sensors

MDPI

Article

An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices

Shamsa Kanwal [1], Saba Inam [1], Mohamed Tahar Ben Othman [2,*], Ayesha Waqar [1], Muhammad Ibrahim [3,4,*], Fariha Nawaz [1], Zainab Nawaz [1] and Habib Hamam [5,6,7,8]

[1] Department of Mathematical Sciences, Faculty of Science and Technology, Fatima Jinnah Women University, The Mall, Rawalpindi 46000, Pakistan; shamsa.kanwal@fjwu.edu.pk (S.K.); saba_inam@hotmail.com (S.I.); ayeshakianee3@gmail.com (A.W.); farihasatti1996@gmail.com (F.N.); zainimath1001@gmail.com (Z.N.)
[2] Department of Computer Science, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[3] Department of Information Technology, University of Haripur, Haripur 22620, Pakistan
[4] Big Data Research Center, Jeju National University, Jeju-si 63243, Korea
[5] Faculty of Engineering, Université de Moncton, Moncton, NB E1A 3E9, Canada; habib.hamam@umoncton.ca
[6] Spectrum of Knowledge Production & Skills Development, Sfax 3027, Tunisia
[7] Department of Electrical and Electronic Engineering Science, School of Electrical Engineering, University of Johannesburg, Johannesburg 2006, South Africa
[8] International Institute of Technology and Management, Commune d'Akanda, Libreville 1989, Gabon
* Correspondence: maathaman@qu.edu.sa (M.T.B.O.); ibrahimayar@uoh.edu.pk or ibrahimmayar@jejunu.ac.kr (M.I.)

Abstract: In the last decade, the communication of images through the internet has increased. Due to the growing demands for data transfer through images, protection of data and safe communication is very important. For this purpose, many encryption techniques have been designed and developed. New and secured encryption schemes based on chaos theory have introduced methods for secure as well as fast communication. A modified image encryption process is proposed in this work with chaotic maps and orthogonal matrix in Hill cipher. Image encryption involves three phases. In the first phase, a chaotic Henon map is used for permuting the digital image. In the second phase, a Hill cipher is used whose encryption key is generated by an orthogonal matrix which further is produced from the equation of the plane. In the third phase, a sequence is generated by a chaotic tent map which is later XORed. Chaotic maps play an important role in the encryption process. To deal with the issues of fast and highly secured image processing, the prominent properties of non-periodical movement and non-convergence of chaotic theory play an important role. The proposed scheme is resistant to different attacks on the cipher image. Different tests have been applied to evaluate the proposed technique. The results of the tests such as key space analysis, key sensitivity analysis, and information entropy, histogram correlation of the adjacent pixels, number of pixel change rate (NPCR), peak signal to noise ratio (PSNR), and unified average changing intensity (UCAI) showed that our proposed scheme is an efficient encryption technique. The proposed approach is also compared with some state-of-the-art image encryption techniques. In the view of statistical analysis, we claim that our proposed encryption algorithm is secured.

Keywords: tent chaotic map; Hill cipher; orthogonal matrix; Henon map; peak signal to noise ratio (PSNR); number of pixel change rate (NPCR); unified average changing intensity (UACI); image encryption; decryption

check for updates

Citation: Kanwal, S.; Inam, S.; Othman, M.T.B.; Waqar, A.; Ibrahim, M.; Nawaz, F.; Nawaz, Z.; Hamam, H. An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices. *Sensors* **2022**, *22*, 4359. https://doi.org/10.3390/s22124359

Academic Editors: Stefania Perri and Guangtao Zhai

Received: 21 February 2022
Accepted: 20 April 2022
Published: 8 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

In the past few years, the use of digital technology has increased. Due to the frequent flow of digital data transmission over electronic media, the security of data is ultimate. Several functions, such as an armed forces database, secret cinematographic conferencing, health systems, digital payments, etc., require a fast, reliable security system to transmit

data. Considering some characteristic highlights of pictures, such as mass information limit and high information repetition, the encryption of pictures is not quite the same as that of writings; consequently, it is hard to deal with them by conventional encryption strategies. Traditional ciphers such as AES [1] and DES [2] are not suitable for fast image encryption, as the ciphers consume huge computing power and high processing time. To fulfill the requirements of security of data and fast computation, many encryption techniques have been developed. Among all encryption techniques, chaotic theory-based encryption techniques are most suitable for image encryption, as they specify high speed, high security, the complexity of the process, and high computational power. Chaotic maps have several properties, including non-periodicity, sensitivity to initial conditions, and property of randomness. These are used for the confusion and diffusion process of data in image encryption. Chaotic maps boost the sanctuary of information.

Numerous encryption schemes of images have been proposed in the past years that used chaotic maps. Matthews in 1989 [3] proposed a non-linear iterative expression that tends to generate a chaotic sequence. He developed an encryption technique using chaotic logistic maps. Bourbakis and Alexopoulos [4] introduced an image encryption scheme that uses the language of SCAN for encryption in 1992. The symmetric image encryption technique was introduced in [5] by using a two-dimensional standard baker map. Scharinger [6] developed a Kolmogorov flow-based chaotic image encryption scheme that uses a register shift pseudo-random generator, in which permutation is performed through a controlled key chaotic system by taking the whole image as a single block. Yen and Guo [7] introduced an encryption technique named BRIE that is based on the chaotic logistic map. The encryption technique BRIE works by recirculating the pixels bitwise. The BRIE secret key contains an initial condition of the chaotic logistic map and two integers. Yen and Guo [8] introduced an encryption technique named CKBA (Chaotic Key Based Algorithm) that works in a way in which a binary sequence is considered as a key that is generated by using a chaotic system. The image pixels are rearranged according to the created parallel arrangement and afterward XORed and XNORed with the chosen key. Recently, Li [9] has introduced a video encryption scheme known as CVES (Chaotic Video Encryption Scheme) based on multiple digital chaotic systems. Pseudo-random signals are generated from $2n$ chaotic maps to cover the video and to execute pseudo-random permutation of the hidden video.

The current work is encouraged by the theme and functions used in the existing literature. A novel image encryption technique has been introduced in this work by combining Henon map and tent logistic maps with Hill cipher which exhibits tight security. The proposed scheme uses chaotic maps to generate a sequence for permutations and bitwise XOR and Hill cipher for the substitution phase. For higher security levels, the key for Hill cipher is generated by the orthogonal matrix from the equation of a plane. The proposed scheme is executed and experimented with considering color images. Security tests such as information entropy, UACI, PSNR, correlation factors analysis, and NPCR are used to assess and evaluate the performance of the proposed approach. The proposed approach is compared with the state-of-the-art approaches.

The rest of the paper is outlined as follows: Section 2 consists of the mathematical preliminaries. Section 3 describes the process of image encryption and decryption algorithms. Section 4 gives the specification of implementation results and performance evaluation of encryption and decryption algorithms. Section 5 summarizes the whole work of the presented scheme.

2. Mathematical Preliminaries

Our proposed scheme is composed of the following mathematical concepts: Henon map, orthogonal matrix, and chaotic tent map. Chaotic maps are simple maps that are sensitive to their starting conditions. A minor change in the values of starting conditions can alter the results at a large scale.

2.1. Henon Map

The Henon map was introduced by Michel Henon in 1969. It is a discrete dynamic map that exhibits chaotic behavior, as it is sensitive to its initial conditions. It is defined as:

$$X(n+1) = 1 - aX(n)^2 + Y(n) \tag{1}$$

$$Y(n+1) = b(X(n)). \tag{2}$$

The vigorous behavior of a chaotic system is dependent on the values of parameters a, b that are called control parameters. The parameters and conditions of the Henon map are as follows:

1. $X(0)$, where $X(0)$ is the initial value.
2. $a \in [0, 1)$, where a is the control parameters.
3. $K_1 = (a, X(0))$ is the secret key of the permutation phase

It contains many effective properties, such as Lyapunov exponent, randomness of behavior, and uniform non-variation of density variable. Due to these characteristics, the Henon map is strongly recommended for applications in the field of cryptography.

This structure is chaotic for $a = 1.4, X(0) = 0.766, b = 0.3, Y(0) = 0.3432$. Eventually, a small change in the values of parameters can lead to the different behavior of a system.

2.2. Chaotic Tent Map (CTM)

The chaotic tent map is a dynamic map with β as a real valued function. It is a piece-wise linear and continuous map having a unique maximum in the chaotic region for analyzing density and power spectrum. A chaotic tent map is defined as:

$$\phi(n+1) = \begin{cases} \frac{\beta}{2} \times \phi(n); \phi(n) < 0.5 \\ \frac{\beta}{2} \times \{1 - \phi(n)\}; \phi(n) \geq 0.5 \end{cases} \tag{3}$$

The conditions and the parameter of CTM are $\phi(0) \in (0, 1)$, which is the initial condition, and $\beta \in (0, 4)$, where β is the control bifurcation parameter. We have used the values $\phi(0) = 0.66$ and $\beta = 3.78$. Figure 1 shows the bifurcation diagram of a chaotic tent map.

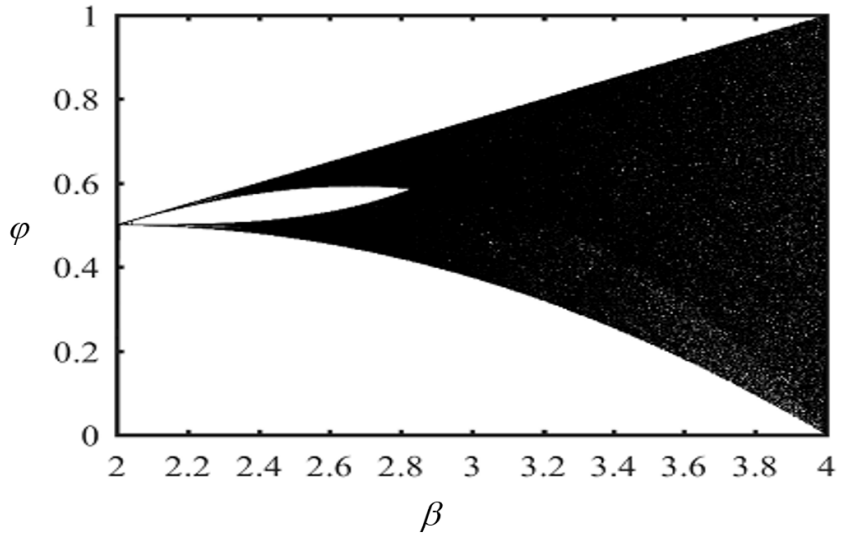


Figure 1. Bifurcation diagram of chaotic tent map.

As shown in Figure 1, by analyzing the dynamic behavior of CTM, it is noted that it has a good enough range of chaos. When the bifurcation phenomenon occurs, the system is indeed chaotic. Due to its sensitivity to initial value, intrinsic randomness,

and a good chaotic parameter interval, the CTM is used for developing chaotic image encryption algorithms.

2.3. Orthogonal Matrix

A matrix A is said to be orthogonal if A has the following property:

$$A^t A = I \Rightarrow A^t = A^{-1},$$

where A^t is the transpose of A, and I is the identity matrix.

3. Image Encryption and Decryption Algorithms

The whole scheme of image encryption consists of three phases. The first phase uses the Henon map to generate a sequence for permuting the pixels of an image. In the second phase, the permuted pixels are multiplied with the key invertible matrix, which is produced by a secret orthogonal matrix. The last phase consists of a process of confusion in such a way that a new sequence which is generated from a new chaotic tent map is XORed with previously generated results. The complexity of the scheme helps in resisting attacks from the attackers. Figure 2 depicts the workflow of our proposed encryption technique.

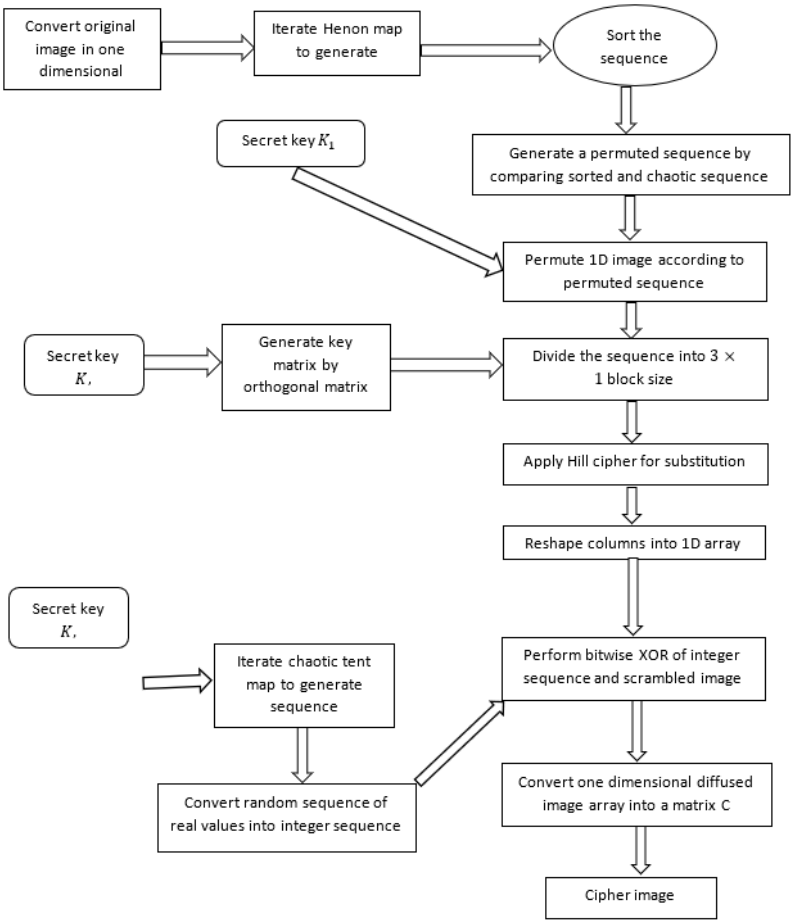


Figure 2. Workflow of proposed encryption scheme.

3.1. Permutation Process

The permutation phase of our proposed cryptosystem consists of permuting the positions of the pixels of an original image as shown in Algorithm 1. In the first phase of our scheme, to permute the pixels' positions, the Henon map is used with the key K_1. By using K_1, the Henon map is reiterated to produce a sequence. The produced chaotic sequence is arranged in ascending order. The permuted sequence is obtained by comparing

the arrangements of chaotic and sorted sequences. The one-dimensional array of the original image is obtained by using the permuted sequence.

Algorithm 1. Pixel Permutation

Input: Secret key $K_1 = (a, X(0))$ Henon map (1), Color image I.
Output: Array L of permuted pixels of an image I.

1. Take the original image I, which is stored in an array Y with size $M = P \times Q \times 3$, where P indicates the number of rows and Q indicates the number of columns of the image matrix I.
2. Use the key K_1 with Henon map (1) to produce a sequence. Generate the chaotic sequence $H = \{h_1, h_2, \ldots, h_M\}$ and sort it in ascending order, the resulting sequence is $\underline{H} = \{\underline{h}_1, \underline{h}_2, \ldots, \underline{h}_M\}$.
3. Compute the permutation vector J by noting the positions of sequence terms of H in $\underline{H}$ and write down the transformed positions $J = \{j_1, j_2, \ldots, j_M\}$.
4. Use J to permute the positions of elements of an array Y to get L.

For the image selection, the general consideration is to take any size of $P \times Q \times 3$ pixels colored image, where P and Q are the height and width, respectively. The size of the encrypted image would be the same as that of the original image.

3.2. Substitution Phase Using Hill Cipher with Orthogonal Matrix

The second phase is the substitution phase as shown in Algorithm 2. In this phase, the secret key K_2 is generated by the orthogonal matrix generated by an equation of a plane. The secret key K_2 is used for Hill cipher in the substitution algorithm given I Algorithm 3. The permuted image is divided into $\frac{M}{3}$ sub-blocks. These $\frac{M}{3}$ sub-blocks are one-by-one multiplied by the generated 3×3 orthogonal matrix. The result is arranged in one-dimensional array E.

Algorithm 2 presents the generation of a key orthogonal matrix from the equation of plane [10].

Algorithm 2. Key Generation of Permutation Process

Input: Equation of plane $ax + by + cz = d, a, b, c, d \in \Re$.
Output: Orthogonal matrix K_2.

1. Let the orthogonal line O be spanned by the unit vector t

$$t = \frac{(a, b, c)}{\sqrt{a^2 + b^2 + c^2}},$$

from the expression $Z_w = w - 2t\langle w, t\rangle$, where $\langle w, t\rangle$ is the inner product of w and t.

2. For $w = \{w_1, w_2, w_3, \ldots, w_m\} \in R^m$ be the basis of O. The basis vectors for $m = 3$ are

$w_1 = [w_{11}, w_{12}, w_{13}] = [1, 0, 0] w_2 = [w_{21}, w_{22}, w_{23}] = [0, 1, 0] w_3 = [w_{31}, w_{32}, w_{33}]$ $= [0, 0, 1]$.

3. The orthogonal key matrix K_2 will be

$$K_2 = \begin{bmatrix} z_{w11} & z_{w12} & z_{w13} \\ z_{w21} & z_{w22} & z_{w23} \\ z_{w31} & z_{w32} & z_{w33} \end{bmatrix}.$$

Algorithm 3. Hill Cipher with Orthogonal Matrix

Input: Permuted image array L, K_2
Output: An array E of order M.

1. Use the given equation of a plane to generate the key orthogonal matrix. K_2 will be the orthogonal key matrix under mod 256 of order 3×3.
2. Making blocks L_r
   (i) Transform one-dimensional array into block vectors of size 3×1. The rth block is L_r, where
   $$r = 1, 2, 3, \ldots, \frac{M}{3}$$
   (ii) Hill cipher is implemented by using the following formula
   $$A^r = K_2 \times L_r (mod 256).$$
   (iii) Write all $A_r's$ in one-dimensional array again such that
   $$E = \left\{ A^1, A^2, A^3, \ldots, A^{\frac{M}{3}} \right\}.$$

3.3. Diffusion Phase

In the last phase, the diffusion of pixels take place as shown in Algorithm 4. In this phase, by using K_3 key, a sequence is produced by iterating a chaotic tent map (CTM) (3), and then the values of the sequence are transformed into an integer sequence by using Equation (4). The one-dimensional array is correspondingly XORed bitwise with the integer sequence. A matrix of order $P \times Q \times 3$ is obtained by rearranging the one-dimensional array and from the matrix of cipher image.

Algorithm 4. Pixel Diffusion

Input: The Array E, sec ret key $K_3 = (\phi(0), \beta)$, CTM (3)
Output: Encrypted image C'.

1. Generate a sequence $W = \{W_1, W_2, \ldots, W_M\}$ with key K_3 and CTM (3).
2. A sequence W is transformed into an integer sequence by the given Equation (4)
   $$P_K = floor\Big(mod(W_K \times 10^{14}, 256\Big)) \quad (4)$$
3. Mix each element of E with the parallel element of P_K and a bitwise XORing is performed to make an array
   $$C_j = P_j \oplus E_j \oplus C_{j-1}, j = 1, 2, \ldots, M.$$
4. Change the array C_j in the matrix form named as C' of the size of
   $$M = P \times Q \times 3.$$

3.4. Image Decryption Process

The process of image decryption is carried out to obtain the original image by using the reverse encryption algorithm. The proposed decryption procedure also includes three phases as shown in Algorithm 5. In the first phase, the sequence generated from the chaotic tent map (CTM) is XORed with the key K_3. The Hill cipher is used with the invertible matrix by using K_2. A random sequence is generated from the Henon map and by using key K_1 inverse permutation is obtained. To converse the permutation, the inverse permutation is employed. The subsequent array is transformed into an image form to obtain the original image.

Algorithm 5. Pixel Decryption Process

Input: Cipher image C, Secret keys K_1, K_2, K_3, Henon Map (1), CTM (3).
Output: Colored image I

1. Place the matrix C' of the cipher image in an array of order $M = P \times Q \times 3$.
2. Generate a sequence W of an order $M = P \times Q \times 3$ by using key K_3 and XOR it with the integer sequence generated from the relation (4).
3. Each element of C' is pre-decrypted as:

$$E_j = C_j \oplus P_j \oplus E_{j-1}\ j = 1, 2, 3, \ldots, M$$

4. Generate an orthogonal matrix K_2 as in Algorithm 2.
5. Transform the one-dimensional array E in block vectors L_r of size 3×1.
6. Hill cipher is executed by using the formula

$$A_r = K_2 \times L_r (mod 256)$$

7. Change all $A_r's$ in one dimensional array L.
8. Use the sec ret key K_1, iterate the Henon map (1) to generate a sequence H and obtain $\underline{H}$ by cataloguing H in ascending order.
9. Obtain the permutation array by inverse transformation position J^{-1}.
10. Using J^{-1} on L to obtain Y
11. Rewrite Y in a matrix formation of order M to get image I

4. Analytical Results and Performance Evaluation

In this section, proposed algorithms are assessed by examining the statistical and differential parameters of the tests. In order to implement and evaluate our proposed encryption scheme, we have used Matlab 2018a. The sample images are downloaded from the USC-SIPI database [11]. The algorithms of permutation of pixels, mixing of the key orthogonal matrix with Hill cipher, and diffusion of a pixel are implemented to obtain the encrypted image and the original image back by using decryption algorithm. The standard colored images of Lena with pixel values of length (256×256), are chosen for evaluating our proposed scheme. We performed the encryption using $K_1 = (0.766,\ 0.3432)$, $K_3 = (0.7666,\ 3.999)$. The sample image of Lena is chosen to compare our performance of our proposed scheme against the other chosen schemes. The input and output of the sample image Lena obtained from encryption and decryption algorithms are shown in Figure 3.

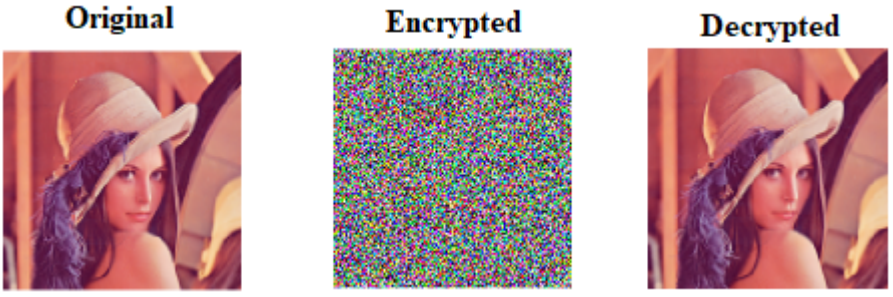


Figure 3. Original, encrypted, and decrypted image of Lena (256×256).

4.1. Statistical Analysis of Histogram

Analysis of histogram is the groundbreaking assessment of image pixels. It should be distinctive from the original and encoded picture. The pixels of the plain image are non-uniform and variant at every single moment. It is clearly visible that the histogram of the cipher image is fairly uniform. It is evident that no information is leaked from the cipher image of the dispersal of pixels in the original image. Figure 4 shows the three components, red, green, and blue histogram, of the coded cipher image. The histogram of

cipher images is moderately uniform, as seen in Figure 4. There is no evidence about the distribution of pixels in the original image.

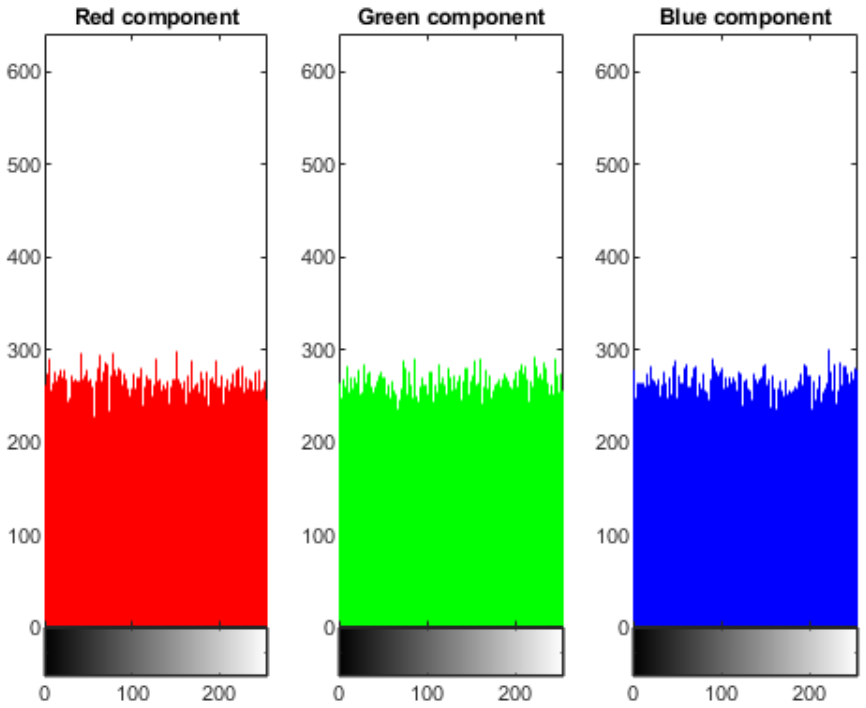


Figure 4. Histogram of Encrypted Image of Lena (256 × 256).

4.2. Histogram Variance Analysis

The variances of the first and encrypted picture histograms are estimated to decide the picture pixel consistency. The pictures have more noteworthy pixel consistency when the changes are more modest. It is estimated by

$$var(X_i) = \frac{1}{r^2}\sum_{m=1}^{r}\sum_{n=1}^{r}\frac{(x_m - x_n)^2}{2} \quad (5)$$

where $X_i = \{x_1, x_2, x_3, x_4, \ldots, x_{256}\}$, m and n signify the grayscale pixel esteems and x_m and x_n signify the number of pixels for every one of the grayscale pixel esteems m and n, individually. The suggested technique exhibits less average variance than the compared approach of [12,13], as shown in Table 1.

Table 1. Comparison of Lena image histogram variance results.

Image	[12]	[13]	Proposed
Lena 256	982.5703	1071.0	980.50

4.3. Chi-Square Test Analysis

The consistency in the histograms of the encoded pictures can likewise be advocated through chi-square test investigation. The low chi-square worth demonstrates high consistency in encoded picture histograms. It is estimated by

$$\chi_t{}^2 = \sum_{j=0}^{255}\frac{(O_j - E_j)^2}{E_j} \quad (6)$$

where the observed frequency of j is O_j and the expected frequency of j is E_j; expected frequency is expressed as

$$E_j = \frac{\text{image size}}{256}$$

Table 2 illustrates that the hypothesis is accepted at both 5% and 1% levels of significance for the proposed technique. In addition, there exists uniformity of the grayscale in the histograms of encrypted images of the proposed and Refs. [12,13] algorithms. It is also depicted that the proposed scheme has a low chi-square value as compared to the Refs. [12,13] techniques, which exhibits the efficiency of our suggested method.

Table 2. Comparison of chi-square test (χ_t^2 test) results.

Image	Ref. [12]	Ref. [13]	Proposed	Testing Results	
				$\chi^2_{255,\ 0.05} = 293.2478$	$\chi^2_{255,\ 0.01} = 310.457$
Lena 256	245.6426	267.7480	255.79	pass	pass

4.4. Correlation Analysis of Adjacent Pixels

The correlation coefficient shows resemblance along the horizontal, vertical, and diagonal direction of nearby pixels. Correlation C_r is used to test the confusion and diffusion process between the plain image and the coded image. It can be calculated by using the formula given in the Equation (7).

$$C_r = \frac{n(\sum_{t=1}^{n} x_t y_t - \sum_{t=1}^{n} x_t \sum_{t=1}^{n} y_t)}{(n\sum_{t=1}^{n}(x_t)^2 - (\sum_{t=1}^{n} x_t)^2))(n\sum_{t=1}^{n} y_t)^2 - (\sum_{t=1}^{n} y_t)^2)} \quad (7)$$

where n is the total pixel value chosen to calculate the coefficient and x_t and y_t are the values of two neighboring pixels. The highest correlation factor value is 1, which shows the existence of a high correlation coefficient among the adjacent pixels. The proposed encryption technique must encrypt with low correlation coefficients which are approximately equal to zero, such that the attacker could not be able to acquire the useful data. Figures 5 and 6 illustrate the distribution of the original and encrypted image pixels in RGB components.

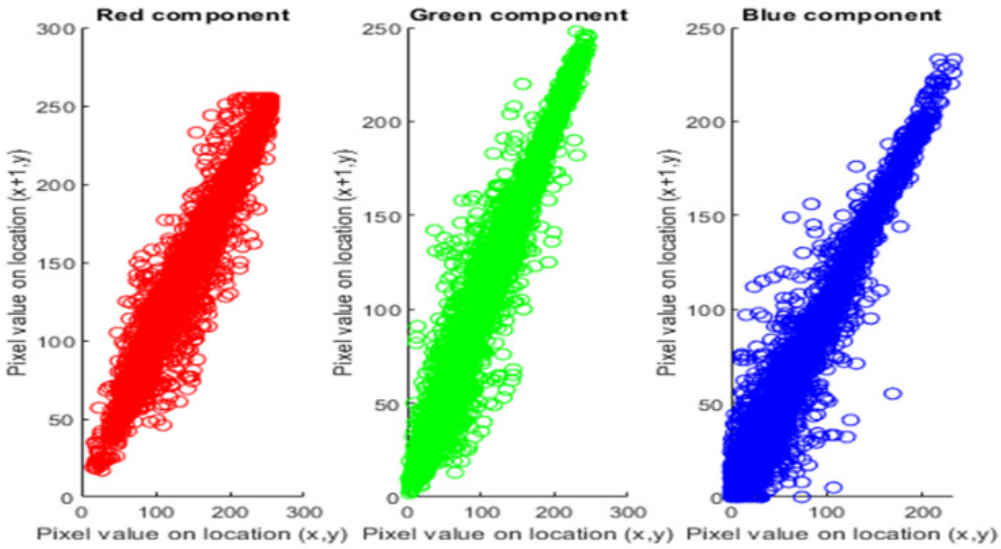


Figure 5. Correlation coefficient of the original color image of Lena (256 × 256 pixels).

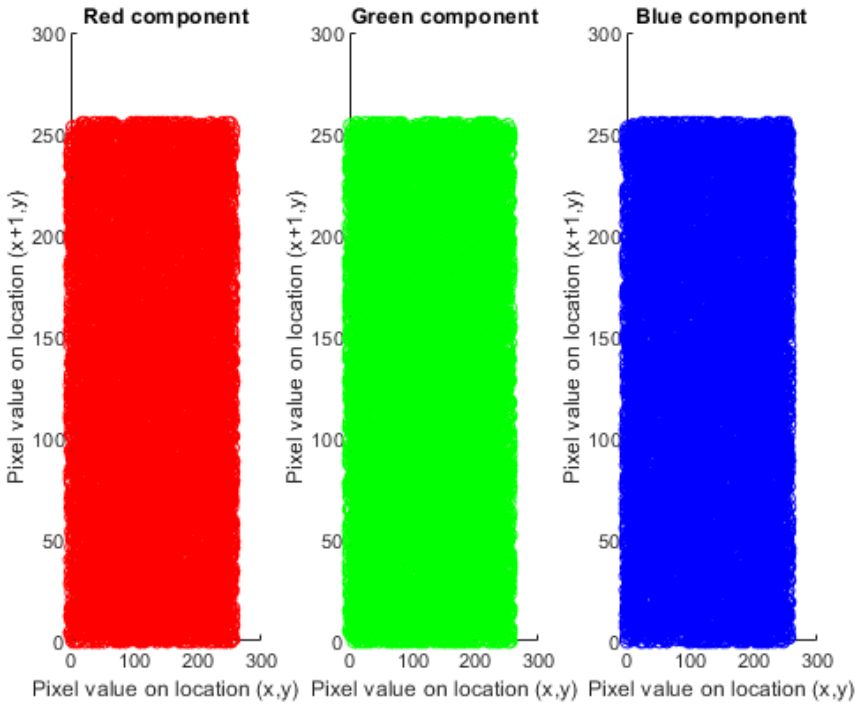


Figure 6. Correlation (row-wise) of the cipher image of Lena 256.

Table 3 show the values of correlation distribution in three directions for the original and cipher image. The values show that in the cipher image the adjacent pixels are almost uncorrelated, as it is closer to zero. The number of random pixels is 16,430 pairs of pixels, and the comparison is carried out on 4500 pairs of neighboring pixels at random.

Table 3. Lena 256 correlation coefficient values.

Direction\Color	Red		Green		Blue	
	Original	**Cipher**	**Original**	**Cipher**	**Original**	**Cipher**
Horizontal	0.9794	0.0004	0.9806	−0.0013	0.9604	0.0073
Vertical	0.9574	−0.0028	0.9593	−0.0062	0.9237	−0.0014
Diagonal	0.9363	−0.0048	0.9400	−0.0002	0.8898	0.0064

4.5. Mean Square Error Analysis

The mean square error (MSE) is used to measure the accuracy and variation among two images. A high value of MSE corresponds to a large difference between the ciphered and plain images. The MSE values are determined by the formulas given in expressions (8).

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} \left(I_P(i,j) - I_D(i,j) \right)^2 \tag{8}$$

where m represents the number of rows and n represents the number of columns of the image. I_P and I_D represent the plain image and the cipher image, respectively. The MSE of the proposed encryption scheme of the image and its comparison with some schemes are illustrated in Table 4. It can be seen from the results that the proposed scheme has a larger MSE value than the methods suggested in Refs. [12,13]. We conclude that there is an extensive difference between plain and ciphered images in the proposed algorithm as compared to the Refs. [12,13] techniques.

Table 4. Performance of MSE.

Image Encryption Scheme	MSE
Ref. [12]	7762.6
Ref. [13]	7764.3
Proposed Scheme	8783.6

4.6. Peak Signal to Noise Ratio Analysis

The analysis of PSNR is used to determine the quality of the ciphered image against the plain image. A low value of PSNR corresponds to a large difference between ciphered and plain image. It is analyzed by the formulas given in Equation (9).

$$\text{PSNR} = 10 \cdot log \frac{255^2}{MSE} \tag{9}$$

The value of PSNR for the proposed scheme is 8.6940.

Another sample-colored image of Onion (198 × 135 pixels) has been chosen to apply on our proposed cryptosystem. The entropy value of the onion image is calculated as 7.9975. Figure 7 shows the results of encryption and decryption of sample images. Figures 8 and 9 show the histogram and correlation coefficient of plain and cipher images, respectively. Table 5 illustrates the correlation coefficient values of the sample image of the onion.

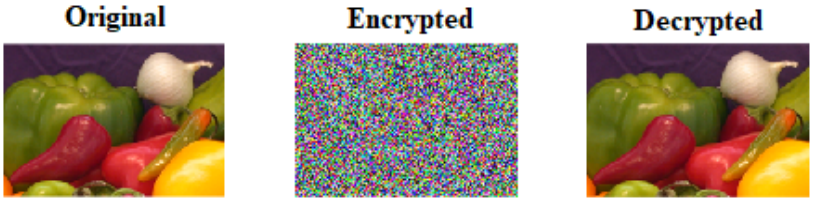


Figure 7. Sample image of onion (colored 198 × 135 pixels).

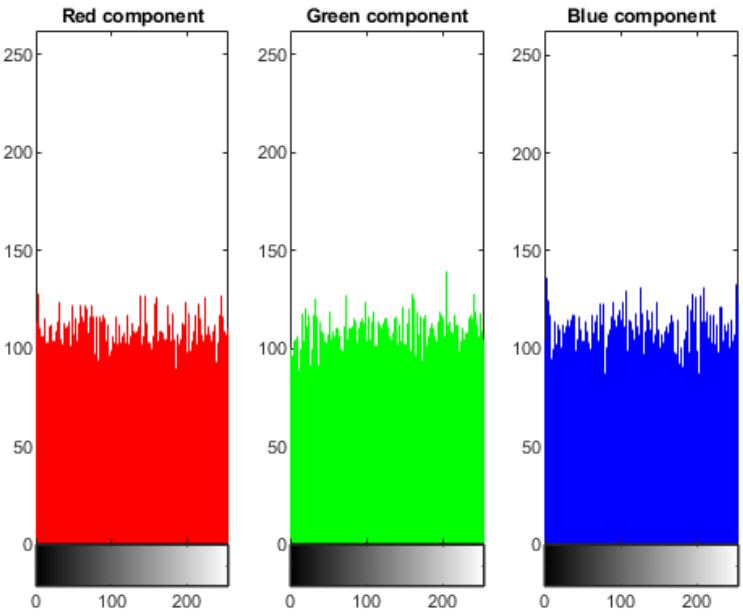


Figure 8. Cipher image histogram analysis of onion (colored 198 × 135 pixels).

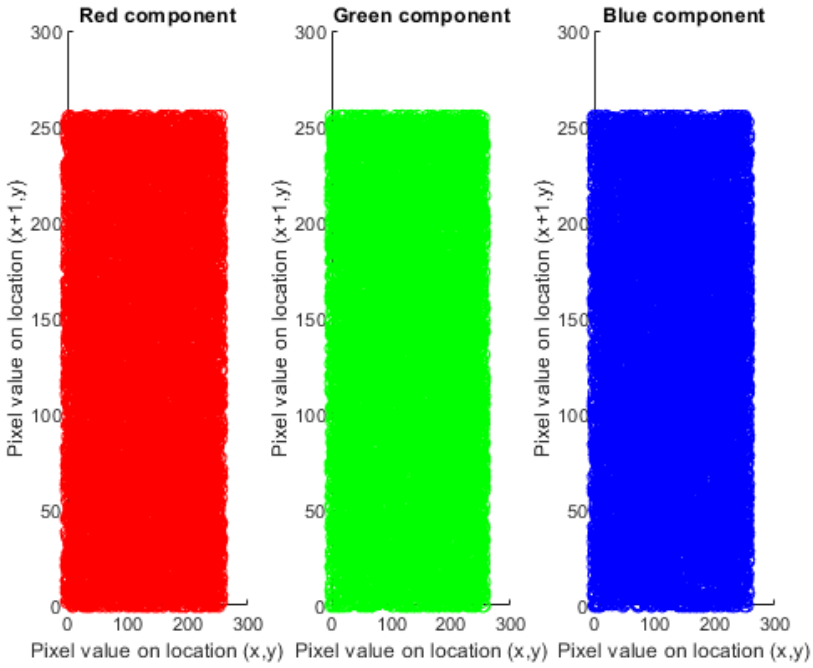


Figure 9. Correlation analysis of color components of onion (colored 198 × 135 pixels) cipher image.

Table 5. Correlation coefficient values of onion (198 × 135) cipher image.

Directions\Colors	Red	Green	Blue
Horizontal	0.0091	−0.0051	0.0095
Vertical	0.0078	−0.0047	0.0093
Diagonal	0.0091	0.0152	−0.0056

4.7. Sensitivity Analysis

In cryptography, plain-text sensitivity analysis is also known as differential evaluation. Two standardized tests of the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are used to observe the original plain image sensitivity against external attacks. The test shows the impact whereby small variation in the plain image causes high alteration in the encrypted images. The more effective cryptosystem is designed when the higher value of NPCR is achieved and will provide security against different attacks. Both indicators can be calculated by using the formulas in Equations (10) and (11) as follows:

$$\text{NPCR} = \frac{\sum_{i,j} K(i,j)}{w \times h} \times 100 \tag{10}$$

$$\text{UACI} = \frac{1}{w \times h}[\sum_{i,j} \frac{|X(i,j) - X'(i,j)|}{255}] \times 100 \tag{11}$$

In Equation (11), w and h represent the width and height of the cipher image, respectively. X denotes cipher image, while X' denotes the change of one pixel in plain image. If $X(i,j) \neq X'(i,j)$, $K(i,j) = 1$; else, $K(i,j) = 0$. It can only be resistant to differential attacks when the values of NPCR and UACI should approach their ideal values. The ideal values of NPCR are 99.61 and UACI is 33.46. We compare the values of NPCR and UACI for the encrypted Lena image in Table 6.

Table 6. Comparison of NPCR and UACI values.

Image Encryption Schemes	NPCR	UACI
Ref. [14]	99.61	33.46
Ref. [15]	99.61	33.48
Ref. [16]	99.59	33.90
Ref. [17]	99.61	33.47
Standard values	99.61	33.46
Proposed scheme	99.61	33.46

It is shown that the present scheme attains peak performance for both values. In this case, the present scheme provides good resistance against "Known plain-text attack" and "Chosen plain-text attack".

4.8. Information Entropy Analysis

Entropy is the measurement of an irregularity of the pixel concentrations in the cipher image. It is used to determine the entropy of information in order to measure the randomness in the cipher image. In the proposed technique, information entropy for the encrypted image g, which is $H(g)$, is evaluated. The measured value of entropy of encrypted image g is given in Equation (12).

$$H(g) = \sum_{i=0}^{255} P(g_i) log_2 \frac{1}{P(g_i)} \tag{12}$$

where g_i is discrete pixel values and P is the probability of these values. In our example of the proposed technique of encrypted image C' with $2N$ as 255, the entropy value is calculated as 7.9992. Table 7 illustrates the comparison of entropy values of different encryption techniques. The calculation of entropy value illustrates that the value of entropy of our encryption algorithm is close to the standard value of entropy that is calculated with Equation (12). It confirms that no information has been lost in our proposed cryptosystem.

Table 7. Comparison of entropy values.

Image Encryption Schemes	Entropy Values
Ref. [14]	7.9990
Ref. [16]	7.9967
Ref. [13]	7.9994
Proposed scheme	7.9992

4.9. Key Space Analysis

Key space analysis is basically analysis of all the possibilities of keys used in the encryption process. The size of the key must be large enough to oppose brute force attacks. With the modern computational techniques, an algorithm can resist exhaustive attacks if the size of key space is larger than 10^{30} [18]. Our proposed image encryption algorithm consists of three different keys. The keys K_1 and K_3 consist of control parameters of Henon and tent maps. By observing the precision of the parameters to be 10^{-15}, the total amount of possibilities to choose the keys could be $(10^{15})^2 \times (10^{15})^2 = (10)^{60} \approx (2)^{240}$. As the size of the key of two algorithms is up to 60, our proposed permutation and confusion process is strong enough to be protected from brute force attack. Since the second key K_2 for substitution phase is generated by an equation of plane $ax + by + cz = d, a, b, c, d \in \Re$, there are infinite possibilities for choosing the four coefficients of a, b, c, d. Consequently, the size of key space for K_2 is also infinite.

4.10. Computational Time Analysis

Consider that the quickest computer can calculate 2^{80} computations in a single second. Thus, in a single year, the wide variety of computations accomplished through the computer is $2^{80} \times 365\ (\text{days}) \times 24\ (\text{h}) \times 60\ (\text{min}) \times 60\ (\text{s})$. As a result, the entirety of $2^{240}/2^{80} \times 365 \times 24 \times 60 \times 60 = 10^{36}$ years is required. This time duration is enough to secure the whole cryptosystem. To face up to the brute force attack in opposition to this encryption algorithm, this computational load is large enough.

4.11. Key Sensitivity Analysis

The secret keys of the scheme are significant for its encryption algorithm. Our proposed encryption algorithm has three keys. In this present technique, the result of the decryption algorithm entirely changes even for a very small variation in any part of the secret key. This means that if we add 0.0000000000000001 to the first key $K_1 = (a, X(0))$, we will not obtain the original image after decryption by using that key. It is clearly observed that any clue or gesture about the original image is not found in the encrypted image. The algorithms of our proposed cryptosystem are highly sensitive to secret keys.

4.12. Cryptanalysis

The cryptanalysts usually mount the chosen-plaintext attack and the chosen-ciphertext attack on a cryptographic technique to break it. By employing these types of attacks, many cryptographic techniques are cracked. We implement these types of attacks and show the resistance of our proposal against them.

4.12.1. Chosen-Plaintext Attack

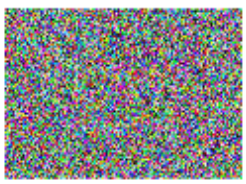
In this scenario of attack, the cryptanalyst has a ciphered image, but the encryption key is unknown. However, he has a plain image P^0 of all-zero (or all-one) and its corresponding ciphered image C^0 obtained with the same unknown key. The cryptanalyst develops the following sub-key extraction for pixel encryption [19].

$$SK^0_{i,j} = C^0_{i,j} \oplus P^0_{i,j} \tag{13}$$

where $P^0_{i,j}$ is a null image in terms of grey values, $C^0_{i,j}$ is its corresponding encrypted variant, and (i, j) is the two-dimensional pixel position. Equation (13) gives a key stream $SK^0_{i,j}$. In trying to obtain the plain image $P_{i,j}$ of the ciphered one $C_{i,j}$, the cryptanalyst makes use of the key stream $SK^0_{i,j}$ as follows.

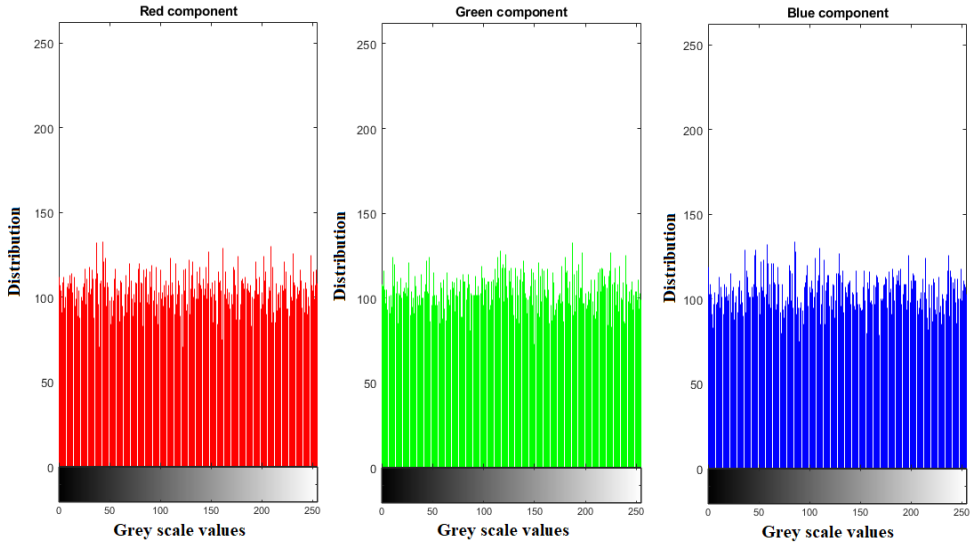
$$P_{i,j} = C_{i,j} \oplus SK^0_{i,j} \tag{14}$$

In Figure 10a, it can be seen that the chosen-plaintext attack on the Lena encrypted image using a null image has failed. The corresponding histograms are given in Figure 10b. It is evident that the chosen-plaintext cannot be mounted in this proposed image encryption procedure. The reason for this failure is that pixel permutation and pixel diffusion phases rely on the techniques which are highly sensitive to insignificant change of a grey value. Therefore, the proposed technique demonstrates a strong resistance to the chosen-plaintext attack.



(**a**)

Figure 10. *Cont.*



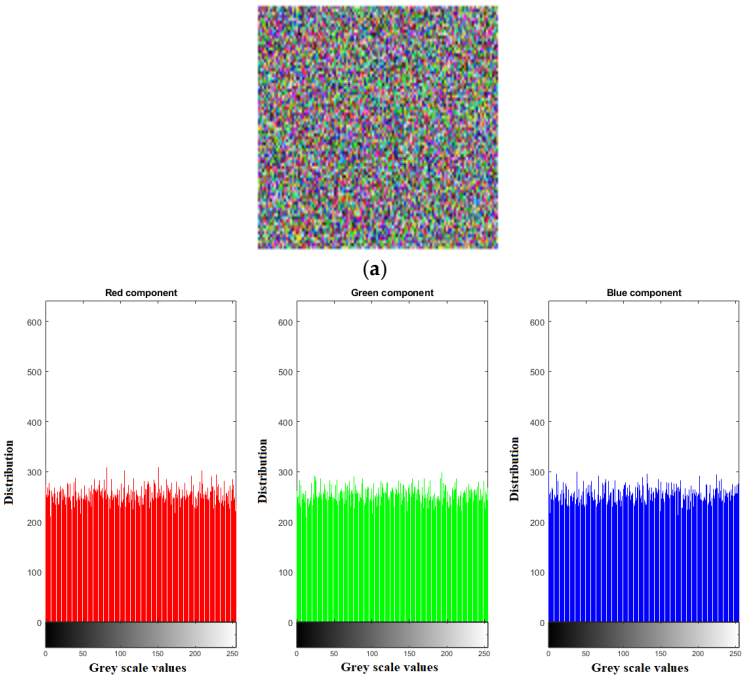
(**b**)

Figure 10. Cryptanalysis (**a**) chosen-plaintext attack of Lena image, (**b**) corresponding image histograms of Lena encrypted image (**a**).

4.12.2. Chosen-Ciphertext Attack

This is another type of attack having no information about the key. Knowing a ciphertext C' of all-one (or all-zero), and its corresponding decrypted variant P', the cryptanalyst tries to determine the key stream $K'_{i,j}$ using Equation (13). Then, the plaintext $P_{i,j}$ would be acquired by Equation (14) [19].

In Figure 11, the chosen-ciphertext attack on the Lena encrypted image with the null-images (all-zero pixel values) is shown. By observing the chosen-ciphertext attack of the Lena image and its corresponding histograms, it is evident that the chosen-ciphertext cannot be mounted in this proposed image encryption procedure.



(**a**)

(**b**)

Figure 11. Cryptanalysis (**a**) chosen-ciphertext attack of Lena image, (**b**) corresponding image histograms of Lena encrypted image (**a**).

5. Conclusions

In our paper, we proposed a novel image encryption technique using chaotic maps. The proposed technique first uses a Henon chaotic map to create a permutation phase. For substitution purposes, a Hill cipher is used whose key is generated from an orthogonal matrix by considering the equation of a plane. Then, in the next diffusion phase, a tent chaotic map is employed to obtain a sequence, and each pixel value is bitwise XORed with the values of the obtained sequence. The proposed algorithm works in two phases that are: the confusion phase is carried by Henon map and the diffusion phase is carried by chaotic tent map. The proposed algorithm has offered resistance to many cryptographic attacks, such as brute force attack. Security analysis is also conducted by using key space analysis, key sensitivity analysis, and entropy analysis. Security analysis tests of the method showed ascendancy on the security and authenticity of the Lena and onion images.

Author Contributions: Conceptualization, A.W.; Formal analysis, S.I. and A.W.; Revision and Related works, M.T.B.O. and M.I.; Investigation, S.I.; Methodology, S.K., A.W. and Z.N.; Resources, M.I.; Supervision, S.K.; Visualization, S.K.; Writing—original draft, A.W.; Writing—review & editing, M.I., F.N. and H.H. All authors have read and agreed to the published version of the manuscript.

Funding: The researchers would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project. The authors also thank Natural Sciences and Engineering Research Council of Canada (NSERC) and New Brunswick Innovation Foundation (NBIF) for the financial support of the global project except the publication fees. These granting agencies did not contribute in the design of the study and collection, analysis, and interpretation of data.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available within the manuscript.

Acknowledgments: The researchers would like to thank the Deanship of Scientific Research, Qassim University, for continuous support.

Conflicts of Interest: This is an original manuscript. This manuscript is neither submitted nor accepted anywhere. All authors declare that we have no competing interest.

References

1. Mahajan, P.; Sachdeva, A. A Study of Encryption Algorithms AES, DES and RSA for Security. *Glob. J. Comput. Sci. Technol.* **2013**, *13*, 15–22.
2. Mandal, A.K.; Parakash, C.; Tiwari, A. Performance Evaluation of Cryptographic Algorithms: DES and AES. In Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 1–2 March 2012; pp. 1–5.
3. Lorenz, E.N. Atmospheric predictability as revealed by naturally occurring analogues. *J. Amos. Sci.* **1969**, *26*, 636–646. [CrossRef]
4. Bourbakis, N.; Alexopoulos, C. Pictyre data encryption using SCAN patterns. *Pattern Recognit.* **1992**, *25*, 567–581. [CrossRef]
5. Jiri, F. Symmetric ciphers based on two dimensional chaotic maps. *Int. J. Bifurcat Chaos* **1998**, *8*, 1259–1284.
6. Scharinger, J. Fast encryption of image data using chaotic Kolmogorov flow. *J. Electron. Eng.* **1998**, *7*, 318–325. [CrossRef]
7. Yen, J.C.; Guo, J.I. A new image encryption algorithm and its VLSI architecture. In Proceedings of the IEEE Workshop Signal Processing Systems, Taipei, Taiwan, 22 October 1999; pp. 430–437.
8. Li, S.; Zheng, X.; Mou, X.; Cai, Y. Chaotic encryption scheme for real time digital video. In Proceedings of the SPIE on Electronic Imaging, San Jose, CA, USA, 19 January 2002.
9. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption based on 3D chaotic maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
10. Fozia, K.; Rehan, S.; Farheen, Q. Hill Cipher Key Generation Algorithm by using Orthogonal Matrix. *Int. J. Innov. Sci. Mod. Eng.* **2015**, *3*, 5–7.
11. Usc-Sipi Image Database for Research in Image Processing, Image Analysis, and Machine Vision. Available online: http://sipi.usc.edu/database/ (accessed on 19 September 2017).
12. Patro, K.A.K.; Soni, A.; Netam, P.K.; Acharya, B. Multiple grayscale image encryption using cross-coupled chaotic maps. *J. Inf. Secur. Appl.* **2020**, *52*, 102470. [CrossRef]
13. Patro, K.A.K.; Acharya, B. An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system. *Nonlinear Dyn.* **2021**, *104*, 2759–2805. [CrossRef]

14. Kanwal, S.; Inam, S.; Cheikhrouhou, O.; Mahnoor, K.; Zaguia, A.; Hamam, H. Analytic study of a novel color Image Encryption Method Based on the chaos System and color codes. *Complexity* **2021**, *2021*, 5499538. [CrossRef]
15. Chen, C.; Sun, K.; Xu, Q. A color image encryption algorithm based on 2D-CIMM chaotic map. *China Commun.* **2020**, *17*, 12–20. [CrossRef]
16. Zhang, L.-M.; Sun, K.-H.; Liu, W.-H.; He, S.-B. A novel color image encryption scheme using the fractional-order hyperchaotic system and DNA sequence operations. *Chin. Phys. B* **2017**, *26*, 10. [CrossRef]
17. Patro, K.A.K.; Acharya, B.; Nath, V. Various dimensional colour image encryption based on non-overlapping block-level diffusion operation. *Microsyst. Technol.* **2020**, *26*, 1437–1448. [CrossRef]
18. Chidambaram, N.; Raj, P.; Thenmozhi, K.; Amirtharajan, R. Advanced framework for highly secure and cloud-based storage of colour images. *IET Image Process.* **2020**, *14*, 3143–3153. [CrossRef]
19. Nkandeu, Y.P.K.; Tiedeu, A. An image encryption algorithm based on substitution technique and chaos mixing. *Multimed. Tools Appl.* **2019**, *78*, 10013–10034. [CrossRef]