

Research Article

Chaotic Lightweight Cryptosystem for Image Encryption

Jannatul Ferdush ¹, Mahbuba Begum ^{2,3} and Mohammad Shorif Uddin ³

¹Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore 7408, Bangladesh

²Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh

³Department of Computer Science and Engineering, Jahangirnagar University, Dhaka 1342, Bangladesh

Correspondence should be addressed to Mahbuba Begum; mahbuba327@yahoo.com

Received 18 February 2021; Revised 24 April 2021; Accepted 11 May 2021; Published 24 May 2021

Academic Editor: Patrick Seeling

Copyright © 2021 Jannatul Ferdush et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Data transmission over the Internet and the personal network has been risen day by day due to the advancement of multimedia technology. Hence, it is today's prime concern to protect the data from unauthorized access and encrypt the multimedia element as they are stored on the web servers and transmitted over the networks. Therefore, multimedia data encryption is essential. But, the multimedia encryption algorithm is complex to implement as it requires more time and memory space. For this reason, the lightweight image encryption algorithm gains popularity that requires less memory and less time along with low power or energy and provides supreme security for limited devices. In this study, we have studied the chaotic-based lightweight image encryption method. At first, we have presented a standard framework and algorithm based on two chaotic maps such as Arnold and logistic for lightweight image encryption and performed some experiments. We have analyzed different groups of images such as miscellaneous, medical, underwater, and texture. Experimentations have provided the largest entropy 7.9920 for medical image (chest X-ray), large key space $2^{m \times m \times 8}$, and average encryption and decryption times are 3.9771 s and 3.1447 s, respectively. Besides, we have found an equal distribution of pixels and less correlation coefficients among adjacent pixels of the encrypted image. These criteria indicate an efficient image encryption method. Also, our method is efficient and less complex than the existing state-of-the-art methods.

1. Introduction

Data are very much sensitive, and its security is essential for today's life. Data distribution over the physical medium and Internet has been increasing day by day which makes data security to become a concerning issue. Data security should avoid eavesdropping and provide confidentiality by encrypting the multimedia element. There exist several image encryption algorithms [1–3]. The conventional encryption algorithms such as Rivest–Shamir–Adleman (RSA), advanced encryption standard (AES), and data encryption standard (DES) are complex to implement. Hence, lightweight image encryption is required that provides enhanced security with low computational complexity. We have described the background and contributions of this work in the following sections.

1.1. Background. The lightweight encryption algorithms are based on the structure of the multimedia element on which they are stored [4]. The conventional encryption algorithm has high computational complexity and hence is not suitable for encryption. Asymmetric encryption algorithms require higher computational complexity compared to symmetric encryption algorithms, where a vector of a real number represents the image. Hence, the vector is very long as the sampling coefficients of the image are very large [5]. A digital image is a two-dimensional (2D) vector that contains pixels whose values are between 0 and 255. An image can be represented by any geometric shapes (circles/curves/lines) using these numbers [6]. So, it is very important to secure digital images. The lightweight encryption algorithm provides enhanced security among various sharing devices such as the Internet of Things- (IoT-) based applications where

data security and privacy are prime concerns. Besides, information technology is rapidly developing. Hence, cloud computing spread severely in all sectors including industry, railway, commerce, and administration, where security is the most essential. Therefore, security architecture is needed in these sectors, so that unauthorized users cannot access the cloud [7–9]. For the last two decades, the applications of surveillance systems have been considerably increased. These systems are spread over all the places (public or private). The authenticated users identify or track the object which they want. Surveillance encryption algorithm encrypts the message or video frame to provide security [10]. These IoT-based controlled applications and other applications need data security that should be provided by a lightweight image encryption method. The lightweight image encryption algorithm can be used in the cloud, surveillance systems, railway, dedicated network, Internet of Things (IoT), and medical applications.

1.2. Contributions. For protecting content from unauthorized access and distribution, an efficient image encryption technique is very important. Data privacy along with data security is a concerning issue for today's Internet world. The lightweight image encryption method gives a promising framework by providing low computational complexity. The main contributions of this research are as follows:

- (i) To design a lightweight image encryption method that requires less time, less value for key transformation, and ensures lower correlation coefficients between adjacent pixels of the encrypted image
- (ii) To design a highly sensitive key for encrypting and decrypting images
- (iii) To compare our method with the existing state-of-the-art methods from various perspectives

The rest of the study is organized as follows: Section 2 describes the related literature with the problem statement. Some theories are described in Section 3. We described our proposed framework along with detailed steps of image encryption and decryption in Section 4. The experimental results are described in Section 5. Finally, we concluded our study along with future work in Section 6.

2. Literature Review and Problem Statement

This section describes the related literature of lightweight image encryption and addresses some issues that must be improved.

2.1. Literature Study. Several studies [6–8] have already been performed based on lightweight image encryption. In the scheme [11], a rotation matrix based on bit-level permutation and block-diffusion was proposed. At first, the host image is divided by 8×8 nonoverlapping blocks with a random matrix, and then, each block is transformed into an $8 \times 8 \times 8$ three-dimensional (3D) cube-shaped binary matrix. Then, the 3D matrix is multiplied with the random matrix,

and the permutation is carried out. After that, the system performs block diffusion for coping with any further statistical change of the image. The experiments show satisfactory security performance along with better robustness under several attacks. In another scheme [12], a technique based on heterogeneous bit permutation and correlated chaos was proposed for color image encryption. Here, for reducing the computational cost and improving the permutation efficiency, the heterogeneous bit permutation is used before the expanded XOR operation on three channels (red (R), green (G), and black (B)) of the color image. Then, pseudorandom sequences are generated by a one-dimensional (1D) chaotic map during the encryption process. The experiment gave secure and effective results. Besides, a novel algorithm based on bit permutation and DNA encoding was proposed by Zhang et al. [13]. At first, the hash value is calculated for an input DNA sequence, and the image is scrambled by using the chaotic sequence. The bit permutation of the image is implemented by the butterfly network, and the DNA matrix of the image is generated. For improving the security of the system, an algebraic operation with the DNA sequence is performed. Finally, the operation of the DNA sequence enhances the confusion and diffusion matrices. The experiments show that the algorithm has a large key space, strong sensitivity, and high robustness under various attacks. A lightweight chaotic image encryption algorithm for a 32 bit microcontroller was proposed for designing a real-time embedded system [14]. The performance of the algorithm is suitable for real-time applications, and its safety is observed via different studies such as randomness analysis, sensitivity analysis, encryption quality analysis, differential analysis, statistical analysis, visual analysis, and attack analysis. Besides, for railway cloud service, a lightweight authenticated encryption scheme based on a novel discrete chaotic S-box coupled map lattice (SCML) was proposed in the scheme [15]. SCML minimizes the dynamic degradation of the chaotic system, and the encryption process protects the data from unauthorized access. Also, it maintains the data integrity in one pass. The proposed scheme is secure and robust under various attacks. Besides, privacy for surveillance video is also essential. The entire video is encrypted by the region of interest (ROI) scheme. A lightweight encryption method based on layered cellular automata (LCA) for satellite applications was proposed in the scheme [16]. Here, the ROI's are encrypted individually and stored at the camera memory and used by the individual depends on the user's needs. Any user can see this surveillance video online without ROI in real-time, and the results show that the method is robust and secure. For mobile cloud storage, another privacy-preserving lightweight image encryption (PLIE) method was proposed in the scheme [17], where data privacy is very important. Here, the image metadata is saved in the mobile cloud by using a lightweight encryption method. User's privacy is maintained by the process SDS (split, distribute, and scramble) in mobile. Then, the data are stored in the mobile cloud. In this case, the encryption time is reduced by 50% than the AES method. Image encryption requires a large volume of data that needs an efficient algorithm. In 2018 [18], a secure and

time-efficient image encryption method was proposed based on permutation, diffusion, and multiple one-dimensional (1D) chaotic maps. Here, chaotic maps such as beta, logistic sine, logistic tent, tent-sine, and PWLCM (piece-wise linear chaotic map) are used for ensuring the security of the system. The system ensures large key space and higher information entropy that indicate improved security. The method is robust against chosen plaintext attack (CPA) and known plaintext attack (KPA). But, the system is not designed for color images. Existing cryptosystems perform permutation at the pixel level. But the pixel level permutation methods do not ensure enough security for the system. Hence, a new 3D puzzle for bit permutation along with a chaotic system for encryption was proposed in the scheme [19]. The method is secure and robust against statistical and differential attacks for diffusion and confusion.

In another scheme [20], the method first divides the color image into three channels (R, G, and B) and transposes the channels to the bit-plane. Then, the Arnold cat map (ACM) scrambles the bit-plane matrix and alternate logistic map confuse and diffuse the R, G, and B channels of the scrambled image. The system is highly secure and robust against brute-force attacks. A quantum image encryption method was proposed based on the logistic map using intrabit and interbit permutation in the scheme [21]. At first, the image is represented by the quantum model, and then, the permutation operations (intra and inter) are performed on the bit planes. The encrypted image is finally achieved by the chaotic diffusion process. The method is robust against the brute-force attacks and uniformly bit distributed and secure. For transferring the text files between embedded IoT devices, a secured and efficient, lightweight symmetric encryption method was proposed in [22]. Here, a novel tiny symmetric encryption algorithm (NTSA) is used for transferring large files with enhanced security among IoT devices. In this case, during each round of encryption, an additional key of confusion is introduced dynamically. The method is robust and secured than existing methods. Fast data sharing among various devices is increasing day by day. But it creates challenges for data security. In this regard, a Huffman coding-based lightweight encryption method for data transmission was proposed in the scheme [23]. Here, a HELiOS (Huffman compression-based encryption method using lightweight dynamic order statistic tree) method is used to transmit the digital data. The digital data is first compressed as "secret" or small-sized, so that an attacker does not decode it. The method is fast and secure for data transmission for smart devices. Another work has been developed based on permutation [24]. But, the computational complexity is not observed in this method. In 2019, Patro and Acharya [25] proposed bit-level image encryption based on 1D chaotic maps. The method can be applied to real-time applications. But, the method is not designed for color images. Another image encryption method [26] is proposed based on permutation, diffusion, chaotic, and hyperchaotic maps. For increasing privacy and security, a new encryption/decryption method [27] was proposed by integrating multiple chaotic maps. A new map is generated from this combined multiple chaotic maps, which is robust against various attacks. For good image encryption, the lowest value is selected as a correlation factor. The best

correlation value of the selected chaotic map is used for image encryption and decryption. The proposed method provides satisfactory results in terms of robustness compared to existing methods. Also, the method is secure, has lower computational complexity, and provides better information entropy. The conventional image encryption algorithms ensure high security, but they are complex to calculate and slow in speed for real-time applications. For overcoming these issues, a novel image encryption algorithm with high speed was designed based on the Bülban chaotic map [28]. This chaotic map is generated by using only a limited number of rows and columns. A substitution-permutation system is designed to increase the security of the system. This procedure removes the correlation between adjacent pixels. For preventing the leakage of information, the pixel values are masked. The system is highly secure and fast by the experimental results for real-time applications. But the method is not suitable for real-time applications with high resolution of images. Zheng et al. proposed an image encryption method based on a multichaotic system and DNA coding [29]. Here, the two chaotic maps such as N2D-LSCM (two-dimensional logistic-sine coupling map) and NHenon (new Henon map) are combined. The generated two pseudorandom sequences by N2D-LSCM are used for scrambling the sequence and DNA coding matrix, respectively. Their proposed system is highly secure and robust against common image processing attacks. But the method is not suitable for color images and functioning efficiently. The traditional chaotic algorithms require more cost. Hence, in the scheme [30], a lightweight image encryption algorithm was designed based on the message passing (MP) algorithm and chaotic map. The proposed algorithm is cost-effective in terms of time and space. The adjacent pixels are interconnected to each other without any extra space cost by the MP algorithm, and the encrypted image is produced. The pseudorandom sequences are generated by the two-dimensional (2D) logistic map. The edge pixels are affected by the external message that is produced from these pseudorandom sequences. The experimental results ensure that the method is robust against various attacks, secure, cost-effective, reduces correlation coefficients between adjacent pixels of the encrypted image, and ensures a good information entropy value of 7.996749.

A secure encryption algorithm protects the images from unauthorized access. There exist various image encryption algorithms such as symmetric and asymmetric key cryptographies. A session key-based fast, secure, and lightweight image encryption method was designed by Gupta et al. [31]. The session key is generated by the genetic algorithm. The system security is ensured by the crossover and mutation operators of the genetic algorithm. The method is suitable for both grayscale and color images and outperforms better than existing methods. But the method is not designed for the devices based on the Internet of Things (IoT). There exists a variation of lightweight image encryption algorithms in cost-effectiveness (time and memory space) and security. For developing these issues, a secure lightweight image encryption algorithm was designed for smart cities and IoT-enabled devices [32]. The enhanced security is achieved by increasing the block sizes, key, and number of rounds. The method is not functioning well for IoT-based devices that

consume more power and memory. For resisting KPA and differential attacks, the sensitivity of high key and high plaintext is essential. An improved algorithm was designed by Lin and Wu [33] for analyzing the existing cryptographic methods based on chaotic maps and resisting the CPA. Here, the plaintext image is dependent on image encryption. In this case, an enhanced CIES-UBPRPD (chaotic map-based image encryption system using both plaintexts related permutation and diffusion) is designed to get a higher plaintext sensitivity than the original CIES-UBPRPD method. The method is secure and robust, but it requires more time to execute than the original CIES-UBPRPD method. In 2020, an image encryption method [34] was proposed based on compressive sensing and random numbers insertion. In this case, three encryption methods are required for ensuring the security of the system. The method requires less time to encrypt the image and is robust against rotation, noise, and cropping attacks. Also, the reconstructed image is good in quality. But the pixel values of the encrypted image are not equally distributed by the histogram analysis, which may lead to a statistical attack. Huang et al. [35] proposed an encryption method based on a chaotic system and 2D linear canonical transform (LCT). The method is robust and secure than the previous methods. But the method is not implemented for color images. A four-dimensional (4D) chaotic system is designed based on coexisting hidden chaotic attractors [36]. The method is secure and implemented on hardware. But the key sensitivity, correlation analysis, histogram analysis, key space, and time complexity are not observed. Ye et al. [37] proposed an encryption method based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. The transmission load is reduced, and encryption capacity is increased. But the method is not tested for color images. In 2020, an image encryption method [38] is proposed based on permutation, diffusion, and 1D chaotic maps. The method is robust against KPA and CPA. The method evaluates the performance of various 1D chaotic maps for encrypting images. Experimental results show that 1D chaotic maps such as logistic-sine map (LSM), Kent map (KM), logistic map (LM), logistic tent map (LTM), tent map (TM), tent-sine map (TSM), and beta map (BM) ensure better security and are robust against histogram attack except for DM (dyadic map) and SPLM (sinus-power logistic map). Patro et al. [39] proposed a multiple-image encryption method based on cross-coupled chaotic maps. But the system is not tested for color images. In 2020, another image encryption method [40] is proposed based on permutation, diffusion, and PWLCM. But the method is not simulated for color images. Patro et al. [41] proposed a secure, lossless, and noise-resistive image encryption method based on chaos, hyperchaos, and DNA sequence operation. The method is robust against KPA, CPA, differential, statistical, and noise attacks. Also, the method is more secured than previous methods. But the method is not designed for color images. Medical images are transmitted through the Internet and accessed by the general public. Hence, the security of medical images is very important. For addressing this issue, a medical image encryption method [42] is proposed based on

a logistic map, DNA (deoxyribonucleic acid) sequence, and IWT (integer wavelet transform). The method ensures better security than the existing methods and is robust against brute-force attacks. But the system is not designed for color images. Another medical image security system is proposed based on Chua's diode and strange attractor [43]. This system is implemented on a three-layer hardware-software-based interface. But the method does not use any chaotic map for encrypting images. It needs a large storage for storing the medical image. For addressing this issue, in 2020, Lakshmi et al. [44] proposed a medical image encryption method in a cloud platform based on HNN (Hopfield neural network). The method ensures improved security than the existing methods. Also, the method is robust against CPA. But, the conventional chaotic maps are not used in this method. In 2021, an efficient medical image encryption method is proposed based on IWT, DNA computing, and chaos [45]. The method is robust against KPA and CPA. But, it is not implemented for color images.

2.2. Problem Statement. From the discussions of Section 2.1, we can conclude

- (i) Some encryption algorithms are slow, while some require more time to execute
- (ii) Some algorithms are not suitable for IoT devices and real-time applications
- (iii) Some are less robust against plaintext and differential attacks
- (iv) Also, some algorithms are limited by image type and complex to calculate
- (v) Besides, most of the existing lightweight image encryption algorithms have low plaintext sensitivity and are not functioning well for images with high resolution

We are motivated by the above limitations in developing an optimized framework for lightweight image encryption by combining Arnold and logistic maps.

3. Theoretical Background

The chaotic map is an evolution function that displays the chaotic behavior in terms of continuous-time or discrete-time parameters [46]. There exist some chaotic maps such as Arnold cat map, basin chaotic map, circle map, Chen-Lee system, complex cubic map, exponential map, Gauss map, Henon map, and logistic map. These maps are used in a dynamic system. This section keeps an eye on the theoretical background of our used two chaotic maps.

3.1. Arnold's Chaotic Map. Arnold's chaotic map is a chaotic map mathematically generated from a revolving surface, discovered by Vladimir Arnold [47]. This surface (or torus) is created by rotating a circle in 3D space. This chaotic map is the transformation $\Upsilon: T^2 \rightarrow T^2$, where T^2 is the torus. In matrix notation, this can be written by the following equation:

$$Y \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1, \quad (1)$$

where x and y are the row and columns of the matrix, respectively.

3.2. Logistic Chaotic Map. The logistic map is one of the chaotic maps and a polynomial function of degree 2 [48]. In this case, the chaotic behavior is generated from the nonlinear system. In mathematics, this map can be written by the following nonlinear equation:

$$x_{n+1} = rx_n(1 - x_n), \quad (2)$$

where x_n is the ratio between the existing population and maximum population and $0 < x_n < 1$. r is the parameter whose value is between 0 and 4.

4. Research Method

This section discusses the proposed framework and the detailed steps of image encryption and decryption algorithms.

4.1. Proposed Framework. At first, the Arnold map is applied to the plain (or host) image. Then, the parameters for the logistic map are selected. After then, the cipher (or encrypted) image is generated. The image decryption is performed in a reverse way. The above-discussed framework is shown in Figure 1(a). The flowchart for finding the best parameter for the logistic map is illustrated in Figure 1(b). At first, the parameter is initialized, and the estimation function is calculated. If the termination occurs, then the method will be stopped. Otherwise, the mutation occurs, and a looping condition is generated for calculating the estimated function.

4.2. Detailed Steps of Image Encryption and Decryption. The image encryption and decryption phases of the proposed method are simple. The detailed algorithms for image encryption and decryption are shown in Algorithms 1 and 2, respectively. The genetic algorithm is used to find the optimum initial value for the logistic map, which is shown in step 2 in Algorithm 1. For the Arnold method, there is one parameter, and for logistic, there are two parameters: L_p , which is the initial value and r , which is the control variable. AEncrypt and LEncrypt are the processes related to the Arnold and logistic encryptions, respectively. LDecrypt and ADecrypt are related to the decryption for logistic and Arnold maps, respectively.

Suppose our image is 3×3 in dimensional and the image has the following pixel values. The pixel values are shown in Figure 2(a). We have encrypted the pixels of this figure by our proposed method. The total steps are described as follows:

4.2.1. Select Arnold Parameter. This step is completely independent of image type and size. In this step, the user generates an Arnold parameter (A_p) for shuffling the image. Let the selected value for (A_p) is 10.

4.2.2. Select Best Parameter for Logistic Map. In this step, the optimization algorithm is used to find the best initial value for the logistic map. The range for the initial value is between 0 and 1. Depending on this initial value, the chaotic series is generated. For a chaotic map, there exist two values: one initial value, L_p , and another chaotic control variable, r . At first, the user randomly chooses r from the range (0–4). Then, the best L_p is chosen by the genetic algorithm. For 0.1, we get the entropy of 3.1699 for Figure 2, and this is the best entropy.

4.2.3. Get Entropy and Coefficient Values. Then, we have encrypted the pixels of Figure 2(a) by Arnold parameter 10 and got the horizontal coefficient of 0.3298. After then, the logistic parameter 0.1 is used for encrypting the image, and the encrypted pixel values are generated. This is shown in Figure 2(b). In this case, the values of entropy and horizontal coefficient are 3.1699 and -0.1558 , respectively.

Hence, by combining Arnold with a logistic map, the image information entropy is not increased. But this combination decreases the correlation coefficient between adjacent pixels, which is one of the important parameters for an ideal image encryption system. Therefore, we can select the best parameter for information entropy.

5. Experimental Results

The experiment has been performed in MATLAB R2016, an environment with a computer of core i7, 2.90 GHz processor, and 16 GB RAM. We have used four groups of images for conducting our experiment. The image groups are miscellaneous, medical, underwater, and texture images. Miscellaneous (lena and baboon) images are taken from the USC-SIPI (the University of Southern California-Signal and Image Processing Institute) image database [49]. The chest X-ray and ECG signals belonging to medical images are taken from the Chest X-ray Images (pneumonia) database [50] and ECG heartbeat categorization dataset [51], respectively. Underwater-like fish species and marine animal images are taken from the fish species image dataset [52] and the brackish dataset [53], respectively. Also, the texture (straw and grass) images are taken from the USC-SIPI image database [49].

We have chosen two images from each group. Each image is divided into three different sizes such as 128×128 , 256×256 , and 512×512 pixels. We have applied Arnold, logistic, Arnold + logistic, and (half Arnold + half

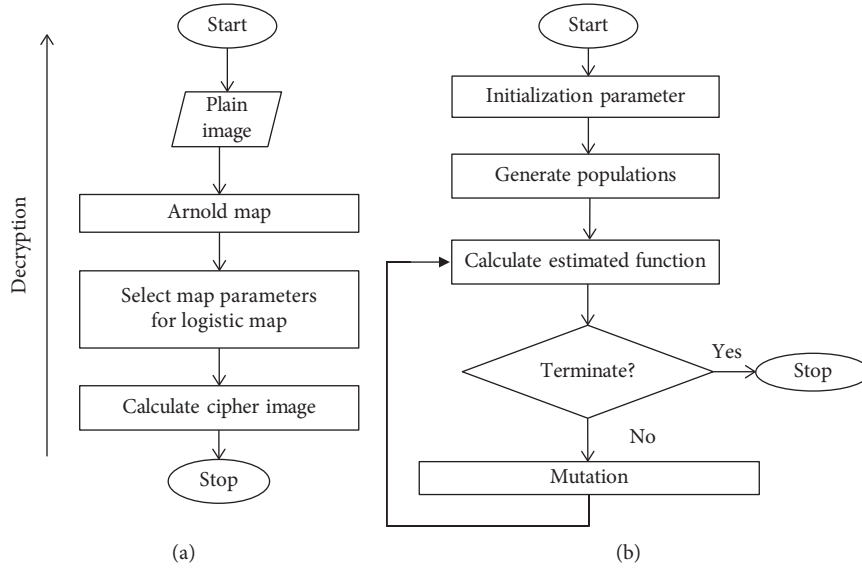


FIGURE 1: (a) Proposed framework for image encryption and decryption. (b) Optimized framework for finding the best parameter for the logistic map.

```

Input: original image,  $I$ 
Output: encrypted image,  $I_C$ , and key,  $K$ 
Step 1: select Arnold parameter: user generated a random value  $A_p$  for Arnold encryption.
Step 2: select  $r$  as random value for the logistic map
Select best parameter (initial value) for the logistic map, which is  $L_p$ 
  for  $i = 0: 0.1: 1$ 
     $I_{temp} = LEncrypt(I, i, r)$ 
     $EI_{temp}(i) = Entropy(Itemp)$ 
    if  $EI_{temp}(i) > EI_{temp}(i - 1)$ 
       $L_p = i$ 
    else
       $L_p = i - 1$ 
    end
  end
Step 3:  $Temp_{IC} = AEncrypt(I, A_p)$ 
        $I_C = LEncrypt(Temp_{IC}, L_p)$ 
        $K = [A_p, L_p, r]$ 

```

ALGORITHM 1: Pseudocode for the proposed image encryption algorithm.

```

Input: encrypted image,  $I_C$  and key,  $K$ 
Output: original image,  $I$ 
Step 1: extract  $K$  as  $[A_p, L_p, r] = Extract(K)$ 
Step 2: decrypt by logistic map:
        $Temp_{IC} = LDcrypt(I_C, L_p, r)$ 
Step 3: decrypt by Arnold map:
        $I = ADcrypt(Temp_{IC}, A_p)$ 

```

ALGORITHM 2: Pseudocode for the proposed image decryption algorithm.

logistic) maps to our host image “Lena” of size 512×512 , which is shown in Figure 3. Here, for each map, the original image size is 79 kB. We have seen that the size of

the encrypted image for the Arnold map, which is 253 kB, is lower than the other chaotic maps. The encryption and decryption times in second (s) are increased for all the methods except logistic map and half Arnold + half logistic, which are 0.8147 s and 0.8638 s and 4.6695 s and 4.5395 s, respectively. Therefore, we can say that the logistic map requires less time to encrypt and decrypt the host image than other chaotic maps.

However, this section discusses various analyses such as entropy analysis, histogram analysis, correlation analysis, key sensitivity analysis, key space analysis, and computational complexity analysis. At the end of this section, our proposed method is compared with existing lightweight image encryption methods. We have compared our results with existing state-of-the-art methods by complexity

127	272	134	92	213	10
100	250	220	234	139	40
134	233	140	76	252	135

(a) (b)

FIGURE 2: Sample image. (a) Original pixels. (b) Encrypted pixels.











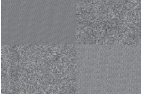

Chaotic maps	Original image	Encrypted image	Decrypted image
(a) Arnold	 Size = 79 kB	 Size = 79 kB; encryption time = 9.4743 s	 Size = 79 kB; decryption time = 9.3650 s
(b) Logistic	 Size = 79 kB	 Size = 258 kB; encryption time = 0.8147 s	 Size = 79 kB; decryption time = 0.8638 s
(c) Arnold + logistic	 Size = 79 kB	 Size = 258 kB; encryption time = 10.5176 s	 Size = 79 kB; decryption time = 10.4687 s
(d) Half Arnold + half logistic	 Size = 79 kB	 Size = 256 kB; encryption time = 4.6695 s	 Size = 79 kB; decryption time = 4.5395 s

FIGURE 3: Lena image 512×512 . (a) Arnold. (b) Logistic. (c) Arnold + logistic. (d) Half Arnold + half logistic.

analysis, statistical analysis, and correlation coefficients analysis of the encrypted image.

5.1. Entropy Analysis. Information entropy measures the uncertainty or randomness of an encryption system. It is the significant criterion of a standard encryption algorithm. Usually, a higher information entropy value produces a better encryption algorithm. In our proposed method, we have combined Arnold and logistic chaotic maps. The optimization technique is used for getting the best initial value for a chaotic map. Based on our method, Table 1 provides some statistical data for different groups of images with different sizes. It includes image types, image name, image size, NPCR (number of changing pixel rate), UACI (unified averaged changed intensity), PSNR (peak signal-to-noise ratio), MSE (mean squared error), and entropy of the encrypted image. From this table, our observations are as follows:

- (i) When the image size is increased, the largest NPCR, UACI, and entropy values are found, but the PSNR values are the least. This indicates an efficient image encryption technique.

- (ii) General (miscellaneous) images get the least entropy than other images

5.2. Histogram Analysis. A perfect image encryption technique divides the encrypted image into equal frequency. Therefore, the attacker gets only a little information from the encrypted image. The image histogram represents an image by the total number of pixels for each tonal value. The histograms of several general original and encrypted images are shown in Figures 4 and 5, respectively. From the original histogram, we get an idea about the frequency of pixels. But there is approximately equal distribution of pixels for encrypted images. Hence, the attacker cannot get any information from the histograms of the encrypted images.

5.3. Correlation Analysis. The correlation identifies the relationship between adjacent pixels of the image. For an original image, there is a relationship between adjacent pixels. From Figures 6(a)–6(d), we have seen that the pixels are so much close to each other. This criterion defines the tightly correlated image. But for Figures 7(a)–7(d), there exists no relationship between pixels. Therefore, the pixels

TABLE 1: Statistical analysis for different groups of images.

Image type	Image name	Size	NPCR	UACI	PSNR	MSE	Entropy
Miscellaneous	Lena	128 × 128	0.9953	0.2651	9.8189	6.7793×10^3	7.9642
		256 × 256	0.9937	0.2075	11.8325	4.2642×10^3	7.4077
		512 × 512	0.9954	0.2651	9.808	6.73964×10^3	7.9762
	Baboon	128 × 128	0.9954	0.241	10.6388	5.6131×10^0	7.9375
		256 × 256	0.9949	0.2377	10.747	5.4750×10^3	7.9434
		512 × 512	0.9949	0.2389	10.7089	5.5232×10^3	7.9472
Medical image	Chest X-ray	128 × 128	0.9967	0.3419	7.5785	1.1356×10^4	7.9851
		256 × 256	0.9959	0.3435	7.5195	1.1511×10^4	7.9920
		512 × 512	0.9962	0.3442	7.4964	1.1573×10^4	7.4964
	ECG signal	128 × 128	0.9966	0.353	7.377	1.1896×10^4	7.9370
		256 × 256	0.9957	0.3516	7.3883	1.1864×10^4	7.9438
		512 × 512	0.9957	0.3533	7.3498	1.1970×10^4	7.9480
Underwater image	Fish species	128 × 128	0.9965	0.3379	7.7698	1.0867×10^4	7.9753
		256 × 256	0.9962	0.3371	7.7796	1.0842×10^4	7.9852
		512 × 512	0.9963	0.3393	7.7255	1.0978×10^4	7.9882
	Marine animal	128 × 128	0.9899	0.1587	14.1337	2.5102×10^3	6.9153
		256 × 256	0.9957	0.2786	9.416	7.4385×10^3	7.9692
		512 × 512	0.9961	0.2789	9.4126	7.4443×10^3	7.9725
Texture	Straw	128 × 128	0.9953	0.2555	10.2246	6.1748×10^3	7.9426
		256 × 256	0.9961	0.2651	9.8573	6.7197×10^3	7.9628
		512 × 512	0.9956	0.2741	9.5634	7.1903×10^3	7.9739
	Grass	128 × 128	0.9952	0.2433	10.5522	5.7262×10^3	7.9419
		256 × 256	0.994	0.2065	0.994	4.3034×10^3	7.5377
		512 × 512	0.9958	0.2789	9.3568	7.5405×10^3	7.9827

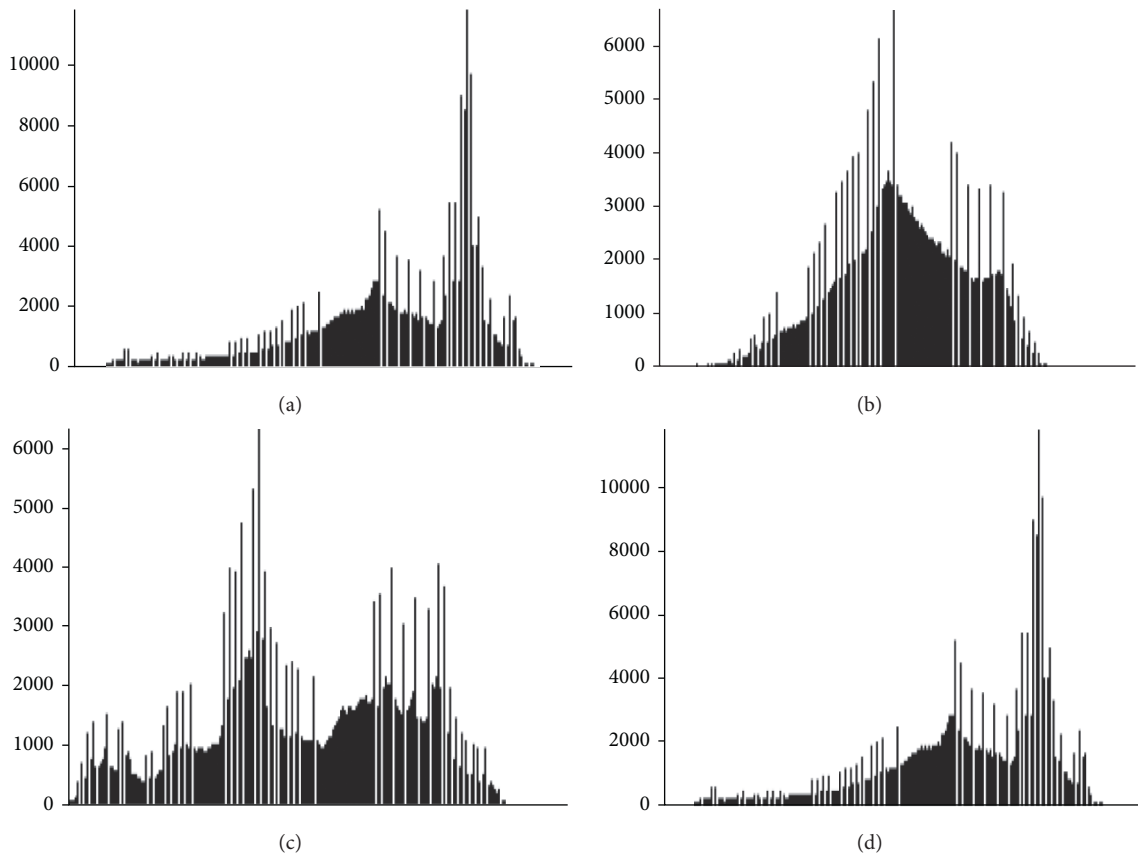


FIGURE 4: (a)–(d) Histograms of original images (lena, baboon, pepper, and boat).

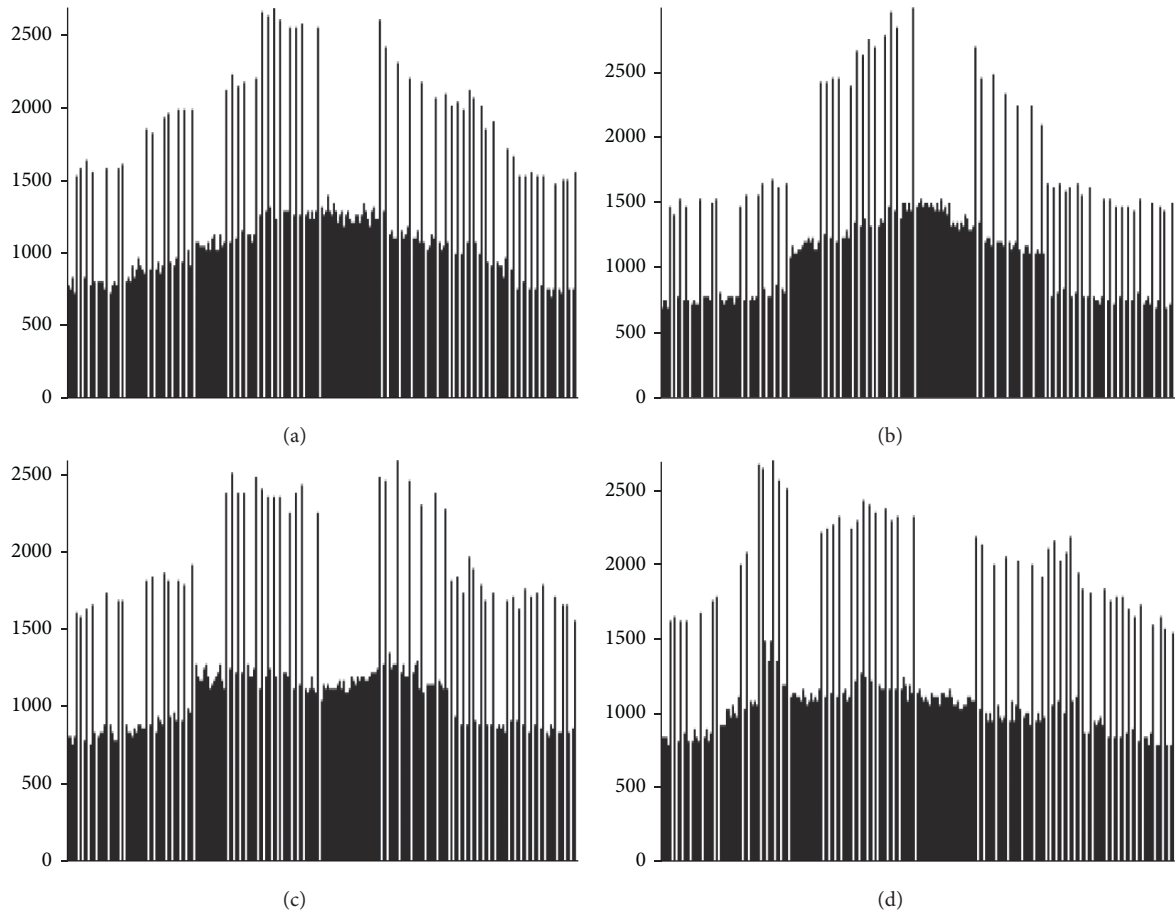


FIGURE 5: (a)–(d) Histograms of encrypted images (lena, baboon, pepper, and boat).

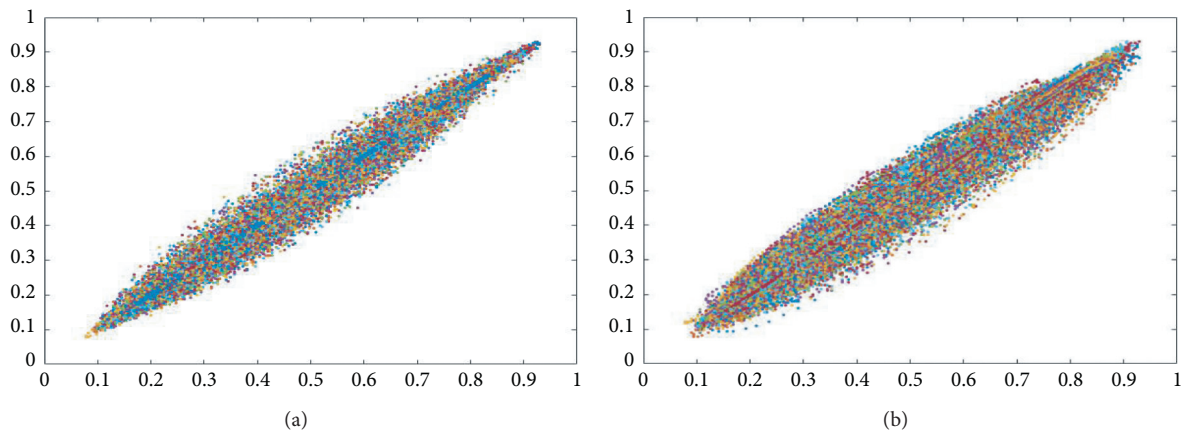


FIGURE 6: Continued.

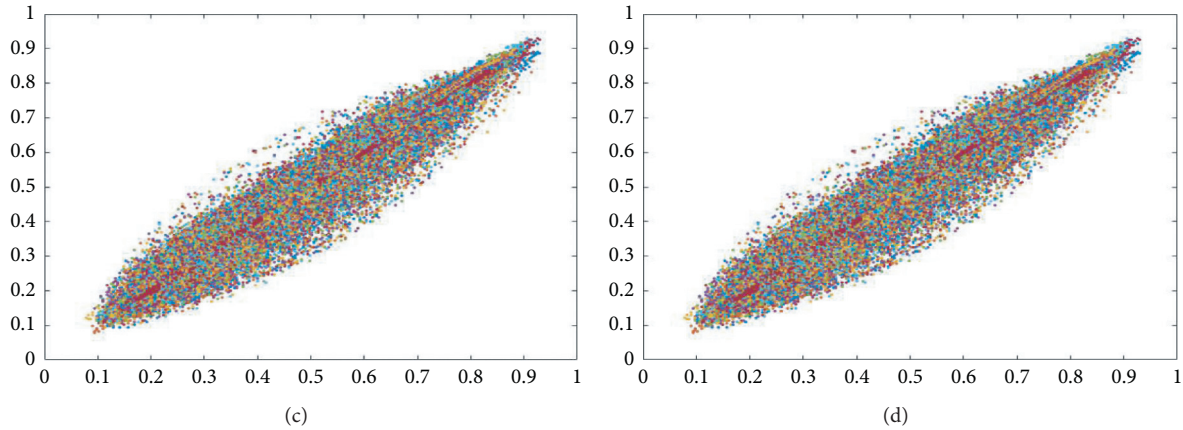


FIGURE 6: (a)–(d) Original image correlation for lena image of 512×512 (horizontal, vertical, diagonal, and antidiagonal).

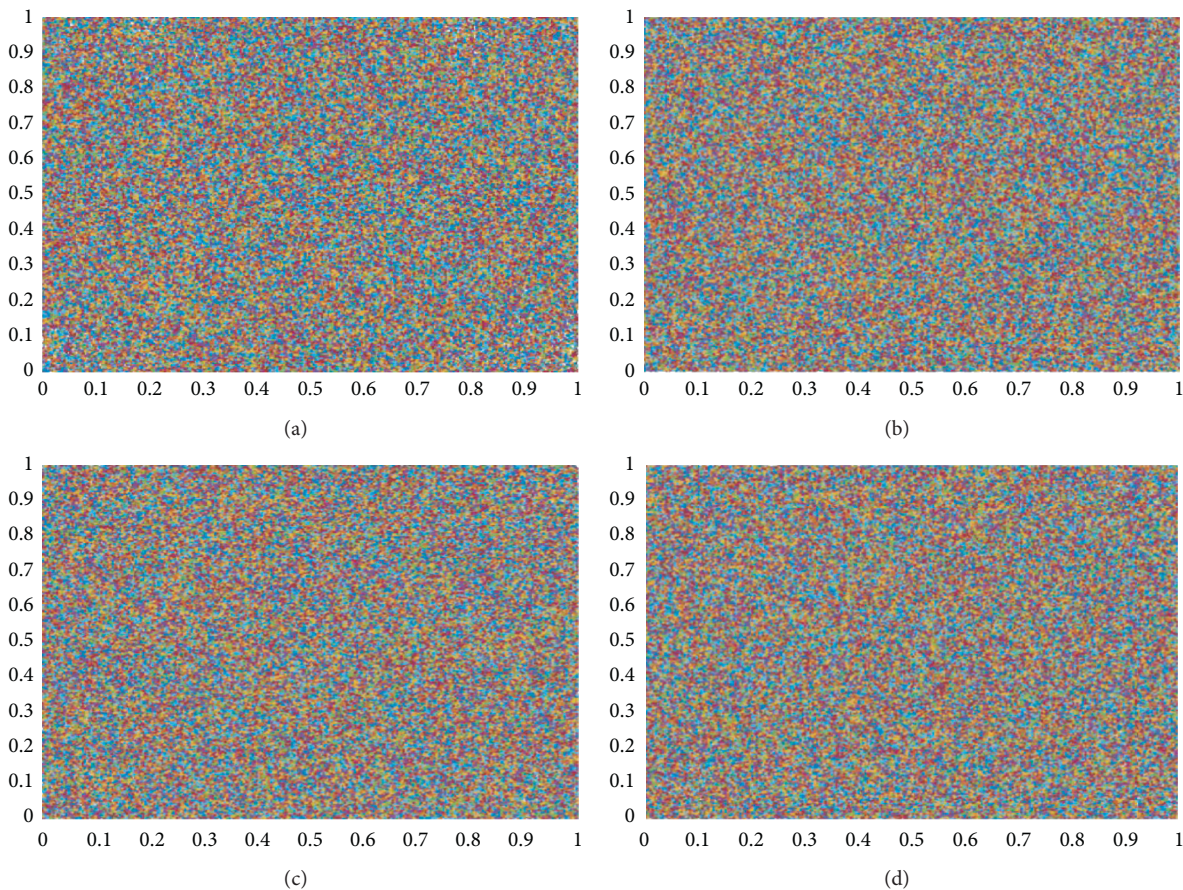


FIGURE 7: (a)–(d) Encrypted image correlation for lena image of 512×512 (horizontal, vertical, diagonal, and antidiagonal).

are not so much close to each other. Rather, they are equally distributed into the whole places of the image.

Table 2 provides the correlation coefficients between adjacent pixels for different groups of images. We have measured the correlation coefficients between adjacent pixels in horizontal, vertical, diagonal, and antidiagonal directions. The correlation coefficients of encrypted images are decreased for

each image of three different sizes. Hence, there exists less relation between adjacent pixels of the encrypted image. Therefore, it is difficult for an attacker to guess about the neighborhood pixel values of the encrypted image. Also, less correlation indicates that the proposed method is robust against statistical attack [54]. These criteria indicate an efficient image encryption method.

TABLE 2: Correlation coefficients between adjacent pixels for different groups of images.

Image type	Image name	Size	Original image				Encrypted image			
			Horizontal	Vertical	Diagonal	Antidiagonal	Horizontal	Vertical	Diagonal	Antidiagonal
Miscellaneous	Lena	128 × 128	0.9028	0.9563	0.8642	0.8995	0.011	0.01	-0.0082	0.0021
		256 × 256	0.9754	0.9894	0.961	0.9717	-0.0414	-0.0342	0.1083	-0.1502
		512 × 512	0.9936	0.9972	0.9895	0.9923	-0.00011	0.0024	-0.0012	3.4004×10^{-4}
	Baboon	128 × 128	0.8701	0.87	0.8086	0.8115	0.0087	0.0052	0.0031	-0.0127
		256 × 256	0.9685	0.9684	0.9413	0.9421	-0.00021	0.0022	0.0033	-0.00091
		512 × 512	0.9915	0.9914	0.9832	0.9834	0.0037	-0.0024	-0.001	4.6074×10^{-4}
Medical image	Chest X-ray	128 × 128	0.9531	0.9513	0.914	0.9123	0.0066	-0.002	0.0017	-0.0066
		256 × 256	0.9676	0.9664	0.9436	0.9399	-0.0014	-0.0102	0.0082	0.006
		512 × 512	0.9831	0.9806	0.9685	0.9658	0.9831	0.0206	-0.00052685	-0.00053
	ECG signal	128 × 128	0.7767	0.6625	0.4893	0.4769	-0.00066	-0.0583	-0.0134	0.0044
		256 × 256	0.8574	0.8104	0.6931	0.6786	0.0043	-0.059	-0.0052	-0.00032
		512 × 512	0.9222	0.905	0.8457	0.8362	-0.00022	-0.0566	-0.0044	0.0017
Underwater image	Fish species	128 × 128	0.8778	0.8692	0.7507	0.8476	-0.0055	-0.0384	9.0022×10^{-4}	-0.0105
		256 × 256	0.9248	0.9169	0.8452	0.9022	0.0041	0.0533	-0.00042386	-0.0073
		512 × 512	0.9497	0.9441	0.8991	0.9368	-0.0029	-0.0511	9.0768×10^{-4}	-0.0036
	Marine animal	128 × 128	0.9951	0.9942	0.9907	0.9907	0.0055	-0.6072	0.0108	-0.2341
		256 × 256	0.9977	0.9951	0.9936	0.993	0.0017	-0.0171	-0.0019	-0.00027
		512 × 512	0.9991	0.9939	0.9933	0.993	-0.002	-0.0025	-0.0017	-0.00097
Texture	Straw	128 × 128	0.5001	0.5864	0.1169	0.585	-0.0035	-0.0194	0.01	-0.0021
		256 × 256	0.6157	0.5758	0.1672	0.6859	0.0019	-0.0169	0.0029	0.0011
		512 × 512	0.7559	0.7444	0.4281	0.8003	2.5022×10^{-3}	-0.0127	-0.00013054	6.3029×10^{-4}
	Grass	128 × 128	0.4404	0.4977	0.2373	0.3166	-0.013	0.0109	-0.0139	0.0082
		256 × 256	0.5833	0.6409	0.3682	0.4481	-0.021	0.0102	0.03	-0.021
		512 × 512	0.7333	0.7996	0.5821	0.6407	-0.0019	7.2259×10^{-4}	-0.0021	-0.0015

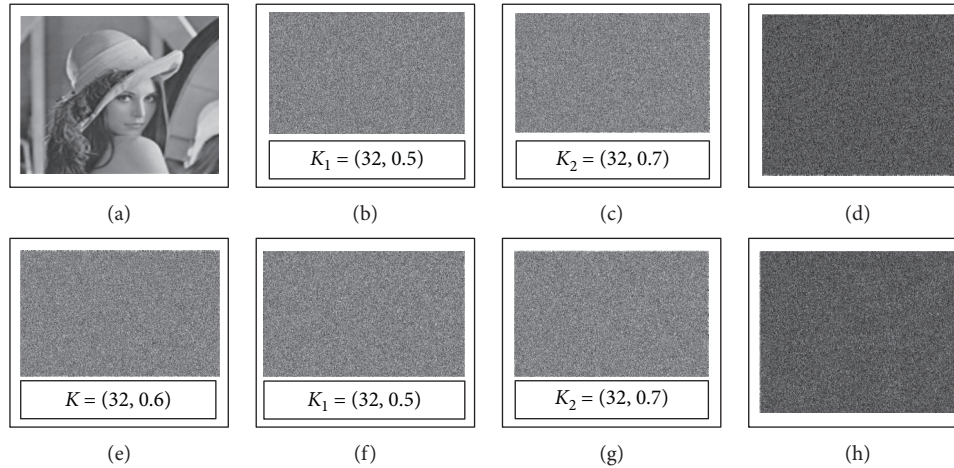


FIGURE 8: (a) Original image. (b) Encrypted image with key K_1 . (c) Encrypted image with key K_2 . (d) Difference of (b) and (c) images. (e) Encrypted image with original key K . (f) Decrypted image with key K_1 . (g) Decrypted image with key K_2 . (h) Difference of (f) and (g) images.

5.4. Key Sensitivity Analysis. A good image encryption system is very much sensitive to the key. A little bit of change in the input key has a larger impact on the encryption system. In Figure 8, we have encrypted an image with the key, K . To check the image's sensitivity, we have also encrypted the image with two other keys: K_1 and K_2 . The generated images are shown in Figures 8(b) and 8(c), respectively. The difference between these two images is shown in Figure 8(d), which is close to a black image that means a significant difference occurs. On the other hand, we have encrypted the host image of Figure 8(a) by the original key, K , which is shown in Figure 8(e). The encrypted image of Figure 8(e) is decrypted with two other keys: K_1 and K_2 , which are seen in Figures 8(f) and 8(g), respectively. These generated two images are completely different from the encrypted image. The difference between these two generated images is shown in Figure 8(h). This image is also a black image that means a significant difference occurs. Therefore, the proposed method is very much sensitive for both encryption and decryption keys. Hence, our proposal is an ideal image encryption method.

5.5. Key Space Analysis. For resisting the brute force attacks, the key space of an image should be large enough. But, we have to remember about the speed. There is a relationship between speed and key size. We have mainly two keys: one for the Arnold map and another for the logistic map. The parameter for the Arnold map is chosen randomly for the user-defined domain, μ , and the parameter for the logistic map is chosen from 0-1. The value is increased by 0.1, and then, the series of the logistic map is mapped by a user-defined another domain λ . This domain is completely secret, and only the sender knows about it. Even the receiver does not know about this domain. From the logistic map, we have generated the logistic series with the size of $m \times m$. This size is the same as to image size. So, there exist $m \times m \times 8$ bits only for the logistic map. Hence, there are $2^{m \times m \times 8}$ ways only for the logistic map, which is very large from the

cryptographic perspective. Thus, it is not possible for the attacker to find the key easily. Therefore, our system is robust against brute-force attacks and indicates an efficient image encryption method.

5.6. Computational Complexity Analysis. We have analyzed for computational complexity in terms of time for different groups of images. When the image size is increased, the image encryption and decryption times in second (s) have been increased. But the growth rate for image encryption time is greater than the image decryption time. For selecting the best initial value, we must run an optimization algorithm. The encryption and decryption times are independent of the image type. But these times are dependent on the image size. This analysis is given in Table 3. From this table, we have observed that there exists a little bit of difference between encryption and decryption time. It takes time to find out the best parameter for the chaotic map in encryption, which is dependent on the image. On the other hand, the value of the parameter for the chaotic map was already known in the decryption phase. Hence, it requires more time to encrypt the images than to decrypt.

5.7. Comparison with Existing State-of-the-Art Methods. We have compared our proposed method with existing lightweight image encryption methods. The computational complexity of our proposed method is compared with existing methods, which is given in Table 4. We have seen that our method requires less time in total in second (s) to execute than existing methods [20, 30]. Method [14] is a hardware-based encryption system. So, it is fast. On the other hand, the encryption time for the image of size 256×256 for method [31] is also less than our method, as method [31] applies the genetic algorithm on the key. But we have used this optimization algorithm on the image, which is more applicable. Method [33] uses a more advanced

TABLE 3: Analysis of obtained computational complexity in terms of time for different images.

Image type	Image name	Size	Encryption time (s)	Decryption time (s)	Total time (s)
Miscellaneous	Lena	128 × 128	0.6296	0.445	1.0747
		256 × 256	2.227	1.7223	3.9492
		512 × 512	9.5097	7.4552	16.9648
	Baboon	128 × 128	0.626	0.4399	1.0659
		256 × 256	2.2441	1.7865	4.0306
		512 × 512	8.8939	7.0877	15.9817
Medical image	Chest X-ray	128 × 128	0.6316	0.4436	1.0753
		256 × 256	2.2314	1.8311	4.0625
		512 × 512	8.9985	7.1753	16.1737
	ECG signal	128 × 128	0.6422	0.469	1.1112
		256 × 256	2.2348	1.7248	3.9597
		512 × 512	9.031	7.2521	16.2831
Underwater image	Fish species	128 × 128	0.6263	0.4486	1.0749
		256 × 256	2.2499	1.745	3.995
		512 × 512	8.9202	7.1831	16.1033
	Marine animal	128 × 128	0.8724	0.5213	1.3938
		256 × 256	2.2589	1.7382	3.9971
		512 × 512	9.0816	7.1498	16.2314
Texture	Straw	128 × 128	0.6327	0.4605	1.0931
		256 × 256	2.2493	1.7534	4.0026
		512 × 512	8.910	7.2109	16.1208
	Grass	128 × 128	0.6540	0.4690	1.123
		256 × 256	2.2462	1.7445	3.9907
		512 × 512	8.8482	7.2158	16.064

TABLE 4: Comparison of computational complexity in time (s).

Parameter	Janakiraman et al. [14], 128 × 128	Bisht et al. [20], areal color 170 × 170	Proposed method, lena 256 × 256	Yousif et al. [27], lena 512 × 512	Liu et al. [30], lena 512 × 512	Gupta et al. [31], lena 256 × 256	Lin and Wu [33], lena 512 × 512	Proposed method, lena 512 × 512
Encryption time (s)	—	34.4626	2.227	—	109.887853	0.0114	3.7944	9.5097
Decryption time (s)	—	—	1.7223	—	—	—	—	7.4552
Total time (s)	0.17815	—	3.9492	5.39	—	—	—	16.9648

TABLE 5: Comparison of statistical parameters.

Parameter	Zhang et al. [13]	Patro et al. [18]	Raza and Satpute [19]	Bisht et al. [20]	Patro et al. [24]	Yousif et al. [27]	Talhaoui et al. [28]	Zheng et al. [29]	Liu et al. [30]	Gupta et al. [31]	Abed and Boyaci [32]	Lin and Wu [33]	Proposed method
NPCR (%)	—	99.6121	99.6227	99.7024	99.6091	100	99.6162	0.99596	0.996097	0.9958	—	99.6096	0.9954
UACI (%)	—	33.4711	33.5196	27.9796	33.4914	33.48	33.4675	0.33459	0.334557	0.2848	—	33.4673	0.2651
Entropy	7.990	7.9969	7.9974	7.9939	7.9991	7.71	7.902741	7.99923	7.568285	7.9971	7.9976	—	7.9762
PSNR	—	—	—	8.96	—	8.33	—	—	—	—	—	—	9.808

personal computer (PC) than us that is configured with Intel Core i7, 3.2 GHz processor, and 32 GB RAM. Hence, it takes less time to execute. The statistical parameters indicate the system's security, which are given in Table 5. We have seen that NPCR, UACI, and entropy values are not satisfied with the previous methods. It is because of using the plain chaotic map to encrypt the image in our method. The values of

correlation coefficients between adjacent pixels of the encrypted image are given in Table 6. From this table, we can say that for using the Arnold map, our correlation values getting lower than most of the existing methods except methods [20, 24] and [33] because methods [20, 33] use color images where the values are more changed. Method [24] uses bit-level permutation along with a chaotic map for

TABLE 6: Comparison of correlation coefficients of encrypted image.

	Direction	Zhang et al. [13]	Patro et al. [18]	Raza and Satpute [19]	Bisht et al. [20]	Patro et al. [24]	Talhaoui et al. [28]	Zheng et al. [29]	Liu et al. [30]	Gupta et al. [31]	Lin and Wu [33]	Proposed method
Encrypted image	Horizontal	0.0082	0.0024	0.000561	-0.0012	0.0064	0.0039	0.6578	0.0020	0.0065	-0.0036	-0.00011
	Vertical	0.0032	0.0029	0.000578	-0.0170	0.0004	0.0059	0.7301	0.0035	0.0058	-0.0008	0.0024
	Diagonal	0.0150	-0.0039	0.001547	0.0148	-0.0095	-0.0050	0.6387	0.0027	—	-0.0017	-0.0012

image encryption. Therefore, these methods exhibit fewer correlation coefficients between adjacent pixels of the encrypted image.

Therefore, from the above discussions, we can say that the overall performance of our proposed method is good enough because fewer values are required to be transformed as the key, which is one of the important properties of the lightweight cryptosystem.

6. Conclusions and Future Works

Usual multimedia encryption algorithms require more time and memory space. For this reason, the lightweight image encryption algorithm gains wide acceptance, as it requires less memory and less time along with high security. With this view, here, we have proposed an optimized framework by combining two chaotic encrypting methods such as Arnold and logistic maps. We have performed experimental analysis and obtained satisfactory results. Our proposal is very much sensitive to the secret key. The attacker does not get any information from the encrypted image. Also, the proposed method is robust against brute force attacks and requires less time to execute than the existing methods. It also requires less value to transform the key, which ensures an efficient lightweight image encryption method. Besides, the method provides lower correlation coefficients between adjacent pixels of the encrypted image than other methods, indicating an efficient image encryption system. But the statistical parameter values are less than the existing methods because of using the plain chaotic map. The more the values of statistical parameters are, the more the system will be secured. Arnold's chaotic map has a disadvantage like a periodicity. Besides, the logistic chaotic map has the characteristic of simplicity but not ergodicity, as well as it has a short chaotic range of 3.57–4.0. In the future, we will try to increase the values of statistical parameters by combining improved Arnold chaotic map and logistic-sine map or logistic-tent map or tent-sine map or piece-wise linear chaotic map for increasing the security level of the system. By observing histogram images, it is found that the grayscale pixel values are not properly uniformed. So, there may be a chance of a statistical attack. Subsequently, we will analyze our proposal for different attacks such as statistical, noise, and occlusion attacks to test the robustness. We will perform histogram variance analysis and chi-square test analysis to measure the grayscale uniformity quantitatively. For this, we will compare our proposal for robustness with existing state-of-the-art methods to prove our method a better one. After that, we will analyze the time complexity of our proposal step-by-step. Also, the

proposed method can be implemented for color images in the future.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

All authors have contributed equally to write this manuscript.

Acknowledgments

The authors are thankful to the Information and Communication Technology Division of the Government of the People's Republic of Bangladesh for a Ph.D. fellowship to Mahbuba Begum.

References

- [1] S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in *Proceedings of the International Conference on Electronics and Information Engineering*, pp. 141–145, Kyoto, Japan, August 2010.
- [2] G. M. B. S. S. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," in *Proceedings of the 4th IEEE Conference on Industrial Electronics and Applications*, pp. 3662–3666, Xi'an, China, May 2009.
- [3] Y. Zhou, K. Panetta, and S. Aгаian, "Image encryption using binary key-images," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, pp. 4569–4574, Hyatt Regency Riverwalk, San Antonio, TX, USA, October 2009.
- [4] K. Nahrstedt, J. Dittmann, and P. Wohlmacher, "Approaches to multimedia and security," in *Proceedings of the IEEE International Conference on Multimedia and Expo. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532)*, pp. 1275–1278, New York, NY, USA, August 2000.
- [5] A. Massoudi, F. Lefebvre, C. DeVleeschouwer, B. Macq, and J. J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," *EURASIP Journal on Information Security*, vol. 2008, Article ID 179290, 2008.
- [6] Chapter 1, *Digital Image Representation*, https://pippin.gimp.org/image_processing/chap_dir.html, 2021.

- [7] M. S. Farash, S. A. Chaudhry, M. Heydari, S. M. S. Sadough, S. Kumari, and M. K. Khan, "A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security," *International Journal of Communication Systems*, vol. 30, no. 4, 2017.
- [8] G. Hu, D. Xiao, T. Xiang, S. Bai, and Y. Zhang, "A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud," *Information Sciences*, vol. 387, pp. 132–145, 2017.
- [9] B. Gupta, D. P. Agrawal, and S. Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global, Hershey, PA, USA, 2016.
- [10] P. Carrillo, H. Kalva, and S. Magliveras, "Compression independent reversible encryption for privacy in video surveillance," *Eurasip Journal on Information Security*, vol. 2009, Article ID 429581, 2010.
- [11] Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74–82, 2014.
- [12] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Optics Communications*, vol. 342, pp. 51–60, 2015.
- [13] X. Zhang, F. Han, and Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Computational Intelligence and Neuroscience*, vol. 2017, pp. 6919675–11, 2017.
- [14] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: implementation and analysis on 32 bit microcontroller," *Microprocessors and Microsystems*, vol. 56, pp. 1–12, 2018.
- [15] Q. Zheng, X. Wang, M. Khurram Khan, W. Zhang, B. B. Gupta, and W. Guo, "A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service," *IEEE Access*, vol. 6, pp. 711–722, 2018.
- [16] X. Zhang, S.-H. Seo, and C. Wang, "A lightweight encryption method for privacy protection in surveillance videos," *IEEE Access*, vol. 6, pp. 18074–18087, 2018.
- [17] M. Sankari and P. Ranjana, "PLIE- a light-weight image encryption for data privacy in mobile cloud storage," *International Journal of Engineering & Technology*, vol. 7, no. 4, pp. 368–372, 2018.
- [18] K. A. K. Patro, A. Banerjee, and B. Acharya, "A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1 D chaotic maps," in *Smart and Innovative Trends in Next Generation Computing Technologies. NGCT 2017*, Communications in Computer and Information Science, Springer, Berlin, Germany, vol. 828, pp. 396–418, 2018.
- [19] S. F. Raza and V. Satpute, "A novel bit permutation-based image encryption algorithm," *Nonlinear Dynamics*, vol. 95, no. 2, pp. 859–873, 2019.
- [20] A. Bisht, M. Dua, S. Dua, and P. Jaroli, "A color image encryption technique based on bit-level permutation and alternate logistic maps," *Journal of Intelligent Systems*, vol. 342, pp. 1–15, 2019.
- [21] X. Liu, D. Xiao, and Y. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2019.
- [22] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.
- [23] M. Islam, N. Nurain, M. Kaykobad, S. Chellappan, and A. B. M. A. A. Islam, "HELIOS: huffman coding based lightweight encryption scheme for data transmission," in *Proceedings of 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, ACM, pp. 70–79, Houston, TX, USA, November 2019.
- [24] K. A. K. Patro, B. Acharya, and V. Nath, "A secure multi-stage one-round bit-plane permutation operation based chaotic image encryption," *Microsystem Technologies*, vol. 25, no. 6, pp. 2331–2338, 2019.
- [25] K. A. K. Patro and B. Acharya, "A simple, secure, and time-efficient bit-plane operated bit-level image encryption scheme using 1 D chaotic maps," in *Innovations in Soft Computing and Information Technology*, J. Chattopadhyay, R. Singh, and V. Bhattacharjee, Eds., Springer, Berlin, Germany, pp. 261–278, 2019.
- [26] K. A. K. Patro, B. Acharya, and V. Nath, "Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps," *Microsystem Technologies*, vol. 25, no. 12, pp. 4593–4607, 2019.
- [27] B. Yousif, F. Khalifa, A. Makram, and A. Takieldean, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Advances*, vol. 10, Article ID 075220, 2020.
- [28] M. Z. Talhaoui, X. Wang, and M. A. Midoun, "Fast image encryption algorithm with high security level using the bülbán chaotic map," *Journal of Real-Time Image Processing*, vol. 18, pp. 85–98, 2020.
- [29] J. Zheng, Z. Luo, and Z. Tang, "An image encryption algorithm based on multichaotic system and DNA coding," *Discrete Dynamics in Nature and Society*, vol. 2020, Article ID 5982743, 16 pages, 2020.
- [30] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, "A lightweight image encryption algorithm based on message passing and chaotic map," *Security and Communication Networks*, vol. 2020, Article ID 7151836, 12 pages, 2020.
- [31] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, pp. 10391–10416, 2020.
- [32] A. M. Abed and A. Boyaci, "A lightweight cryptography algorithm for secure smart cities and IOT," *Electrica*, vol. 20, no. 2, pp. 168–176, 2020.
- [33] C.-Y. Lin and J.-L. Wu, "Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 22, no. 5, p. 589, 2020.
- [34] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, Article ID 107563, 2020.
- [35] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Journal of Materials Chemistry*, vol. 124, Article ID 105821, 2020.
- [36] L. Gong, R. Wu, and N. Zhou, "A new 4 D chaotic system with coexisting hidden chaotic attractors," *International Journal of Bifurcation and Chaos*, vol. 30, no. 10, Article ID 2050142, 2020.
- [37] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional hartley transform and improved pixel adaptive diffusion," *Signal Processing*, vol. 175, Article ID 107652, 2020.

- [38] D. Sravanthi, K. A. K. Patro, B. Acharya, and M. Prasanth Jagapathi Babu, "Simple permutation and diffusion operation based image encryption using various one-dimensional chaotic maps: a comparative analysis on security," *Lecture Notes in Networks and Systems*, Springer, vol. 94, pp. 81–96, Berlin, Germany, 2020.
- [39] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, Article ID 102470, 2020.
- [40] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 12959–12994, 2020.
- [41] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Technical Review*, vol. 37, no. 3, pp. 223–245, 2020.
- [42] S. Aashiq Banu and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical and Biological Engineering and Computing*, vol. 58, pp. 1445–1458, 2020.
- [43] S. Rajagopalan, S. Poori, M. Narasimhan et al., "Chua's diode and strange attractor: a three-layer hardware-software co-design for medical image confidentiality," *IET Image Processing*, vol. 14, no. 7, pp. 1354–1365, 2020.
- [44] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, S. Rajagopalan, R. Amirtharajan, and N. Chidambaram, "Neural-assisted image-dependent encryption scheme for medical image cloud storage," *Neural Computing and Applications*, 2020.
- [45] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Medical & Biological Engineering & Computing*, vol. 59, no. 3, pp. 589–605, 2021.
- [46] "List of Chaotic Maps," 2021, https://en.wikipedia.org/wiki/List_of_chaotic_maps.
- [47] "Arnold's Cat Map," 2021, https://en.wikipedia.org/wiki/Arnold's_cat_map.
- [48] "Logistic Map," 2021, https://en.wikipedia.org/wiki/Logistic_map.
- [49] "The USC-SIPI Image Database," 2021, <http://sipi.usc.edu/database/>.
- [50] "Chest X-Ray Images (Pneumonia)," 2021, <https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia/>.
- [51] "ECG Heartbeat Categorization Dataset," 2021, <https://www.kaggle.com/shayanfazeli/heartbeat/>.
- [52] "Fish Species Image Data," 2021, <https://www.kaggle.com/sripaadsrinivasan/fish-species-image-data/>.
- [53] "The Brackish Dataset," 2021, <https://www.kaggle.com/aalborguniversity/brackish-dataset/>.
- [54] X.-J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu, and J. Ma, "A fast encryption algorithm of color image based on four-dimensional chaotic system," *Journal of Visual Communication and Image Representation*, vol. 33, pp. 219–234, 2015.