entropy

MDPI

Article

An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map

Priya Ramasamy [1], Vidhyapriya Ranganathan [2], Seifedine Kadry [3], Robertas Damaševičius [4,*] and Tomas Blažauskas [4]

[1] Department of Applied Mathematics and Computational Sciences, PSG College of Technology, Coimbatore, TamilNadu 641004, India
[2] Department of Biomedical Engineering, PSG College of Technology, Coimbatore, TamilNadu 641004, India
[3] Department of Mathematics and Computer Science, Beirut Arab University, Beirut 11-5020, Lebanon
[4] Department of Software Engineering, Kaunas University of Technology, Kaunas 51386, Lithuania
* Correspondence: robertas.damasevicius@ktu.lt

Received: 10 May 2019; Accepted: 1 July 2019; Published: 3 July 2019

Abstract: Nowadays, the images are transferred through open channels that are subject to potential attacks, so the exchange of image data requires additional security in many fields, such as medical, military, banking, etc. The security factors are essential in preventing the system from brute force and differential attacks. We propose an Enhanced Logistic Map (ELM) while using chaotic maps and simple encryption techniques, such as block scrambling, modified zigzag transformation for encryption phases, including permutation, diffusion, and key stream generation to withstand the attacks. The results of encryption are evaluated while using the histogram, correlation analysis, Number of Pixel Change Rate (NPCR), Unified Average Change Intensity (UACI), Peak-Signal-to-Noise Ratio (PSNR), and entropy. Our results demonstrate the security, reliability, efficiency, and flexibility of the proposed method.

Keywords: image encryption; chaotic system; block scrambling; modified zigzag transformation; 3D logistic map; entropy analysis

1. Introduction

With rapid spread of cloud computing, mobile networks, internet of things, and social networking, the issue of secure transmission of image data has become increasingly relevant [1,2]. Encrypting secret information that is sent over Internet or wireless networks as multimedia is important in satisfying the need of a secure route of data transmission over various communications channels. Averting unapproved access, adjustment, or the destruction of data ought to anchor the data exchanged through these channels. Different types of data are transmitted over the channels, for example, text, images, audio, video, three-dimensional (3D), and others for many domains of application, such as military, medical, financial institutions, etc. However, the security of those images is a challenge. The critical part of exchanging images is security, in order to protect the image from unauthorized access and modification.

The utilization of cryptographic strategies for image encryption is especially required in order to provide a powerful solution to the security of images. The cryptographic strategies convert the image into an irrelevant data sequence that cannot be effortlessly broken by the attacker. The target of image encryption is to provide high security and avoid unauthorized access. Standard cryptography techniques, such as Advanced Encryption Standard (AES), are regularly applied for text messages.

However, those techniques, due to specific qualities, for example, extensive information and high correlation among image pixels, are not reasonable for media data.

The essential methods for an encryption framework can be arranged into two fundamental classes: diffusion and confusion [3]. The chaotic sequence creates the mapping with random sequence. These structures are excessively unpredictable and hard to break down and anticipate [4,5]. Previously, various encryption techniques that are dependent on chaos have been examined and broadly contemplated. Image encryption algorithms have been constructed based on a logistic and two-dimensional (2D) chaotic economic map [6], variable length codes that are based on Collatz conjecture [7], 2D discrete wavelet transform and Arnold mapping [8], logistic mapped convolution and cellular automata [9], cat map [10], 2D Chebyshev-sine map [11], 2D Sine Logistic modulation map [12], one-dimensional (1D) delay with linearly coupled Logistic chaotic map [13], a hyper-chaotic system that combines Dynamic Filtering, DNA computing, and Latin Cubes (DFDLC) [14], Arnold Transform followed by Qubit Random Rotation [15], 2D Baker's map with diffusion process based on XORing [16], ant colony optimization [17], Chebyshev Map followed by Rotation Equation [18], an algorithm combining Julia fractal and Hilbert curve [19], four-dimensional (4D) hyper-chaotic nonlinear Rabinovich system [20], Josephus traversing and mixed chaotic map [21], 2D logistic-modulated-sine-coupling-logistic chaotic map [22], multiple permutation of pixels followed by the 2D Chebyshev function [23], chaos map with pixel permutation [24], improved hyperchaotic sequences [25], high-dimension Lorenz chaotic system with a perceptron model [26], rotation matrix bit-level permutation with block diffusion [27], and discrete Chirikov map with chaos-based fractional random transform [28].

Cryptanalysis is the science of deciphering secret keys or plaintext when compared with cryptography [29–33], comprising a further branch of cryptology. Research on cryptanalysis is of high importance in promoting cryptology advancement. Applying insecure algorithms for communication will result in severe security threats and losses on both ends of communications if security bugs are not found in encryption cryptosystems. The latest studies have demonstrated that some image encryption methods that are based on chaos schemes have vulnerabilities. Li et al. [29] used the chaotic tent map (CTM) with the diffusing phase only, while the confusing phase was skipped. Consequently, the CTM based image encryption has security defects. Wu et al. [30] used CTM with rectangular transform. The scheme included confusion and diffusion, followed by an improved 2D Arnold transform, which thus improves the security of the classical CTM based method. Wu's algorithm has the advantages of easy design, high encryption speed, and good cryptographic efficiency as a typical colour image encryption method is concerned. However, it cannot resist the chosen plaintext attack, and the encryption method is insensitive to all secret keys. Li et al. [31] evolved the cipher text-only, known-plaintext, and chosen-plaintext attacks on the Ye's scheme [24]. Li et al. [32] created the known-plaintext attack on the Zhu's system [25]. Guo et al. [33] used the equivalent key attack on the 3D chaotic Baker map based image cryptosystem. Some of the chaos-based image encryption schemes that have been broken are discussed in [34]. Cryptanalysis can also assist developers to enhance the safety of the encryption algorithm, in addition to revealing weaknesses in encryption algorithms. Sam et al. [35] used shift rotate within the chaotic framework, which allowed for adaptability proficiency, straightforwardness, and resistance against known assaults. Wang et al. [36] added a shift operation to Huang's scheme [23], which prevents the recovery of the shuffle vectors, thus increasing the security against the chosen-plaintext attack, but without a noticeable loss of efficiency. Wang et al. [37] offered an encryption technique that used logistic mapping and the combined row and scrambling technique to improve the security characteristics.

So far, few results depending on confusion and diffusion have been suggested [38–43], providing an understanding that there is a solid connection between chaos and cryptography. The chaotic behavior system framework ensures high efficiency and high safety due to pseudo-randomness, as they are sensitive to initial conditions. The one-dimensional (1D) chaotic systems, such as pseudo-randomly enhanced logistic map (PELM) [44], are more attractive than multi-dimensional (MD) chaotic systems in order to create pseudo-random keystream [45], due to high speed and simplicity. However, it still has some limitations, such as discontinuity, numerical degradation, non-consistency, and weak key space [46], which thus motivates the need for MD maps, such as a3D mixed chaotic map [47]. Articles [48,49] suggested the intertwining of the logistic maps to strengthen the security and to enhance pseudo-randomness and increase the key space.

Here, we propose a novel key generation algorithm that uses block scrambling, modified zigzag transformation, and enhanced logistic–tent map for image encryption. The current work extends we work of Li et al. [50], by suggesting the use of Enhanced Logistic–Tent Map (ELTM) instead of 3D logistic map to obtain better encryption characteristics. The principal contribution of the paper is the proposed key generation algorithm using ELM, which provides high security, as it takes plain image and key for each iteration of key generation. Here, a new efficient ELTM bases algorithm is proposed. The statistical test analysis is done by the National Institute of Standards and Technology (NIST) statistical test suite demonstrates its better security characteristics.

The remaining parts of the paper are as follows. We describe the methods used in Section 2. In Section 3, the results are presented. In Section 4, the NIST statistical test suite results are given. Finally, we summarize our results and present the conclusions in Section 5.

2. Materials and Methods

2.1. Logistic Map

Chaotic maps are highly sensitive to the initial value, which makes them unpredictable. A change in the numerical sequence that is generated by the function can occur, even if a minor change in the initial value is executed [51]. Different forms of chaotic maps are used; however, the logistic map is perhaps the most known map and is defined in Equation (1) [13], as follows:

$$T_{n+1} = rT_n(1 - T_n), \tag{1}$$

here T_n is the state, r is the behavior parameter, and n is the count of iterations used to generate the state values iteratively.

This 1D logistic map can be extended to a three-dimensional (3D) one, as indicated in Equation (2) [52].

$$\begin{aligned} T_{n+1} &= \alpha T_n(1 - T_n) + \lambda U_n^2 T_n + \beta V_n^3 \\ U_{n+1} &= \alpha U_n(1 - U_n) + \lambda V_n^2 U_n + \beta T_n^3 \\ V_{n+1} &= \alpha V_n(1 - V_n) + \lambda T_n^2 V_n + \beta U_n^3 \end{aligned} \tag{2}$$

If the values of the parameters fall within the ranges $0.53 < \alpha < 3.8$, $0 < \lambda < 0.022$, $0 < \beta < 0.015$, here T_0, U_0, V_0 are in [0, 1], and then the chaotic behavior is observed.

2.2. Skew Tent Map

The skew tent map is represented by the nonlinear equation [52]:

$$T_{n+1} = \begin{cases} T_n/c, 0 < T_n \leq c \\ (1 - T_n)/(1 - c), c < T_n < 1 \end{cases}, \tag{3}$$

here $T_n \in [0, 1]$ is the state, $c \in [0, 0.5] \cup [0.5, 1]$ is the behaviour parameter, and n is the count of permutations that are used to create state values iteratively.

2.3. Block Scrambling

First, the RGB image, which has the dimension of 256 × 256 × 3 is segregated into four quadrants. Subsequently, each quadrant is further segregated into four sub-quadrants, while each sub-quadrant is rotated anti-clockwise by 90° to form 64 sub-blocks. While this procedure scrambles the image, it does not fully remove the associations between the nearby pixels.

2.4. Modified Zigzag Transformation

Zigzag Transformation (ZT) is a procedure to have an image scrambled [53]. The red, green, and blue image channels are treated as separate matrices having the size of 256 × 256 pixels. In ZT, the upper left pixel is shifted to one side, which allows for the attacker to crack the strategy. In the modified ZT, the upper left and next horizontal neighboring pixels are exchanged with the base right pixel.

The change is performed to the pixels of every matrix, starting from the upper left corner and ending with the base right corner to execute encryption. The first and the second elements of the matrix are moved to the last and one-before-last position of the matrix, and the remaining elements are swapped in a zigzag way.

The first and second elements of the matrix are moved to the last and the one-before-last elements of the matrix and the remaining elements of the matrix are swapped in a zigzag way to execute decryption. The change is connected to the pixels of every framework as delineated. This strategy totally twists the relationship among the nearby pixels of the image, which results in the modified ZT of the image.

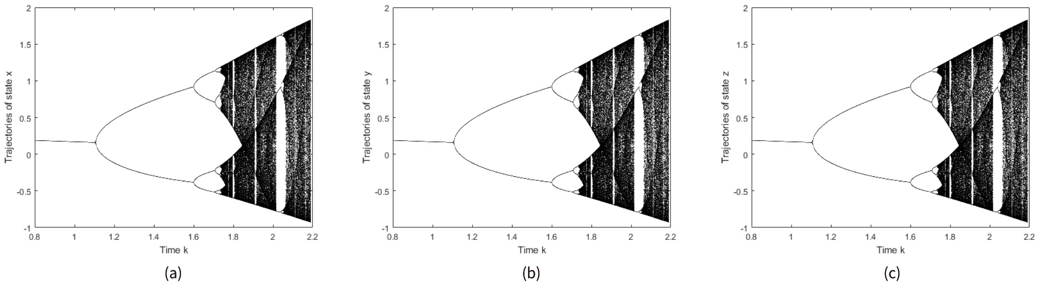
2.5. Enhanced Logistic Map (ELM)

The proposed Enhanced Logistic Map (ELM) enhances the security of the scheme by employing the chaotic diffusion method. The ELM is 3D, as it separately deals with RGB of the color image. The ELM is defined, as follows:

$$\begin{aligned} X_{i+1} &= -\lambda T_i(1-X_i) + \beta Y_i^2 X_i + \alpha Z_i^3 + c \\ Y_{i+1} &= -\lambda U_i(1-Y_i) + \beta V_i^2 Y_i + \alpha X_i^3 + c \\ Z_{i+1} &= -\lambda Z_i(1-Z_i) + \beta X_i^2 Z_i + \alpha Y_i^3 + c \end{aligned} \tag{4}$$

where, $\lambda,\ \beta,\ \alpha,\ c$ are the constants, $0.8 < \lambda < 2.60$, $0 < \beta < 0.15$, $0.42 < \alpha < 0.85$, $0 < c < 0.35$. The range of all $\lambda,\ \beta,\ \alpha,\ c$ are greater than the 3D logistic map, thus it provides better security than the 3D logistic map.

The bifurcation diagram and the Lyapunov Exponent of ELM are shown in Figures 1 and 2, respectively.



(a)

(b)

(c)

Figure 1. Bifurcation diagram of x, y, and z values for Enhanced Logistic Map (ELM): (**a**) x values, (**b**) y values, and (**c**) z values.

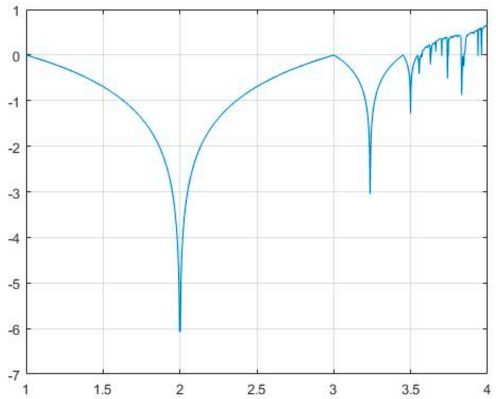


Figure 2. Lyapunov Exponent of Enhanced Logistic Map.

2.6. Key Generation

Both encryption and decryption processes use the same key. $X_0,\ Y_0,\ Z_0$ have their values in [0, 1]. Accordingly, the values are transformed to the range 0–255. The equation for generating the values of X, Y, Z are presented below:

$$\begin{aligned} X_i &= \left\lfloor 10^{14}(X_i)\text{mod}256 \right\rfloor \\ Y_i &= \left\lfloor 10^{14}(Y_i)\text{mod}256 \right\rfloor \\ Z_i &= \left\lfloor 10^{14}(Z_i)\text{mod}256 \right\rfloor \end{aligned} \tag{5}$$

For example, the initial values for X_i, Y_i, Z_i are defined as $X_0 = 0.790$, $Y_0 = 0.889$, and $Z_0 = 0.590$, respectively, and the values of constants are $\lambda = 2.741$, $\beta = 0.021$,$\alpha = 0.041$, and $c = 0.9$.

The cryptosystem is secured with the plain image, the novel proposed system employs a 256-bit key (K), which has 192-bit data calculated from ELM, the secret key (K_e), and 64-bit data chosen by the user from a plain image (K_d). K_d retains pixels $R\left(r_i,\ r_j\right)$, $G\left(g_i,\ g_j\right)$, $B\left(b_i,\ b_j\right)$, which are selected by the encoder. Now, $K = K_eK_d$, where the key K is segregated into 16-bit parts $ks_1,\ ks_2 \ldots\ ks_{16}$.

The initial condition I_c, the parameter P_x and the iteration count n of the skew tent system are defined by the following equations:

$$\begin{aligned} &I_c = \ ks_2 \oplus ks_4 \oplus \cdots \oplus ks_{14} \oplus ks_{16})/256 \\ &P_x = ks_1 \oplus ks_3 \oplus \cdots \oplus ks_9 \oplus ks_{11}) \ + ks_{13} + ks_{15})/758 \\ &n = (ks_{14} \oplus ks_{15}) + ks_{16} \end{aligned} \tag{6}$$

As a result, the generated key depends on the image and EX-OR operation is executed with each value of $R,\ G,\ B$.

2.7. Encryption Algorithm

The proposed framework can be used for any M × M color image. Encryption has two parts: confusion and diffusion. Blocks scrambling is used to obtain 64 squares when confusion is performed. Finally, the modified ZT is performed to remove the association between the adjacent pixels. Key generation executed while using the 3D ELM to produce secret keys in the range 0–255 for every X, Y, and Z. In the final step, the EX-OR operation is executed to obtain the cipher image.

Algorithm 1 summarizes the algorithm of encryption.

Algorithm 1: Algorithm of the encryption process

```
Input: plain color image $P$ of size $256 \times 256$
Output: cipher image $C$
Step 1: Block scrambling is applied on $P$, which is split into 64 blocks each of size $32 \times 32$ represented as $C_1$.
Step 2: Modified zigzag transform (ZT) is performed on the scrambled blocks $C_1$ to obtain $C_2$.
Step 3: $C_2$ is split into RGB channels each of size $256 \times 256$.
Step 4: Using ELM, the intermediate key is generated with initial values are taken as
$X_0 = 0.790,\ Y_0 = 0.889,\ Z_0 = 0.590$, respectively.
Step 5: The final key is generated by applying the chosen values from image and external user as initial
condition and parameters.
Step 6: The secret key K is EX-OR-ed with the RGB channels received after modified ZT to obtain $C$.
```

Figure 3 presents the block diagram for the encryption procedure. The decryption process is performed in reverse of encryption to obtain plain image *P*.

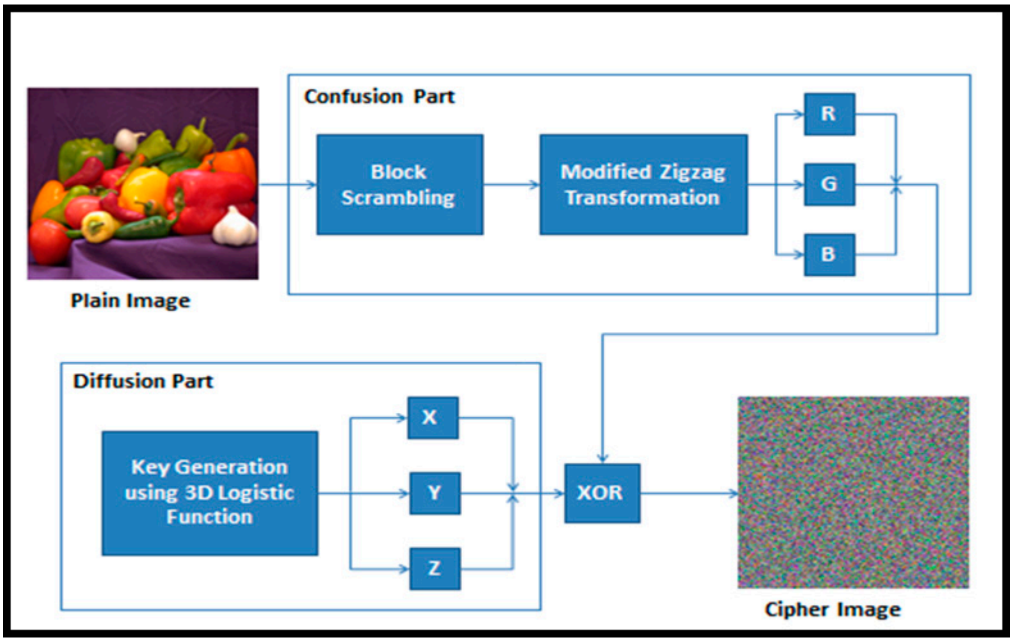


Figure 3. Block diagram of encryption process.

2.8. Evaluation

We assess the security characteristics of the proposed scheme while using histogram analysis, information entropy analysis, correlation coefficient, Number of Pixels Change Rate (NPCR), Unified Average Change Intensity (UACI), Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR).

2.8.1. Key Space Analysis

The proposed method is heavily dependent on the key, it should ensure that the key is secure, and that the key space should be adequately large to make the brute force attack impossible. As the proposed algorithm uses a 256-bit key, the number of admissible secret key combinations is 2^{256} for R, G, and B separately, making it quite difficult to break while using brute force.

2.8.2. Key Sensitivity Analysis

The good encryption method must be very sensitive to changes in the keys. Implementing a small change to the encryption key, the output image must be very different when compared to the unmodified encrypted image.

2.8.3. Histogram Analysis

The histogram represents the distribution of pixel values in an image. An encrypted image is expected to have a uniform distribution of the histogram values, making for the attacker difficult to learn something about the image. Thus, the suitability of the proposed encryption method is shown by the uniform distribution of pixel values in a coded image.

2.8.4. Correlation Coefficient Analysis

Usually, the neighboring pixels of the plain image are related, while the adjacent pixels of the encrypted image are weakly correlated, which suggests that there are no associations between them.

Correlation Coefficient Analysis (CCA) is performed to assess the level of similarity between the pair of pixels. This involves the calculation and assessment of the Pearson correlation coefficient alongside the vertical, horizontal, and diagonal directions of both the plain and encrypted image.

A good encryption method should break the correlation between adjacent pixels. The less the correlation is, the more effectively the method performs. The correlation coefficient is calculated, as follows:

$$\begin{array}{l} CR = \frac{\mathrm{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \\ \mathrm{cov}(X,Y) = \frac{1}{256}\sum_{1}^{256}(X_i - E(X))(Y_i - E(Y)) \end{array}, \tag{7}$$

here X and Y are the pixels and neighboring pixels of the original and encrypted image, $\mathrm{cov}(X,Y)$ is the covariance between X and Y, $D(X)$ is variance of X, and $E(X)$ is the expected value of X.

2.8.5. NPCR and UACI Analysis

Number of Pixels Change Rate (NPCR) assesses the pixel difference between the original and encrypted images [54,55], as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MN} \cdot 100, \tag{8}$$

here $D(i,j)$ is calculated as

$$D(i,j) = \begin{cases} 0 & P(i,j) = C(i,j) \\ 1 & P(i,j) \neq C(i,j) \end{cases}, \tag{9}$$

Higher randomization of the pixel values leads to a larger value of NPCR.

The Unified Average Changing Index (UACI) assesses the mean intensity of differences between the original image and encrypted image [56,57], as follows:

$$D(i,j) = \begin{cases} 0 & P(i,j) = C(i,j) \\ 1 & P(i,j) \neq C(i,j) \end{cases}, \tag{10}$$

here $P(i,j)$ and $C(i,j)$ are pixel values of the original and encrypted images, and L is the largest pixel value of both images.

The values of both NPCR and UACI indicate the resistance of the encryption method against the differential attack.

2.8.6. Information Entropy Analysis

Information entropy assesses uncertainty of a random variable, as follows [56]:

$$E = \sum_{i=1}^{256} P(i) \log\left(\frac{1}{P(i)}\right), \tag{11}$$

here $P(i)$ is the probability of the presence of pixel i.

A larger entropy value indicates a greater level of security when applied to evaluate image encryption. Usually, an entropy value that is very close to a perfect value of 8 is considered to be safe from a brute force attack.

2.8.7. PSNR Analysis

The Peak-Signal-to-Noise Ratio (PSNR) can be used to assess the quality of an image. A good image encryption method is expected to produce encrypted images with a low value of PSNR. Mathematically, PSNR is calculated by:

$$PSNR = 10 \log_{10} \frac{255 \cdot 255}{\sqrt{MSE}}, \tag{12}$$

where $P(i, j)$ is pixel value of the original image, and $C(i, j)$ is pixel value of the encoded image, and Mean Square Error (MSE) is calculated as:

$$MSE = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{[P(i, j) - C(i, j)]^2}{NM}, \tag{13}$$

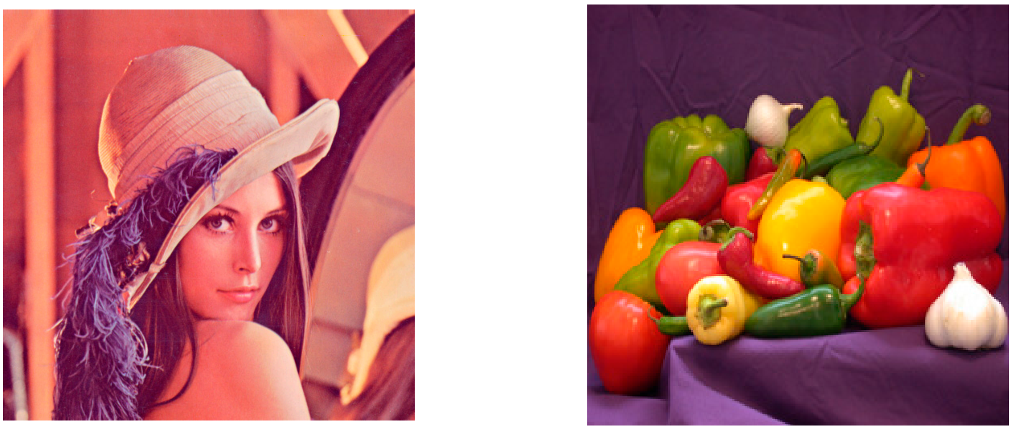
3. Results and Analysis

3.1. Settings

All of the simulations were performed on a desktop computer with Intel ®Core™ i5-2430M CPU 2.4GHZ Processor, 4GB RAM, and Windows 8 Professional operating system. We used the freely available images from the USC-SIPI image dataset, such as Baboon, Plane, Lena, and Peppers, as the original protected images (see Figure 4). Figure 5 shows the encrypted images.

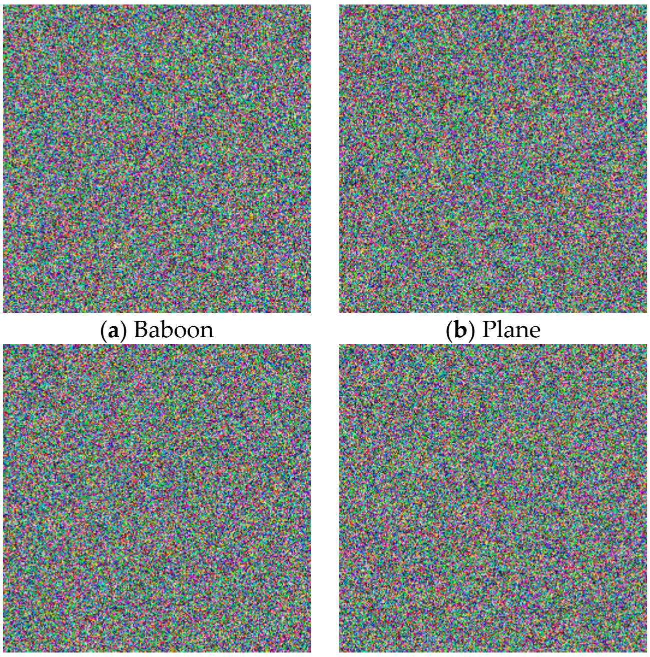
(a) Baboon (b) Plane

Figure 4. *Cont.*



(c) Lena (d) Peppers

Figure 4. Original images: (**a**) Baboon, (**b**) Plane, (**c**) Lena, and (**d**) Peppers.



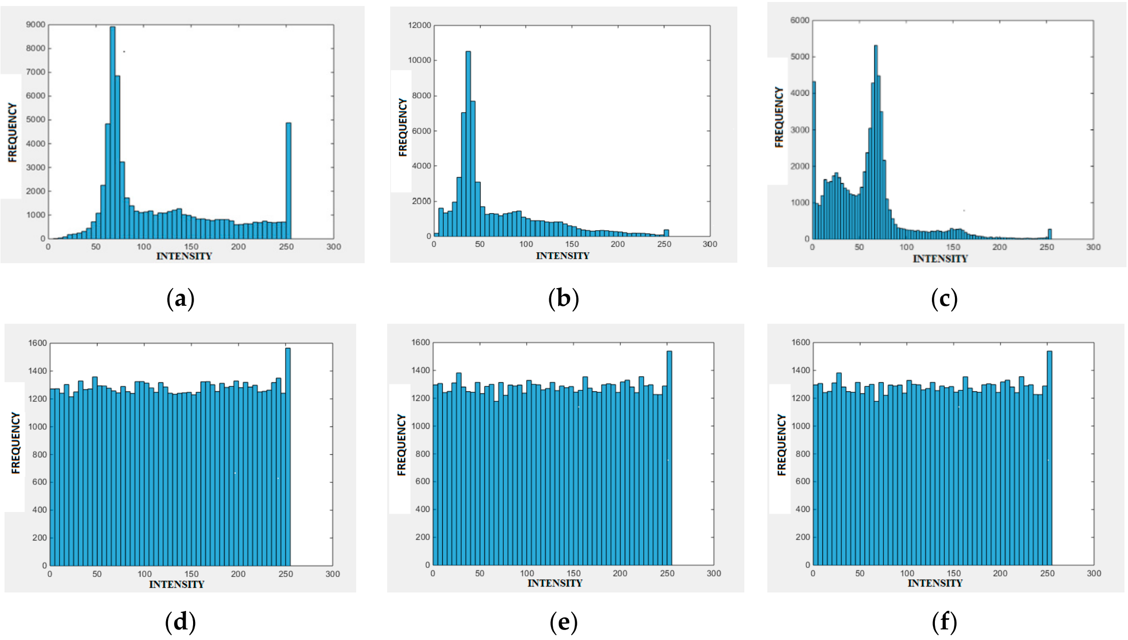
(**a**) Baboon (**b**) Plane

(**c**) Lena (**d**) Peppers

Figure 5. Encrypted images: (**a**) Baboon, (**b**) Plane, (**c**) Lena, and (**d**) Peppers.

3.2. Results

Standard techniques and tests are recommended for evaluating the results [51–53]. The quality of the proposed encoding method is indicated by the uniform distribution of pixel values in an encrypted image while using the histogram analysis method. As an example, see a histogram of the Peppers image for red (R), green (G), and blue (B) channels in Figure 6a–c. Figure 6d–f presents the RGB channels of the encrypted Peppers image. Here, the uniform distribution indicates that it would be difficult for the attacker to decipher the data.

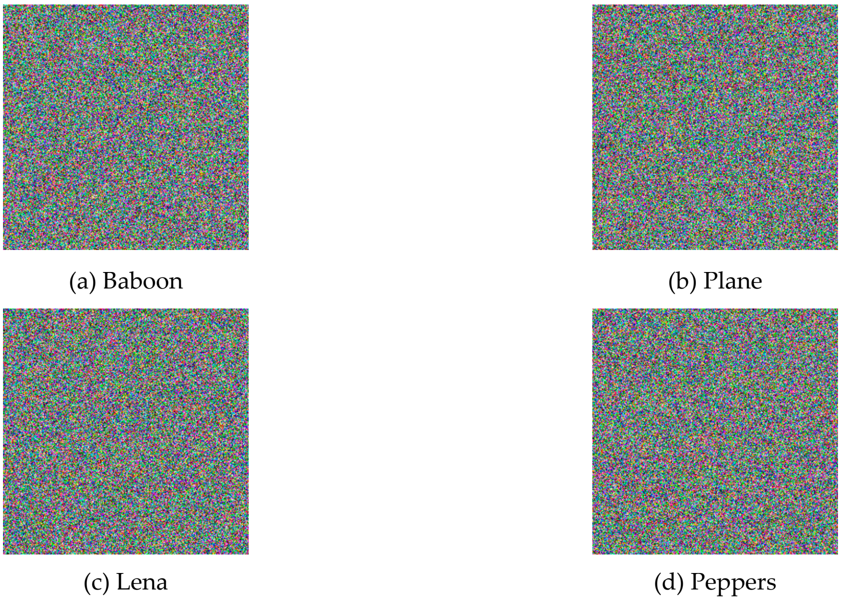


(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 6. Histograms of Peppers image for red (**a**), green (**b**) and blue (**c**) channels, and histogram of an encrypted Peppers image for red (**d**), green (**e**), and blue (**f**) channels.

It will not be possible to reconstruct the enciphered image if the keys differ by a small value [23]. As an example, Figure 7 shows the reconstructed images with a minor change of the secret key from $X_0 = 0.790$ to $X_0 = 0.791$, leading to totally different images.

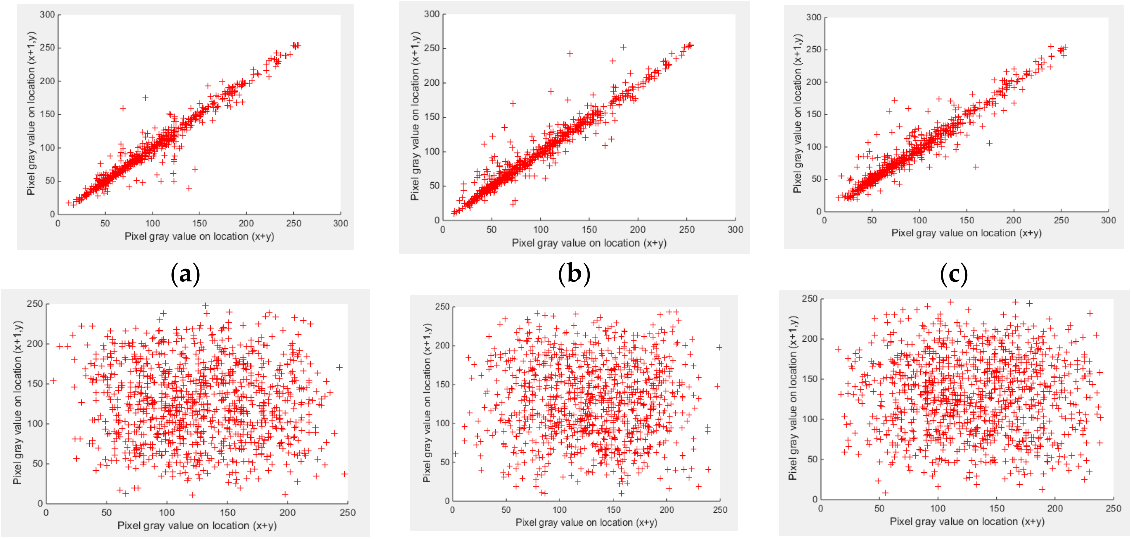


(a) Baboon (b) Plane

(c) Lena (d) Peppers

Figure 7. Decrypted images with correct secret key, but the initial value changed from $X_0 = 0.790$ to $X_0 = 0.791$: (**a**) Baboon, (**b**) Plane, (**c**) Lena and (**d**) Peppers.

The scattered graph can show the correlations between the neighboring image pixels. 1000 random neighboring pixels from an image are used to show the relationship. As an example, Figure 8a–c demonstrates a strong correlation between adjoining pixels, along horizontal, vertical, and diagonal neighboring pixels in the Peppers plain image. However, the correlation between the neighboring pixels is weak for an encrypted Pepper image (see Figure 8d–f).



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 8. Relationship between neighboring pixels in horizontal (**a**), vertical (**b**), and diagonal (**c**) directions of plain Pepper image, and relationship between neighboring pixels in horizontal (**d**), vertical (**e**), and diagonal (**f**) directions of encrypted Pepper image.

The correlation values for plain and encrypted images are given in Table 1 for the Lena, Peppers, Barbara, and Baboon images, along the horizontal, vertical and diagonal directions.

Table 1. Results of correlation analysis.

Images	**Horizontal**		**Vertical**		**Diagonal**	
	Plain	**Cipher**	**Plain**	**Cipher**	**Plain**	**Cipher**
Lena	0.9505	−0.0237	0.9745	−0.0237	0.9668	−0.0284
Peppers	0.9789	−0.0727	0.9750	−0.0225	0.9711	−0.0242
Barbara	0.9444	−0.0298	0.9555	−0.0611	0.9225	−0.0294
Baboon	0.9618	−0.0261	0.9686	−0.0572	0.9475	−0.0356

Table 2 presents the results of NPCR and UACI, PSNR, and Entropy. The values of NPCR and UACI demonstrate that the algorithm is very resistive against differential attack. The entropy is quite close to a perfect value of 8, and demonstrates that the proposed encryption method randomized the pixels in the encrypted image well. The obtained PSNR values are low, hence they also show that the proposed algorithm is good.

Table 2. Results of Number of Pixels Change Rate (NPCR), Entropy, Unified Average Change Intensity (UACI), and Peak Signal to Noise Ratio (PSNR).

Images	**NPCR (%)**	**UACI (%)**	**PSNR**	**Entropy Plain Image Cipher Image**	
Baboon	99.6017	33.2039	11.8337	7.2730	7.9993
Barbara	99.6073	33.5692	8.6936	7.6320	7.9990
Lena	99.6221	33.5887	6.7494	7.7329	7.9994
Peppers	99.5987	33.9060	9.8369	7.3785	7.9992

The proposed method is compared with other methods, while using entropy, NPCR, UACI, and correlation analysis for the Lena image of size 256 × 256 in Table 3. Here, we compare our method with other methods that were proposed by Li et al. [50] by Zhang et al. [27], Xu et al. [58], Wang et al. [59], Liu and Wang [60], Hussain et al. [61], Wang and Zhang [62], and Ahmad et al. [56].

Table 3. Performance evaluation and comparison with other methods (best values are shown in bold).

Measure	[50]	[56]	[27]	[58]	[59]	[60]	[61]	[62]	Proposed
Horizontal correlation	0.0327	0.9407	**0.0018**	−0.0230	0.0020	0.0965	−0.0067	−0.0098	−0.0237
Vertical correlation	0.0219	−0.0273	0.0011	0.0019	**−0.0007**	−0.0318	−0.0137	−0.0050	−0.0178
Diagonal correlation	0.0180	−0.0140	**−0.0012**	−0.0034	−0.0014	0.0362	−0.0563	−0.0013	−0.0284
Entropy	7.9993	n/a	7.9994	7.9974	7.9970	n/a	n/a	7.9974	**7.9995**
UACI	n/a	15.38	33.4365	3.5100	27.97	n/a	33.4647	32.48	**33.5887**
NPCR	n/a	99.10	99.6166	99.6200	98.36	n/a	98.6810	93.21	**99.6221**

In an occlusion attack, the enciphered image, which is transmitted over communication channels, could lose blocks of information. The robustness of the proposed algorithm against 12.5%, 25%, and 50% of occlusion in an encrypted image is evaluated while using MSE. The resulting MSE values are 1542.8362 for 12.5%, 3214.7971 for 25%, and 6927.9417 for 50% occlusion. We can claim that the proposed method can resist an occlusion attack, as the deciphered image still can be retrieved.

Following the suggestion of Askar et al. [63], the original images are corrupted by adding Gaussian noise with the mean of 0 and variance of 0.001, as well as with salt and pepper noise with the density of 0.05. Figure 9 shows the obtained deciphered images. To compare, Table 4 shows the MSE and PSNR values. Based on Table 4, it can be concluded that the proposed method is resistant to salt and pepper noise, since the PSNR value exceeded 58 dB.

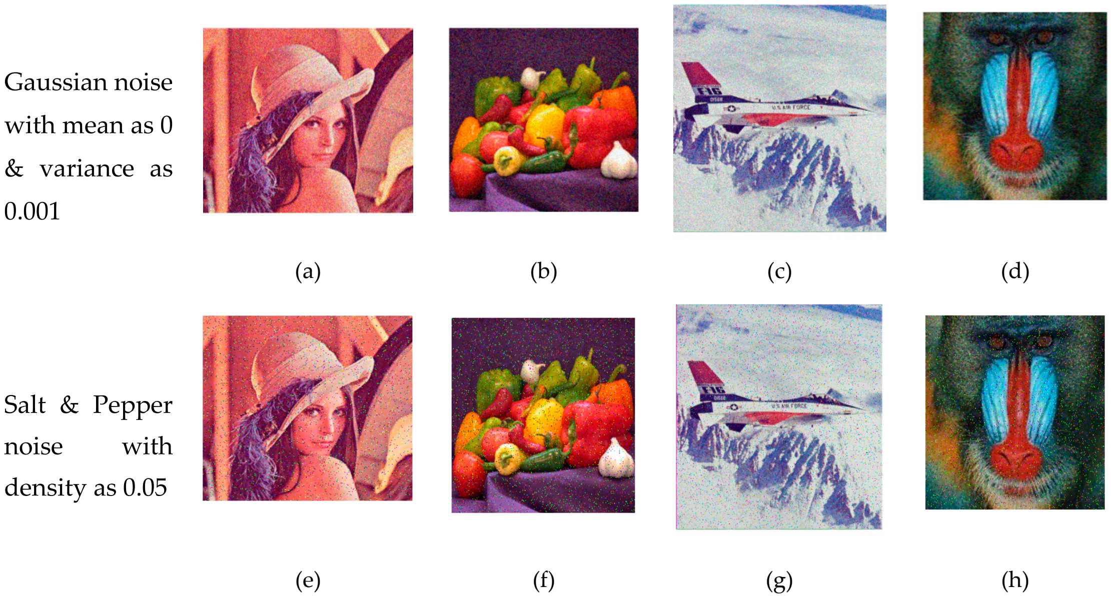

Gaussian noise with mean as 0 & variance as 0.001
(a)
(b)
(c)
(d)
Salt & Pepper noise with density as 0.05
(e)
(f)
(g)
(h)

Figure 9. Analysis of noise attack: decrypted images after adding Gaussian noise, (**a**–**d**); decrypted images after adding salt and pepper noise (**e**–**h**).

Table 4. Mean Square Error (MSE) and PSNR between input images and decrypted images distorted by adding noise.

Sample Images	Gaussian Mean = 0 & Variance = 0.001		Salt & Pepper Density = 0.05	
	MSE	PSNR	MSE	PSNR
Baboon	0.2698	53.8199	0.1711	58.7987
Plane	0.2711	53.7987	0.0793	59.1405
Lena	0.2013	54.1722	0.1022	58.0382
Peppers	0.2368	54.3872	0.0995	58.3375

The Tang's algorithm [64], Zhang's algorithm [65], and Karawia's algorithm [66] were compared for the computational performance analysis. The results are shown in Figure 10 for the same set of four images, and they demonstrate that the proposed algorithm is computationally more efficient.

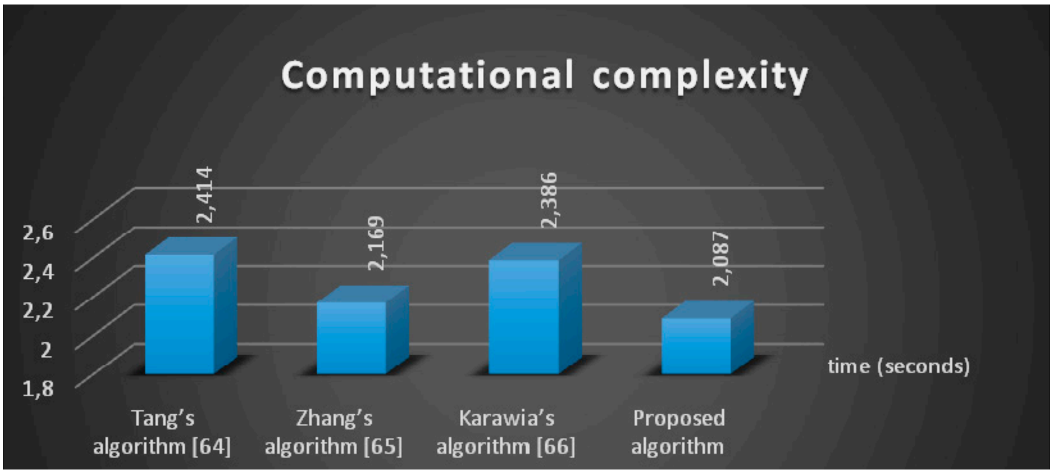


Figure 10. Comparison of computational time for the proposed algorithm.

4. Statistical Test Analysis

The NIST statistical test suite (version 2.1.1, National Institute of Standards and Technology, Gaithersburg, MD, USA) [67] was used to evaluate the randomness of the bit sequence that was produced by the proposed system. The suite involves 15 tests, which assess the randomness that might occur in a series. Table 5 presents the results. Table 5 indicates that the NIST test is effectively performed: all p−values among 1000 sequences used for testing are evenly distributed in the 10 subintervals, while the pass rate is also acceptable. The average pass rate is 99.1% with a minimum pass rate of 98.4%.

Table 5. Results of NIST statistical test [67] for 1000 sequences, 1 million bits each, generated by the proposed scheme.

NIST Test	p-Value	Pass Rate
Frequency (monobit)	0.576884	995/1000
Block-frequency	0.783572	996/1000
Cumulative sums (Forward)	0.541882	996/1000
Cumulative sums (Reverse)	0.914691	993/1000
Runs	0.843905	984/1000
Longest run of Ones	0.062147	986/1000
Rank	0.400721	991/1000
FFT	0.186524	993/1000
Non-overlapping templates	0.497492	993/1000
Overlapping templates	0.230513	990/1000
Universal	0.087607	986/1000
Approximate entropy	0.198766	994/1000
Random-excursions	0.689012	615/621
Random-excursions Variant	0.397213	618/621
Serial 1	0.893692	992/1000
Serial 2	0.699795	993/1000
Linear complexity	0.344217	992/1000

5. Conclusions

We introduced an image encryption method that is based on a chaotic map with a new symmetric key generation system. The scheme uses Block Scrambling and Modified Zigzag Transformation, while key generation is performed using the enhanced logistic-tent map. Confusion and diffusion are achieved by pixel shuffling. It provides priority to resisting the brute-force attack to the suggested algorithm. The experimental results revealed that the suggested method has generated the encrypted images with uniform distribution in pixel histograms. Moreover, the suggested algorithm has shown that the encrypted pictures have information entropy of close to 8. It is able to robustly resist chosen/known plaintext attacks, is robust to salt and pepper noise, and it can withstand up to 50 percent occlusion attack. The comparison experiments were performed with other recent algorithms. The results of the statistical testing indicate that the new pseudo-random bit combiner can provide file encryption/decryption safety. We claim that the method is secure and computationally efficient based on the analysis of the proposed method. The proposed algorithm is simple, fast, and has strong practical application value.

Author Contributions: Conceptualization, S.K.; Funding acquisition, T.B.; Investigation, P.R. and V.R.; Methodology, S.K.; Software, P.R. and V.R.; Supervision, S.K.; Validation, P.R. and V.R.; Writing—original draft, P.R., V.R. and S.K.; Writing—review & editing, R.D. and T.B.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kadhim, I.J.; Premaratne, P.; Vial, P.J.; Halloran, B. Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing* **2019**, *335*, 299–326. [CrossRef]
2. Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Comput. Sci. Rev.* **2018**, *27*, 45–60. [CrossRef]
3. Arul Murugan, C.; KarthigaiKumar, P. Survey on image encryption schemes, bio cryptography and efficient encryption algorithms. *Mob. Netw. Appl.* **2018**, 1–6. [CrossRef]
4. Kozioł, F.; Borowik, G.; Woźniak, M.; Chaczko, Z. Toward dynamic signal coding for safe communication technology. In Proceedings of the Asia-Pacific Conference on Computer-Aided System Engineering, APCASE, Washington, DC, USA, 14 July 2015; pp. 246–251. [CrossRef]
5. Khalifa, N.; Filali, R.L.; Benrejeb, M. A Fast Selective Image Encryption Using Discrete Wavelet Transform and Chaotic Systems Synchronization. *Inf. Technol. Control.* **2016**, *45*, 235–242. [CrossRef]
6. Askar, S.S.; Karawia, A.A.; Al-Khedhairi, A.; Al-Ammar, F.S. An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps. *Entropy* **2019**, *21*, 44. [CrossRef]
7. Ballesteros, D.M.; Peña, J.; Renza, D. A Novel Image Encryption Scheme Based on Collatz Conjecture. *Entropy* **2018**, *20*, 901. [CrossRef]
8. Fan, C.; Ding, Q. A Novel Image Encryption Scheme Based on Self-Synchronous Chaotic Stream Cipher and Wavelet Transform. *Entropy* **2018**, *20*, 445. [CrossRef]
9. Hanis, S.; Amutha, R. Double image compression and encryption scheme using logistic mapped convolution and cellular automata. *Multimed. Tools Appl.* **2018**, *77*, 6897–6912. [CrossRef]
10. Huang, L.; Cai, S.; Xiao, M.; Xiong, X. A Simple Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion. *Entropy* **2018**, *20*, 535. [CrossRef]
11. Liu, H.; Wen, F.; Kadir, A. Construction of a new 2D chebyshev-sine map and its application to color image encryption. *Multimed. Tools Appl.* **2019**, *78*, 15997–16010. [CrossRef]
12. Huang, X.; Ye, G. An Image Encryption Algorithm Based on Time-Delay and Random Insertion. *Entropy* **2018**, *20*, 974. [CrossRef]
13. Li, S.; Ding, W.; Yin, B.; Zhang, T.; Ma, Y. A Novel Delay Linear Coupling Logistics Map Model for Color Image Encryption. *Entropy* **2018**, *20*, 463. [CrossRef]
14. Li, T.; Shi, J.; Li, X.; Wu, J.; Pan, F. Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes. *Entropy* **2019**, *21*, 319. [CrossRef]

15. Liu, X.; Xiao, D.; Liu, C. Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation. *Entropy* **2018**, *20*, 867. [CrossRef]
16. Mondal, B.; Kumar, P.; Singh, S. A chaotic permutation and diffusion based image encryption algorithm for secure communications. *Multimed. Tools Appl.* **2018**, *77*, 31177–31198. [CrossRef]
17. Sreelaja, N.K.; Vijayalakshmi Pai, G.A. Stream cipher for binary image encryption using ant colony optimization based key generation. *Appl. Soft Comput. J.* **2012**, *12*, 2879–2895. [CrossRef]
18. Stoyanov, B.; Kordov, K. Image Encryption Using Chebyshev Map and Rotation Equation. *Entropy* **2015**, *17*, 2117–2139. [CrossRef]
19. Sun, Y.; Chen, L.; Xu, R.; Kong, R. An image encryption algorithm utilizing Julia sets and Hilbert curves. *PLoS ONE* **2014**, *9*, e84655. [CrossRef]
20. Tong, X.; Liu, Y.; Zhang, M.; Xu, H.; Wang, Z. An Image Encryption Scheme Based on Hyper chaotic Rabinovich and Exponential Chaos Maps. *Entropy* **2015**, *17*, 181–196. [CrossRef]
21. Wang, X.; Zhu, X.; Zhang, Y. An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access* **2018**, *6*, 23733–23746. [CrossRef]
22. Zhu, H.; Zhao, Y.; Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [CrossRef]
23. Huang, X. Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn.* **2012**, *67*, 2411–2417. [CrossRef]
24. Ye, G. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognit. Lett.* **2010**, *31*, 347–354. [CrossRef]
25. Zhu, C.X. A novel image encryption scheme based on improved hyper-chaotic sequences. *Opt. Commun.* **2012**, *285*, 29–37. [CrossRef]
26. Wang, X.-Y.; Yang, L.; Liu, R.; Kadir, A. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn.* **2010**, *62*, 615–621. [CrossRef]
27. Zhang, Y.; Xiao, D. An image encryption scheme based on rotationmatrix bit-level permutation and block diffusion. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 74–82. [CrossRef]
28. Zhang, Y.; Xiao, D. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Opt. Lasers Eng.* **2013**, *51*, 472–480. [CrossRef]
29. Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. *Nonlinear Dyn.* **2017**, *87*, 127–133. [CrossRef]
30. Wu, X.; Zhu, B.; Hu, Y.; Ran, Y. A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. *IEEE Access* **2017**, *5*, 6429–6436.
31. Li, C.; Lin, D.; Lü, J. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimed.* **2017**, *24*, 64–71. [CrossRef]
32. Li, C.; Liu, Y.; Xie, T.; Chen, M.Z.Q. Breaking a novel image encryption scheme based on improved hyperchaotic sequences. *Nonlinear Dyn.* **2013**, *73*, 2083–2089. [CrossRef]
33. Guo, J.; Zhang, F. An equivalent key attack on an image cryptosystem. *Acta Electron. Sin.* **2010**, *38*, 781–785.
34. Zhang, Y.-Q.; Wang, X.-Y. A new image encryption algorithm based on non-adjacent coupled map lattices. *Appl. Soft. Comput.* **2015**, *26*, 10–20. [CrossRef]
35. Sam, I.S.; Devaraj, P.; Bhuvaneswaran, R.S. An intertwining chaotic maps based image encryption scheme. *Nonlinear Dyn.* **2012**, *69*, 1995–2007.
36. Wang, X.; Luan, D.; Bao, X. Cryptanalysis of an image encryption algorithm using Chebyshev generator. *Digit. Signal Process.* **2014**, *25*, 244–247. [CrossRef]
37. Wang, X.; Teng, L.; Qin, X. A novel colour image encryption algorithm based on chaos. *Signal Process.* **2012**, *92*, 1101–1108. [CrossRef]
38. Chen, J.; Zhu, Z.; Fu, C.; Zhang, L.; Zhang, Y. An efficient image encryption scheme using lookup table-based confusion and diffusion. *Nonlinear Dyn.* **2015**, *81*, 1151–1166. [CrossRef]
39. Liu, R. New binary image encryption algorithm based on combination of confusion and diffusion. *J. Chem. Pharm. Res.* **2014**, *6*, 621–629.
40. Murugan, B.; Nanjappa Gounder, A.G. Image encryption scheme based on block-based confusion and multiple levels of diffusion. *IET Comput. Vis.* **2016**, *10*, 593–602. [CrossRef]
41. Praveenkumar, P.; Amirtharajan, R.; Thenmozhi, K.; Rayappan, J.B.B. Fusion of confusion and diffusion: A novel image encryption approach. *Telecommun. Syst.* **2017**, *65*, 65–78. [CrossRef]

42. Sinha, R.K.; Sahu, S.S. Secure image encryption based on improved bat optimized piecewise linear chaotic map through integrated permutation-confusion and double diffusion. *J. Intell. Fuzzy Syst.* **2018**, *35*, 1567–1578. [CrossRef]
43. Zhang, W.; Wong, K.; Yu, H.; Zhu, Z. An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. *Opt. Commun.* **2012**, *285*, 2343–2354. [CrossRef]
44. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dyn.* **2017**, *87*, 407–425. [CrossRef]
45. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2014**, *97*, 172–182. [CrossRef]
46. Arroyo, D.; Alvarez, G.; Fernandez, V. On the inadequacy of the logistic map for cryptographic applications. *arXiv* **2008**, arXiv:0805.4355.
47. Naseer, Y.; Shah, D.; Shah, T. A Novel Approach to improve multimedia security utilizing 3D Mixed Chaotic map. *Microprocess. Microsyst.* **2019**, *65*, 1–6. [CrossRef]
48. Ye, G.; Huang, X. An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing* **2017**, *251*, 45–53. [CrossRef]
49. Kumar, M.; Kumar, S.; Budhiraja, R.; Das, M.K.; Singh, S. Intertwining logistic map and Cellular Automata based color image encryption model. In Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, India, 13 March 2016; pp. 618–623.
50. Li, Y.; Li, X.; Jin, X.; Zhao, G.; Ge, S.; Tian, Y.; Wang, Z. An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map. In *Applications and Techniques in Information Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 3–13.
51. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
52. Khade, P.N.; Narnaware, M. 3D chaotic functions for image encryption. *Int. J. Comput. Sci. Issues* **2012**, *9*, 323–328.
53. Kadir, A.; Hamdulla, A.; Guo, W.Q. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Opt.-Int. J. Light Electron Opt.* **2014**, *125*, 1671–1675. [CrossRef]
54. Xu, X.; Feng, J. Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector. In Proceedings of the 2010 IEEE International Conference on Granular Computing, San Jose, CA, USA, 16 August 2010; pp. 556–561. [CrossRef]
55. Ahmad, J.; Larijani, H.; Emmanuel, R.; Mannion, M. Secure Occupancy Monitoring System for IoT Using Lightweight Intertwining Logistic Map. In Proceedings of the 2018 10th Computer Science and Electronic Engineering (CEEC), Essex, UK, 19 September 2018; pp. 208–213.
56. Ahmad, J.; Hwang, S.O. A secure image encryption scheme based on chaotic maps and affine transformation. *Multimed. Tools Appl.* **2016**, *75*, 13951–13976. [CrossRef]
57. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. *J. Sel. Areas Telecommun.* **2011**, *1*, 31–38.
58. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25. [CrossRef]
59. Wang, X.Y.; Zhang, Y.Q.; Bao, X.M. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **2015**, *73*, 53–61. [CrossRef]
60. Liu, H.J.; Wang, X.Y. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [CrossRef]
61. Hussain, I.; Shah, T.; Gondal, M.A. Image encryption algorithm based on PGL (2, GF (28)) S-boxes and TD-ERCS chaotic sequence. *Nonlinear Dyn.* **2012**, *70*, 181–187. [CrossRef]
62. Wang., X.Y.; Zhang, H.L. A color image encryption with heterogeneous bit-permutation and correlated chaos. *Opt. Commun.* **2015**, *342*, 51–60. [CrossRef]
63. Askar, S.S.; Karawia, A.A.; Alammar, F.S. Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map. *IET Image Process.* **2018**, *12*, 158–167. [CrossRef]
64. Tang, Z.; Song, J.; Zhang, X.; Sun, R. Multiple-image encryption with bit-plane decomposition and chaotic maps. *Opt. Lasers Eng.* **2016**, *80*, 1–11. [CrossRef]

65. Zhang, X.; Wang, X. Multiple-image encryption algorithm based on mixed image element and chaos. *Comput. Electr. Eng.* **2017**, *62*, 401–413. [CrossRef]
66. Karawia, A. Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy* **2018**, *20*, 801. [CrossRef]
67. Rukhin, A.L.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application*; NIST Special Publication 800-22; Revision 1a (Revised: April 2010); Lawrence, E.B., III, Ed.; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010. Available online: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic (accessed on 2 July 2019).