29]. Wai et al. implement the modified chaotic cryptographic technique which executes on the logistic map. The result proves the diffusion of the encoded text compliment and to minimize the execution time [30].

So in this research Paper, modified memetic differential expansion is used for upgrading the first situation recommend by the modified logistic chaotic map. This paper implements the image encryption technique by evaluating the modified logistic chaotic map and memetic differential expansion.

Firstly, the color image is split among three different channels like red, blue and green. Then, the modified logistic chaotic map is used to create different secret keys to encode the channels. The memetic differential expansion modifies the input of the modified logistic chaotic map. Afterward, all distinct encoded channels are combined to get the final encoded image.

The rest of the portion of this paper explains the "Preliminaries" part that briefly tells about the modified logistic chaotic map and memetic differential expansion. The implemented approach of image encryption is discussed under the "Proposed Technique" section. The section "Evaluation of Performance" explores the examination of the implemented approach. The conclusion part describes in the section "Conclusion".

II. Preliminaries

This section briefly explains the modified logistic chaotic map and memetic differential expansion.

A. Modified Logistic Chaotic Map

Modified Logistic Map is represented by the expression which is given below:

$$y_{i+1} = \frac{(2\beta) - y_i^2}{\beta} \tag{1}$$

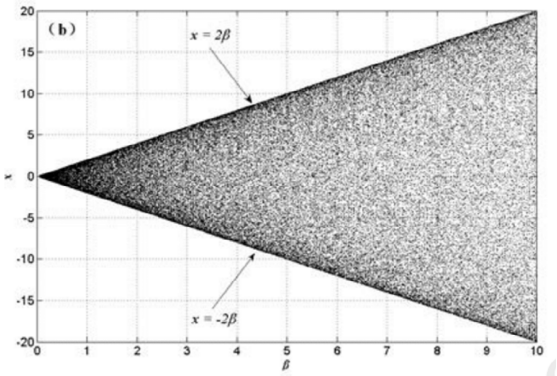

Fig. 1. Diagram for the bifurcation

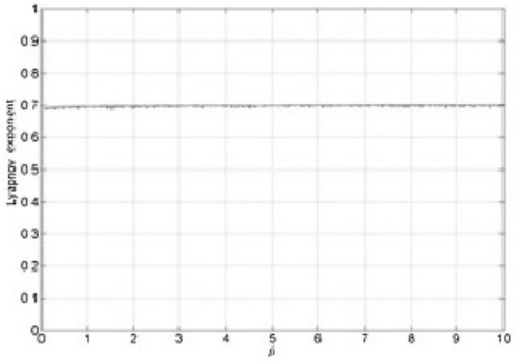

Fig. 2. Lyapunov value spectrum

β is the function and y_i is the primary value of the operation. As soon as the β value is changed in the above equation 1, the complete mapping will execute along with the occurrence of continual chaos and static Lyapunov Value with the correlating continual function where the range of the complete mapping is given by range $\in$ [-2β, 2β] [29].

Fig. 1 and Fig. 2 respectively represents the diagram of Bifurcation and Lyapunov Value Spectrum of the given equation. The essential part along with the mapping range will lead to infinity when the static chaotic indication generator builds on the modified Logistic map is put in the communication area. The Modified logistic chaotic map is used as an artificial random series generator in the area of image encryption.

B. Memetic Differential Expansion

Jia et al. in 2011 implement the memetic differential expansion which is built on confined chaotic explore [31]. There are several benefits of this technique over the normal differential expansion. The first advantage is that the functions of differential expansion such as Scaling element (E) and traverse rate (TR) which are nearly link along with convergence execution are easily managed by this technique. The stability between the Community variety and convergence rate is created by it. Another advantage is, as soon as the technique is converted into an inactive mode in community exploration, then the differential expansion becomes familiar for worldwide development. To increase the development production in community exploration

the memetic differential expansion utilizes the chaotic process. To reduce the implementation time, the purified parameters apply to the Chaotic community exploration (CCE). The steps involved in the memetic differential expansion are given below:

1) **Preparatory:** With the help of normal distribution, the primary community is created that includes the values for random responses. The strength of every response of the community is evaluated.
2) **Alteration:** Three randomly chosen response from the community is used to create alteration responses.
3) **Traverse:** The test response is implemented with the combination of estimated response and alteration response. Based on the traverse rate, the values of test responses are picked from the estimated response and alteration response.
4) **Selecting the test response:** The test response strength is generated and compare it with the estimated response. It will go for the further process only if it has better strength in test response. Else, the further process is executed by using the previous responses.
5) **Chaotic Community Exploration:** To clarify the responses, Community exploration is executed on the estimated response with the help of the chaotic process. The exploration ability of differential expansion is increased and also prevents it from the problem of untimely convergence.
6) **Ending State:** If ending state is fulfilled, the process ends. Else, it will again start executing from the Steps (ii)-(v).

III. Proposed Technique

A. Simulation

The considerable analysis of old techniques designates that most of the old image encryption approaches encounter the loss either in portable keyspace or their beginning situations may be obtained physically. The private key is responsible for the robustness of the encryption technique. Hence, it is obligatory to choose proper starting parameters because they are the reason for the generation of the private key. By stimulating all this certainty, a better encryption technique is proposed in the domain of images. Under this technique, private keys are created by the memetic differential expansion build on a modified logistic chaotic map for the encryption procedure. The encryption and decryption procedure of the implemented encryption technique is explained in the successive sections.

B. Encryption Procedure

The encryption procedure of the implemented technique is shown in Fig. 3. Firstly, a color image is divided into different mediums such as red, blue and green. The modified logistic chaotic map builds on the memetic differential expansion is used to create the private keys to encode the mediums. After that an encrypted image is created which is the result of the combination of all encoded mediums.

Step 1: Initially, a color image (M_{ic}) having j columns and h rows.

Step 2: Divide M_{ic} in among different color mediums such as red (C_r), blue (C_b) and green (C_g) .

Step 3: With the help of the modified logistic chaotic map, private keys are created i.e., q, u, and t. The values which are required by the modified logistic chaotic map is enhanced with the utilization of memetic differential expansion. The size of private keys i.e., q, u, and t is similar to the size of mediums.

Step 3.1 Strength Parameter: The strength parameter which is acquired from the memetic differential expansion is analyzed using the association coefficients and entropy. Every pixel of an encoded image has a similar chance of occurrence if the outcome of entropy is intense [32]. The encoded image should have a minimum value as possible in the case of association [33]. Hence, the major goal of memetic differential expansion is to boost the entropy and reduce the association coefficient of an encoded image.

The strength parameter (s) is evaluated as:

$$s(a_1, a_2) \tag{2}$$

where,

$$a_1 = -\sum_{n=0}^{2^m-1} (Z(p_n) \times log_2 Z(p_n)), \quad s.t. \;\; 7.9 < a_1 \tag{3}$$

and

$$a_2 = \frac{\sum_{n=1}^{T} (b_n - H(b))(d_n - H(d))}{\sqrt{\sum_{n=1}^{T}(b_n - H(b))^2}.\sqrt{\sum_{n=1}^{T}(d_n - H(d))^2}}, \tag{4}$$

where s.t. $a_2 \in$ {-1,0.5}

Entropy (a_1) and association coefficient (a_2) is represented in Eqs. (3) and (4) respectively. The appearance of pixel p_n is denoted by $Z(p_n)$. The quantity of pixel pairs (b_n, d_n) is indicated by the T . The mean of b_n and d_n is denoted by $H(b)$ and $H(d)$, respectively. The amount of gray levels is represented by m.

Step 3.2 Preparatory: The memetic differential expansion has primary responses which are explained as:

$$R_j^n = [r_{j1}^n, r_{j2}^n, \ldots, r_{j8}^n], \quad j \in \{1, 2, \ldots, C_r\} \tag{5}$$

Here, the community size is represented by the C_r. Under the n production the k^{th} variable from j^{th} response is denoted by r_{jk}.

With the help of normal distribution, every response is created randomly in this process. 8 denotes the size of every random response (R_j^n). The end variable serves as the encryption element (η) and the private keys are generated by the initial different variables of every P_j^n which is allocated to the modified logistic chaotic map. Inside the scope of $[0, 1]$, each R_j^n choose scaling element (E) and traverse rate (TR) separately. Eq. (2) is utilized to analyze the strength parameter of an encoded image along with random responses

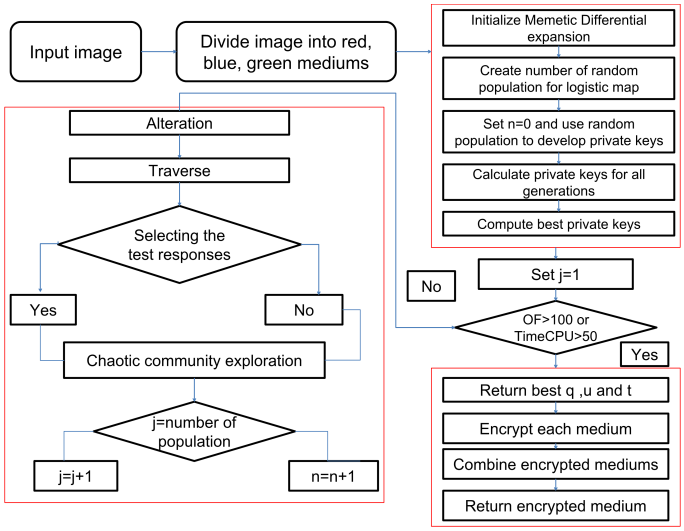

Fig. 3. Flowchart of a proposed image encryption approach

R_j^n.

Step 3.3 Alteration: By aggregating the variation of dual responses into the other one, an alteration response (A_j^n) is created by memetic differential expansion.

$$A_j^n = R_{l_3}^n + E^f \cdot (R_{l_2}^{nf} - R_{l_1}^{nf}) \\ l_1, l_2, l_3 \in \{1, 2, \ldots, C_r\}, \quad f \in \{1, 2\} \tag{6}$$

Here, Randomly picked responses against the similar community (however, $l_1 \neq l_2 \neq l_3 \neq i$) is represented by l_1, l_2, and l_3. The amount of differential response engaged in alteration procedure is denoted by f . Scaling element is represent by E and restricted to range $[0, 1]$.

Step 3.4 Traverse: The combination of alteration response (A_j^n) along with its primary response (R_j^n) is lead to the creation of test response (i.e., P_j^n). The procedure of picking the variables of P_j^n is given as:

$$p_{jk}^n = \begin{cases} a_{jk}^n, & rand(k) \leq TR, \\ r_{jk}^n, & rand(k) > TR. \end{cases} \tag{7}$$

where, Variables of P_j^n and A_j^n is represented by the p_{jk}^n and a_{jk}^n, respectively.
$k \in \{1, 2, \ldots, 8\}$ and Traverse rate is indicated by TR .

Step 3.5 Selecting the test responses: To acquire the private keys, a Modified logistic chaotic map is allocated by the variables of every P_j^n. Encrypted image C_r is created by the utilization of these private keys. The comparison is done under this procedure between the strength of the encoded image which is created through P_j^n and the previous R_j^n. Afterward, the response having the preferable strength will go for further execution.

$$R_j^{n+1} = \begin{cases} P_j^n, & \text{if } f(P_j^n) > f(R_j^n), \\ R_j^n, & \text{otherwise.} \end{cases} \tag{8}$$

Step 3.6 Chaotic community exploration: Chaotic community Exploration (CCE) is used to further clarify the acquired responses i.e., R_j^n. Evaluation of CCE is done as follows:

$$R_j^{'(n)} = (1 - \beta) R_j^n + \beta \gamma_w \tag{9}$$

CCE creates the new response of R_j^n which is denoted by $R_j^{'(n)}$. The diminishing scale is represented by β and is computed as :

$$\beta = 1 - \left| \frac{OFs - 1}{OFs} \right|^{\lambda} \tag{10}$$

where the latest operation estimation is denoted by OFs. λ is used to manage the diminishing rate. Diminishing rate is inversely dependent on the λ, i.e. if the λ is low then the value for diminishing rate is high. γ_w is calculated as given below:

$$\gamma_w = U + \gamma_k^{\nu} \cdot (V - U), \tag{11}$$

Here, the exploration space of R_j is denoted by $[U, V]$. Modified logistic Chaotic map is used to acquire the γ_k^{ν}. The steps for estimation of Modified logistic Chaotic map is given below:

$$\gamma_k^{\nu+1} = \mu \gamma_k^{\nu} (1 - \gamma_k^{\nu}), \quad \nu = 1, 2, \ldots; \quad \gamma_k \in (0, 1), \tag{12}$$

Here, $\gamma_k \neq 0.25, 0.5$, and 0.75 and under the ν^{th} creation, the k^{th} chaotic variable is represent by γ_k^{ν}. The bifurcation standard variable is denoted by μ.

Step 3.7 Ending State: To end the procedure, the dual constraints, i.e., operation estimation and CPU measure are taken into account. The operation estimation gives better appropriate outcomes if its value is at an extreme point. Although, in a few situations, the CPU takes much more time. Therefore, it is the restriction in the technique. Hence, the Ending state is implemented to end the technique which is given as follows:

$$EndingState = \begin{cases} 1, & OF > 100, \\ 1, & Time_{CPU} > 50sec, \\ 0, & otherwise. \end{cases} \tag{13}$$

where the entire evaluation time is taken by the memetic differential expansion so far is denoted by the $Time_{CPU}$.
Steps 3.3 - 3.7 are executed again only if the ending state is not fulfilled. Else, it gives the optimal variable.

Step 4: The mediums C_r', C_b', and C_g' are encrypted by using the encryption element (η) and different private keys,

i.e., q_n, u_n, and t_n (where $n = \{1, 2, \ldots, h \times j\}$) which are acquire through memetic differential expansion.

$$E_R = \mod(\eta \times C'_r + (1-\eta) \times q, p_h) \quad (14)$$

$$E_B = \mod(\eta \times C'_b + (1-\eta) \times u, p_h) \quad (15)$$

$$E_G = \mod(\eta \times C'_g + (1-\eta) \times t, p_h) \quad (16)$$

where, the encoded red, blue and green medium is denoted by E_R, E_G and E_B, respectively. The top pixel of M_{ic} is represented by p_h .

Step 5: In order to estimate the encrypted image (I_{ec}) the encoded mediums E_R, E_B, and E_G are merged all together.

$$I_{ec} = cat(E_R, E_B, E_G) \quad (17)$$

C. Decryption Procedure

The identical private keys (i.e., q, u, and t) and similar encryption element (η) are requisite in order to decrypt the encrypted image. Consequently, the receiver is required to communicate with the tuned variables.

Step 1: I_{ec} is divided among different encrypted color mediums. Red (E_R), green (E_G) and blue (E_B) are the required encrypted mediums.

Step 2: The tunned variables are used to modified logistic chaotic map in order to create the private keys, i.e., q, u, and t .

Step 3: Decryption medium is acquire as follows by applying the q, u, t, and η on every encrypted medium.

$$C'_r = (E_R - (1-\eta) \times q)/\eta \quad (18)$$

$$C'_b = (E_B - (1-\eta) \times u)/\eta \quad (19)$$

$$C'_g = (E_G - (1-\eta) \times t)/\eta \quad (20)$$

where, decrypted color mediums are denoted by C'_r, C'_b, and C'_g .

Step 4: With the combination of C_r, C_b, and C_g mediums, the required decrypted image (I_{dc}) is derived.

$$I_{dc} = cat(C_r, C_b, C_g) \quad (21)$$

IV. Evaluation of Performance

Experiments are carried out on MATLAB software, Intel Core 2.4 GHz $i7$ Processor having RAM 32 GB to estimate the usefulness of the implemented technique. With the 256 × 256 size, different standard color images are extracted [34].

The original color images are represented in Fig. 4 (a)-(e). The images which are the result of the encryption procedure of the proposed technique are designate in Fig. 4 (f)-(j). The images which are created through the decryption procedure of the implemented approach are shown in Fig. 4 (k)-(o). The image which is generated by the decryption procedure and original image are similar. Hence, the remarkable visual standard is achieved by the proposed technique.

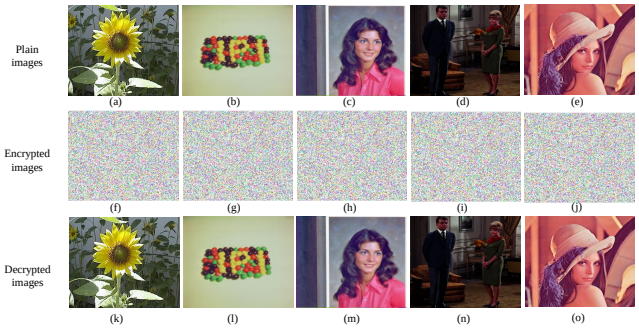

Fig. 4. Evaluation of the performance of implemented technique: (a)-(e) original images, (f)-(j) Image obtained from encryption process, and (k)-(o) Image obtained through decryption process.

TABLE I. Differentiation on the basis of entropy (in bit/pixel)

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	7.9860	7.9837	7.9864	7.9850	7.9871
NL *I.E.* [40]	7.9695	7.9765	7.9793	7.9756	7.9799
LV *I.E.* [41]	7.9765	7.9788	7.9798	7.9755	7.9807
ECB *I.E.* [38]	7.9754	7.9755	7.9775	7.9788	7.9786
SPN C *I.E.* [36]	7.9971	7.9983	7.9984	7.9988	7.9470
FMM ILM *I.E.* [25]	7.9980	7.9873	7.9979	7.9983	7.9988
DE *I.E.* [27]	7.9982	7.9977	7.9986	7.9985	7.9994
Proposed technique	**7.9992**	**7.9991**	**7.9995**	**7.9995**	**7.9997**

A. Security Evaluation

1) Entropy: To examine the amount of randomness, Entropy plays a very vital role. The execution differentiation based on entropy between the old image encryption technique and the implemented technique is represented in Table I. The table predicts that the values which are very near to the perfect parameters (i.e. 8) are given by the proposed technique. On the contrast of other techniques, the implemented approach has the highest entropy.

2) Bar Graph Evaluation: The strength of every pixel is represented by the bar graph. The bar graph helps in escaping the analytical data [1], [35]. Therefore, the bar graph of an encrypted image should be constantly scattered. The bar graph of encoded Sunflower image and different mediums such as red, blue and green is represented in Fig. 5. The bar graph of the encrypted mediums are quite dissimilar to the bar graph of the original mediums is easily predicted through Fig. 5. It is observed that the bar graph of the encoded mediums is constantly scattered. Hence, the implemented technique is proved more secured against all analytical issues.

3) Association coefficient: The analytical data is divulged through the connection between the image pixels. The plain image pixels are correlated with each other. Hence, it is essential to have encrypted image pixels freely associated with each other. The connection between the encrypted image pixels of an implemented technique is calculated by the association coefficient. Eq. (4) is utilized to evaluate the association in different ways, i.e., horizontally, vertically and diagonally.

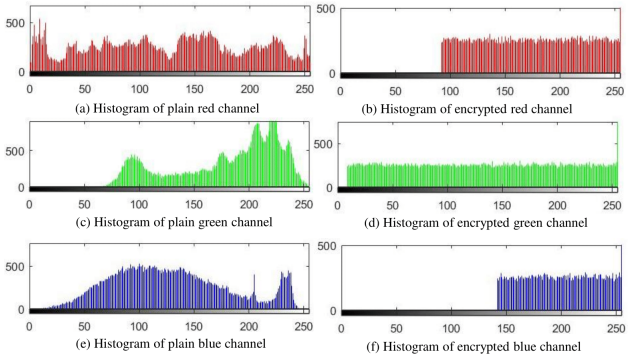

Fig. 5. Sunflower image: Bar Graph of (a) original red medium, (b) encoded red medium, (c) original green medium, (d) encoded green medium, (e)original blue medium, and (f) encrypted blue medium.

TABLE II. DIFFERENTIATION BUILD ON HORIZONTAL ASSOCIATION

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	0.0145	0.0103	0.0056	0.0134	**-0.0129**
NL *I.E.* [40]	0.0070	0.0038	0.0142	-0.0066	0.0171
LV *I.E.* [41]	0.0189	0.0109	0.0131	**-0.0152**	0.0027
ECB *I.E.* [38]	0.0120	0.0208	0.0178	0.0140	0.0082
SPN C *I.E.* [36]	0.0044	0.0134	0.0112	0.0062	0.0057
FMM ILM *I.E.* [25]	0.0010	0.0035	0.0036	0.0004	0.0029
DE *I.E.* [27]	0.0010	0.0014	0.0046	0.0043	0.0020
Proposed technique	**0.0008**	**0.0010**	**0.0008**	**-0.0138**	**-0.0122**

Horizontal, vertical and diagonal association differentiation among the old image encryption technique and proposed approach is portrayed on the Tables II, III, and IV, respectively.

By the review of the mean of the different mediums, the horizontal, vertical and diagonal association of the implemented technique is evaluated under these tables. It is observed from the tables that the implemented technique has the least association in almost every instance. Hence, the implemented technique proves efficient against analytical issues.

Association coefficient of Red medium of original Sunflower image is represented by Fig. 6(a)-(c).

TABLE III. DIFFERENTIATION BUILD ON DIAGONAL ASSOCIATION

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	0.0238	0.0025	0.0064	0.0022	**-0.0269**
NL *I.E.* [40]	0.0078	-0.0021	0.0088	0.0082	0.0243
LV *I.E.* [41]	0.0048	**-0.0075**	0.0072	0.0062	-0.0202
ECB *I.E.* [38]	0.0248	0.0262	0.0082	0.0022	0.0202
SPN C *I.E.* [36]	0.0269	0.0200	0.0220	0.0207	0.0288
FMM ILM *I.E.* [25]	0.0037	0.0027	-0.0003	0.0037	0.0008
DE *I.E.* [27]	0.0047	0.0062	0.0084	0.0068	0.0043
Proposed Technique	**0.0035**	**-0.0076**	**-0.0009**	**0.00011**	**0.0008**

TABLE IV. DIFFERENTIATION BUILD ON VERTICAL ASSOCIATION

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	0.0058	0.0128	0.0038	0.0024	0.0151
NL *I.E.* [40]	0.0101	0.0030	0.0100	0.0002	0.0156
LV *I.E.* [41]	0.0130	0.0121	0.0103	0.0150	**-0.0015**
ECB *I.E.* [38]	0.0120	0.0119	0.0123	0.0104	0.0133
SPN C *I.E.* [36]	0.0125	0.0100	0.0149	0.0090	0.0154
FMM ILM *I.E.* [25]	0.0103	0.0053	0.0028	0.0026	0.0010
DE *I.E.* [27]	0.0126	0.0012	0.0110	0.0130	0.0196
Proposed Technique	**0.0053**	**-0.0040**	**-0.0001**	**-0.0012**	**-0.0016**

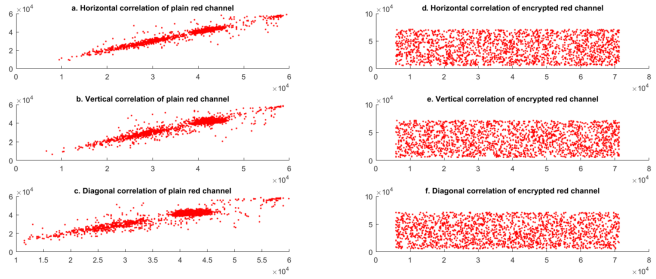

Fig. 6. Sunflower Red medium image before encryption: (a) Horizontal, (b) Vertical, and (c) Diagonal Association (d) Sunflower Red medium image after encryption Horizontal, (e) Vertical, and (f) Diagonal Association

Association coefficient of Red medium of encoded Sunflower image is indicated by Fig. 6(d)-(f). It is observed that the final encoded image is completely random in creation.

4) Comparison evaluation: With the help of Comparison evaluation, the consideration regarding the least changes of the implemented technique can be computed [36]. A very little change is made by the assailant in the plain image. The single private key is used to encode the plain and altered image. Hence, the connection between the plain image and the altered image is found by the assailant. The evaluation of the different attacks is done by using the parameters Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI).
NPCR can be computed as given below [36]:

$$NPCR = \frac{\sum_{n=j}^{n=h}\sum_{n=1}^{n=j} N_{zz}(n,k)}{h \times j} \times 100 \tag{22}$$

where,

$$N_{zz}(n,k) = \begin{cases} 0 & \text{if} \quad I_{ec}(n,k) = I'_{ec}(n,k) \\ 1 & \text{if} \quad I_{ec}(n,k) \neq I'_{ec}(n,k) \end{cases} \tag{23}$$

UACI can be calculated as given below [36]:

$$UACI = \frac{\sum_{n=1}^{n=h}\sum_{n=1}^{n=j} |I_{ec}(n,k) - I'_{ec}(n,k)|}{255 \times h \times j} \times 100 \tag{24}$$

where, the encoded image having the variance of a single-pixel is represented by $I_{ec}(n,k)$ and $I'_{ec}(n,k)$, respectively. To avoid the different attacks, the highest value of NPCR and UACI are required.

The responsiveness of the implemented technique is estimated with the help of Sunflower image. Based on NPCR and UACI parameters, the execution differentiation among the implemented technique and old encryption technique, respectively is presented under Tables V and VI. The table outcome

TABLE V. DIFFERENTIATION BUILD UPON NPCR (IN %)

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	99.5648	99.5720	99.5769	99.5973	99.5873
NL *I.E.* [40]	99.6189	99.5488	99.5990	99.6372	99.6490
LV *I.E.* [41]	99.4689	99.5667	99.4468	99.6009	99.6010
ECB *I.E.* [38]	99.5266	99.5289	99.5492	99.5496	99.4593
SPN C *I.E.* [36]	99.5089	99.5118	99.5378	99.5460	99.6099
FMM ILM *I.E.* [25]	99.5893	99.5972	99.6347	99.6408	99.5391
DE *I.E.* [27]	99.5170	99.5385	99.5677	99.5494	99.5475
Proposed Technique	**99.63022**	**99.6563**	**99.6734**	**99.6486**	**99.6688**

TABLE VI. DIFFERENTIATION BUILD UPON UACI (IN %)

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	33.3675	33.4872	33.5670	33.5870	33.6094
NL *I.E.* [40]	33.4873	33.4926	33.4538	33.5742	33.3992
LV *I.E.* [41]	33.4304	33.4301	33.4405	33.4506	33.4721
ECB *I.E.* [38]	33.3723	33.4962	33.4908	33.4871	33.4860
SPN C *I.E.* [36]	33.2996	33.2987	33.3773	33.3850	33.3769
FMM ILM *I.E.* [25]	33.3968	33.4559	33.4973	33.4968	33.4984
DE *I.E.* [27]	33.4632	33.4511	33.4794	33.5207	33.4787
Proposed Technique	**33.5826**	**33.5877**	**33.5852**	**33.5894**	**33.6657**

predicts that the implemented technique has better NPCR and UACI parameters in contrast to the existing techniques. Hence, the implemented technique has far better potential to avoid different attacks.

5) Private key scope: To make the brute-force attacks impossible, a huge key expansion is significant for image encryption. The primary parameters of a modified logistic chaotic map that is created from the memetic differential expansion are considered as the private keys under this implemented technique. Different keys are stated as q_0, u_0, t_0, s_1, s_2, s_3, and α. If accuracy is fixed to 10^{-14} then the key space of the implemented technique is given by 10^{98}. To withstand the Brute-force attacks, the key space is considered as sufficient.

6) Private key responsiveness: The implemented technique responsiveness against the private keys has been estimated. With the help of modified logistic chaotic map, the private keys, i.e., q, u, and t are originated by using the primary values ,i.e., q'_0, u'_0, t'_0, s_1, s_2, s_3, and α. With the help of q, u, and t , respectively, the different mediums of M_{ic} such as C_r, C_g, and C_b are encoded. To get the encrypted image, i.e., I_{ec} as output, the encrypted mediums are merged together. The encrypted image utilize the real private keys are represented in Fig. 7(b).

The distinct private keys such as q', u', and t' are originated with the modest change in the beginning variable, i.e., q_0. Afterward, the original image mediums such as C_r, C_g, and C_b are encrypted with the support of the new private keys. With the integration of different encrypted mediums, an encrypted image, i.e., $I^{'}_{ec}$ is received. The encrypted image produce with the help of new private keys is shown in Fig. 7(c). The dissimilarity among the different encrypted images, i.e., I_{ec} and I'_{ec} that has very less differentiation in primary parameters is represented in Fig. 7(d). Fig. 7(e) indicates the decrypted image of Fig. 7(b) with the help of real private keys. The decrypted image which is the outcome of executing the new private keys on the initial encrypted image is indicated in Fig. 7(f). It is observed from the outcome that even if there is very little change in starting parameters of the private keys, the recuperate of the initial image is not possible.

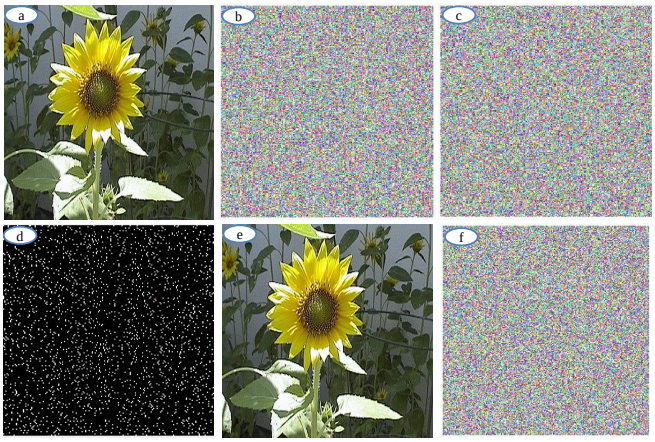

Fig. 7. Private Key Responsiveness: (a) Original Sunflower image, (b) Private keys generate Encrypted image, (c) New Private keys created Encrypted image, (d) Differentiation among (b) and (c), (e) decrypted image create using an initial key, and (f) decrypted image generate using new keys.

TABLE VII. DIFFERENTIATION AMONG I_{ec} AND I'_{ec} IMAGES (IN %)

	Sunflower	Beans	Female	Duplet	Lena
Differentiation	99.9592	99.9798	99.9854	99.9893	99.9984

Table VII represents the Differentiation among I_{ec} and I'_{ec}. It is perceived that the very little changes in the original parameters can result in entirely distinct encrypted images.

7) Peak Signal to Noise Ratio: The productiveness of the encryption approach is used to execute the Peak Signal to Noise Ratio (PSNR) [37]. As known in prior, highest the value of PSNR results in the efficient standard of decrypted images.

The evaluation of the implemented technique and the previous technique of image encryption is represented in Table VIII. It is observed that the Implemented approach results in better PSNR value in contrast to other techniques.

V. CONCLUSION

The issue of the variable tuning linking with the logistic chaotic map is defeated by the implemented technique. The implemented technique used the memetic differential expansion to solve this issue. Based on the distinct popular color images, the virtue of the implemented technique has been evaluated. The average enhancement is perceived in the implemented technique while comparing the outcome of the implemented technique with the existing approach. The proposed technique

TABLE VIII. RELATIVE STUDY WITH THE HELP OF PSNR (IN DB)

Technique	Sunflower	Beans	Female	Duplet	Lena
LW *I.E.* [39]	63.6335	63.4405	63.2536	63.5511	63.3984
NL *I.E.* [40]	67.6652	67.1711	67.2739	68.2491	68.0399
LV *I.E.* [41]	70.7811	71.6982	70.7658	73.7985	72.7544
ECB *I.E.* [38]	68.2811	68.9492	68.2898	68.7765	68.2988
SPN C *I.E.* [36]	69.2768	69.8972	69.9097	69.0676	69.3988
FMM ILM *I.E.* [25]	74.6476	74.2967	74.9758	74.7876	74.8960
DE *I.E.* [27]	78.6695	78.2587	78.4973	78.1284	77.6582
Proposed Technique	**80.6996**	**86.8789**	**83.4994**	**82.2999**	**87.7763**

has better Entropy, NPCR, UACI and PSNR values , i.e. 0.32%, 0.20%, 0.22%, and 30.5% (dB), respectively. The implemented technique has decreased the association coefficient by 2.9%. The outcome divulges that implemented technique gives better security and effectiveness of images in contrast to all other existing techniques.

REFERENCES

[1] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," Neural Computing and Applications, vol. 26, no. 5, pp. 1137–1148, 2014.

[2] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," Neural Computing and Applications, vol. 30, no. 12, pp. 3847–3857, 2017.

[3] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," Computers and Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, 2010.

[4] Y. Mao, G. Chen, and S. Lian, "A Novel Fast Image Encryption Scheme Based On 3D Chaotic Baker Maps," International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3613–3624, 2004.

[5] F. Han, X. Yu, and S. Han, "Improved Baker Map for Image Encryption," 2006 1st International Symposium on Systems and Control in Aerospace and Astronautics.

[6] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," Signal Processing: Image Communication, vol. 52, pp. 6–19, 2017.

[7] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," Computers and Mathematics with Applications, vol. 60, no. 2, pp. 326–337, 2010.

[8] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," Nonlinear Dynamics, vol. 69, no. 4, pp. 2079–2087, 2012.

[9] Y.-Q. Zhang and X.-Y. Wang, "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation," Nonlinear Dynamics, vol. 77, no. 3, pp. 687–698, 2014.

[10] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," Optics Communications, vol. 284, no. 22, pp. 5290–5298, 2011.

[11] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," Optics and Lasers in Engineering, vol. 90, pp. 146–154, 2017.

[12] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An efficient diffusion approach for chaos-based image encryption," Chaos, Solitons and Fractals, vol. 41, no. 5, pp. 2652–2663, 2009.

[13] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," Optics Communications, vol. 284, no. 23, pp. 5415–5423, 2011.

[14] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," Applied Soft Computing, vol. 11, no. 1, pp. 514–522, 2011.

[15] F. Mosso, M. Tebaldi, J. F. Barrera, N. Bolognini, and R. Torroba, "Pure optical dynamical color encryption," Optics Express, vol. 19, no. 15, p. 13779, 2011.

[16] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on Coupled Nonlinear Chaotic Map," Chaos, Solitons and Fractals, vol. 42, no. 3, pp. 1745–1754, 2009.

[17] A. S. Pikovsky and P. Grassberger, "Symmetry breaking bifurcation for coupled chaotic attractors," Journal of Physics A: Mathematical and General, vol. 24, no. 19, pp. 4587–4597, 1991.

[18] M. Joshi, Chandrashakher, and K. Singh, "Color image encryption and decryption using fractional Fourier transform," Optics Communications, vol. 279, no. 1, pp. 35–42, 2007.

[19] C. Fu, J.-J. Chen, H. Zou, W.-H. Meng, Y.-F. Zhan, and Y.-W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," Optics Express, vol. 20, no. 3, p. 2363, 2012.

[20] L. Jiao, M. Gong, S. Wang, B. Hou, Z. Zheng, and Q. Wu, "Natural and Remote Sensing Image Segmentation Using Memetic Computing," IEEE Computational Intelligence Magazine, vol. 5, no. 2, pp. 78–91, 2010.

[21] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," Signal Processing, vol. 125, pp. 187–202, 2016.

[22] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," AEU - International Journal of Electronics and Communications, vol. 66, no. 10, pp. 806–816, 2012.

[23] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," Optics and Lasers in Engineering, vol. 56, pp. 83–93, 2014.

[24] X. Zhang, X. Wang, and Y. Cheng, "Image Encryption Based on a Genetic Algorithm and a Chaotic System," IEICE Transactions on Communications, vol. E98.B, no. 5, pp. 824–833, 2015.

[25] M. Kaur and V. Kumar, "Fourier–Mellin moment-based intertwining map for image encryption," Modern Physics Letters B, vol. 32, no. 09, p. 1850115, 2018.

[26] N. Sreelaja and G. V. Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation," Applied Soft Computing, vol. 12, no. 9, pp. 2879–2895, 2012.

[27] M. Kaur and V. Kumar, "Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain," IET Image Processing, vol. 12, no. 7, pp. 1273–1283, 2018.

[28] K. M. Talarposhti and M. K. Jamei, "A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map," Optics and Lasers in Engineering, vol. 81, pp. 21–34, 2016.

[29] C. Han, "An image encryption algorithm based on modified logistic chaotic map," Optik, vol. 181, pp. 779–785, 2019.

[30] W.-K. Wong, L.-P. Lee, and K.-W. Wong, "A modified chaotic cryptographic method," Computer Physics Communications, vol. 138, no. 3, pp. 234–236, 2001.

[31] D. Jia, G. Zheng, and M. K. Khan, "An effective memetic differential evolution algorithm based on chaotic local search," Information Sciences, vol. 181, no. 15, pp. 3175–3187, 2011.

[32] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 8, pp. 2066–2080, 2013.

[33] F. E. A. El-Samie, "Image Encryption," 2013.

[34] "The USC-SIPI image database," Signal and Image Processing Institute, http://sipi.usc.edu/database, 2017.

[35] T. Sivakumar and R. Venkatesan, "A Novel Image Encryption Using Calligraphy Based Scan Method and Random Number," KSII Transactions on Internet and Information Systems, vol. 9, no. 6, 2015.

[36] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," Signal Processing, vol. 128, pp. 155–170, 2016.

[37] N. Rawat, B. Kim, and R. Kumar, "Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique," Optik, vol. 127, no. 4, pp. 2282–2286, 2016.

[38] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," Multimedia Tools and Applications, vol. 75, no. 21, pp. 13951–13976, 2015.

[39] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," Communications in Nonlinear Science and Numerical Simulation, vol. 20, no. 2, pp. 447–460, 2015.

[40] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," Information Sciences, vol. 349-350, pp. 137–153, 2016.

[41] A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," Optics and Lasers in Engineering, vol. 90, pp. 196–208, 2017.