Journal of Theoretical and Applied Information Technology
31st March 2022. Vol.100. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HENON CHAOTIC MAP BASED IMAGE ENCRYPTION SCHEME USING BIT-LEVEL CIRCULAR SHIFT

SYED SAQLAIN HASSAN[1], ZESHAN IQBAL[1], MUHAMMAD JAWAD IKRAM[2], MOHAMMED ISHAQUE[2]

[1] Department of Computer Science, University of Engineering & Technology Taxila, Pakistan

[2]Department of Computer Science and Information Technology, Jeddah International College, Saudi Arabia

E-mail: syedsaqlainhassan@gmail.com, zeshan.iqbal@uettaxila.edu.pk, m.jawad@jicollege.edu.sa, m.ishaq@jicollege.edu.sa

ABSTRACT

Recently, privacy has become a major issue in digital images transmitted over public networks. Although the said environment is suitable and quite useful, the unfortunate reality is that there exist numerous privacy and security threats. This article addresses the problem by proposing a new image encryption technique using a chaotic system and bit-level circular shift. A Henon Map has been used as a chaotic system to do the bit-level circular shift to encrypt the image. According to the experimental results, the proposed algorithm overcomes the shortcomings of conventional encryption techniques. The proposed technique has lower computational complexity and shows promising results in terms of various security tests. The keyspace is too large to avoid brute-force attacks. For the encrypted image, the histogram is uniformly distributed and far away from the original image. Thus, the statistical attack is not applicable here. The correlation test of the adjacent pixels shows no correlation between them. The proposed algorithm is key sensitive; tiny key-value modifications will end up with another different image. Therefore, the new technique is compatible with real-time image-encryption applications over public networks.

Keywords: *Bit-Level Circular Shift, Chaotic System, Encryption, Decryption, Henon Map*

1. INTRODUCTION

Due to rapid advances in communication technology, digital image information is now shared widely through the internet. In the meantime, the fortification of digital image information - being transferred over the public networks, against illegitimate utilization has become a significant issue. Using an encryption algorithm is a clear and direct way of protecting image data from illegal eavesdropping. Unfortunately, the well-known block encryption algorithms, such as AES, IDEA and Triple-DES, are not appropriate for practical image encryption therefore the security of these algorithms is essentially guaranteed by their high computational costs, making it difficult to meet the online communication needs, considering a large amount of data. Different encryption schemes have been proposed to overcome this challenge. Amongst those, the chaos-based algorithms offer an optimum trade-off between efficiency and Security. In 1949, Claude Shannon in his paper Communication Theory of Secrecy System proposed the permutation substitution network that serves as a foundational treatment of modern cryptography. The most widely used chaos-based image encryption scheme is proposed by [1] adopted the Shannon approach for the design of secure cipher. The pixel positions are initially scrambled in a hidden way in each round of the encryption process, reducing the similarity between neighboring pixels. Afterward, the pixel values are chronologically altered, and the impact of each pixel is diffused to all of its subsequent pixels throughout the modification process. Performing multiple rounds of encryption an insignificant modification in one plain-image pixel may result in a completely new cipher-image.

Conventionally, widely used image scrambling chaotic maps – the standard map, the cat map, and the baker map, the approach of permutation employed by these maps have two key drawbacks. That is, they are only applicable to square images and the periodicity of the discretized version of chaotic maps [2], [3], [4] to overcome the shortcomings [5] proposed a scheme for image scrambling based on a chaotic. sequence sorting mechanism.

Unfortunately, compared to various existing techniques, this technique results in weaker confusion effect individual pixels as the entire column/row of the image is input as the scrambling unit. In [6], proposed a novel scrambling algorithm shuffling images using wave perturbations in an n-dimensional space (nD). Area of perturbations on waves. The initial matrix with pixel-level is viewed as a regular 3D bit matrix and in [7], a new permutation scheme at bit-level 3D is proposed. To further boost the permutation effect, the original and the target bit positions are chosen at random in the permutation stage. Several discrete chaotic maps and continuous chaotic structures, including the most commonly used ones, can be used in the substitution stage to generate key-stream sequences with optimal statistical properties. as in the Lorenz scheme [8], the logistic map [2], the Chen system [9], and high dimensional chaotic system variants [10]. Lowdimensional chaotic systems, in terms of the logistics map, have the advantages of simplicity and performance, but they have limited keyspace. In comparison High-dimensional chaotic systems, especially hyperchaotic systems, provide a significant key space at the cost of computations. It was recently confirmed that several existing image encryption schemes had been successfully cracked by using selected-plain-text attacks [11], [12], [13], [14].It is because the key-stream substitution sequences used in these systems are chosen solely by the secret key. That is, different plain images of the same key-stream sequence are encrypted when a different secret key is used. Therefore, the key-stream sequence may be calculated by encrypting such specially generated images (for Example., an image in which all of the pixels have the same value) and then comparing them to their respective outputs. Obviously, if a key-stream sequence is based on both the plain-text and secret key, the analysis becomes impractical. For instance, in [15], Keystream values are extracted from multiple time iteration of the logistic map and the number of iterations is determined by the plain-pixel values. Unfortunately, repeated iteration function ultimately reduces cryptosystem efficiency. In [16], During the substitution procedure, the value of each key-stream dimension is dynamically changed based on the plain-pixel values. There has been a lot of work implemented to improve the reliability of chaos-based image ciphers to help address the challenge of secure internet image communications. [17] proposed the efficacy of specific bit-plane image encryption and concluded that only a fair level of protection can be achieved by randomly encrypting the image's higher four bit-planes. In [18] as a light-weight replacements for the 1D chaotic map iteration, an even more efficient diffusion approach using simple table lookup and swapping techniques was proposed. Following this study, in [19] an image encryption scheme based on a lookup table has been proposed, which performs both confusion and diffusion operational activities with an advantage of handling channel errors, which tends to cipher data corruption. Images retrieved from the corrupted cipher data have been shown to have adequate visual perception. A novel bidirectional diffusion technique in [20] was proposed to reduce the number of encryption rounds required to spread the impact of each individual pixel over the entire cipher image. Results have illustrated, to achieve an effective diffusion effect the scheme needs one round of permutation following two rounds of diffusion. In [16], [21], [22], [23],[77],[78] Image ciphers based on chaos and bit-level permutation have been proposed. The substitution effect implemented during the permutation stage reduces the number of iteration rounds needed by the time-consuming substitution phase, resulting in a shorter encryption time. In [8] an efficient image cipher based on chaos has been proposed with the permutation key determined by the hash value of the original image. Due to the avalanche nature of the hash function, totally different shuffled images are created even though there is a small variation between the original ones, thus increasing the diffusion process. In this paper, we present a novel chaos-based image encryption technique that is based on Henon chaotic map. Henon map is a discrete time dynamic system, which is a mathematical concept where a fixed rule describes the time dependence of a point in a geometrical space. Henon map is defined by the function [24], [25].

$$x_{i+1} = 1 - ax_i^2 + y_i \quad (1)$$

$$y_{i+1} = bx_i \quad (2)$$

Where a = 0.3, b ∈ [1.07, 1.4]. If one chooses a = 0.3, b = 1.4, the system is chaotic, subsequently, this feature is very useful in image encryption [24], [25]. The movement created by a nonlinear and ensured system is Chaos. Research shows that for a nonauthorized user a chaotic signal looks like noise and ignores the mechanism for generating it and has the characteristics of randomicity, ergodicity, non-periodicity, and so on. Important properties of chaotic systems include 1) lack of periodicity and topological transitivity, 2) pseudo-random property, and 3) high dependence on initial conditions and system parameters [26], [27], [28]. If and only if the parameters are the same as the original value, the chaotic signal is reconstructed. What's more,

generating a chaotic signal is often low-cost. For these characteristics, chaos is introduced into the encryption field. Our chaos-based image encryption technique is based on a henon chaotic map and bit-level circular shift work as follows. Our algorithm takes a grayscale input image as an input, converts it into a bit-level binary image. Then, we shuffle the bits of the image by incorporating a henon map. Finally, a bit-level circular shift is applied, and the encrypted image is produced. The decryption process obtains the image by performing all the encryption steps in reverse order. We perform various performance tests on our technique and found that the proposed technique delivers better quality of service and security.

1.1 Article Contributions

In general, this paper's contributions are as follows.

- A novel chaos-based image encryption technique that incorporates Henon chaotic map and bit-level circular shifting operation has been proposed.
- A comprehensive security review of the proposed methodology was carried out to check its resistance against all known attacks.
- The proposed technique has promising results in terms of avoiding brute-force attacks, a lower correlation between adjacent pixels, key sensitivity, and higher information entropy.
- The comparative analysis of the proposed technique with existing techniques has been performed in terms of resistance to statistical attack using parameters like histogram analysis, correlation coefficient analysis, key sensitivity and information entropy analysis and resistance to differential attack using parameters like the number of pixel change rate (NPCR) and unified average changing intensity (UACI) to validate the results of the proposed technique.

1.2 Article Layout

The rest of this paper is organized according to the following. Section 2 provides material on related work. In section 3, we present our proposed technique. Section 4 presents a performance-security analysis. Section 5 presents a comprehensive comparative analysis of the proposed technique. Finally, in section VI the whole work is concluded.

2. LITERATURE SURVEY

Numerous chaos-based image encryption techniques have been proposed recently. Permutation and diffusion are the two important stages that are involved in these techniques, which results in a better level of security [26], [27]. In [26], a new encryption scheme for images is presented, that Uses the absolute shuffling approach to shuffle the image pixel position and eventually apply a hyper-chaotic scheme. On one hand, substantial improvements have been done in communication networks and the Internet. On the other hand, direct transmission of confidential messages may be unsafe on these public networks. Cryptographic techniques are required for secure communication on these public networks. Conventional symmetric ciphers such as DES have good properties of confusion and diffusion [7], [12]. Generally, Chaos-based systems, which also have the properties of confusion and diffusion, are ergodic and have a sensitivity to system parameters and initial conditions [26], [27]. Numerous chaos-based cryptographic techniques have been proposed. Among those, Some use one-dimensional chaotic maps, which can be used to sequence data or encrypt documents [29], [30], [31].For image processing applications, chaotic map with multi-dimensional (two or more) dimensions are used for the fact that image is treated as two-dimensional array that consists of pixel values [1], [32], [33], [34], [35], [36], [37], [38].

[1] Argued that two methods, namely chaotic confusion, and pixel diffusion, should be included in the technique for the encryption of images based on chaos. The pixels of a plain image with a two-dimensional chaotic map is permuted based on the chaotic confusion, while the gray level value of each pixel is alternated sequentially based on the diffusion of pixels [1]. This architecture serves as a baseline for numerous chaos-based image encryption methods, for instance, Chen [36] applied a 3D cat [39] and 3D baker map [37] in the confusion phase. In the same context, a two-dimensional cat map is used by [32] for position permutation of pixels and the discretized chaotic system of Chen is used for value masking [40].

[34] Noted the presence of weak cipher keys using the cat and baker maps. Cat and baker maps have smaller keys, in contrast to standard maps. For that reason, the emphasis is on employing the standard map for confusion while using the logistic map for the diffusion of a pixel value. A minimum of four rounds of confusion and diffusion was suggested by [34] to achieve an optimum level of security. Thus, leading to 16 rounds of permutations and 4 rounds of diffusion. Though computational complexity is reduced using actions

such as pre-computation of permutation mode and sine tables, the comparatively slow method of diffusion still bounds the performance of this cryptosystem.

[41] presented a DNA based chaotic image encryption system which can resist all forms of classical types of attack, and also improved all the evaluation parameters so that the images can be transmitted effectively having no chance of being disclosed/decoded by the attackers

[42] proposed a double spiral scans-based image encryption algorithm that can effectively scramble pixels in image blocks. Results show that the algorithm has good encryption accurateness and outperforms other popular image encryption algorithms.

[43] 2DHCM is a new 2D chaotic map that was proposed. The 2D-HCM has improved chaotic systems, a higher chaotic index, a wider chaotic range, better ergodicity, and provides unpredictable output than other 1D and 2D chaotic maps, according to performance evaluations such as trajectory, bifurcation diagram, and Lyapunov exponent.

[44]proposed a new secret sharing scheme that utilizes a chaotic map-based encryption algorithm to encrypt/decrypt the data being shared. Ten shares are generated so that coming together of any four shares reconstructs the original plaintext. Utilizing the standard measures, the proposed scheme was shown to be robust and effective. However, a limitation of the proposed system was that the size of each of the generated shares varies slightly in comparison to the input plaintext.

Based on the classical confusion-diffusion structure, an Algorithm for Image Encryption is proposed in [45], In the encryption algorithm, the classical chaotic model is used for generating two sets of chaotic sequences to encrypt the image. The Lorenz 2D chaotic model is used to generate chaotic sequences for encryption.

[46]Proposed a novel scheme in which DNA is used with a new one-dimensional (HST) map structure which has more advantages than a simple chaotic system (henon map, sin map, ten maps, etc.) such as better parameter space, higher randomization, and several chaotic sequences. So the chaotic series created by (HST) is hard to prophesy. Within the medical image, the details of the patient are commonly given for presentation in the corner of the medical image. This makes it easy for anyone to access the information and can be intercepted by authorized users. In this paper using steganography and cryptographic techniques, the medical image is encrypted along with the patient information embedded in the image. Initially, using LSB steganography, the patient's detail is hidden in his / her medical image. Furthermore, the medical image is encrypted using the latest encryption scheme that achieves the confusion and diffusion method by using DNA encoding rules and a new HST map that incorporates henon, sin and ten maps to generate chaotic series with high randomness. for the generation of chaos sequence in quantum computers.

[47] presented an algorithm for image encryption that uses quantum henon mapping to generate chaos sequence, which is the greatest difference from previous works and breaks away from classical computer restrictions.

[48] introduced an encryption algorithm based on several chaotic maps with minimum encryption rounds. The multiple chaotic maps presented a projected encryption scheme with confusion and diffusion capability. Output results indicated the proposed scheme show greater resistance to various attacks.

3. PROPOSED TECHNIQUE

This section presents descriptions of the proposed technique for the encryption of images. The block diagram for the technique proposed is given in FIGURE 1.

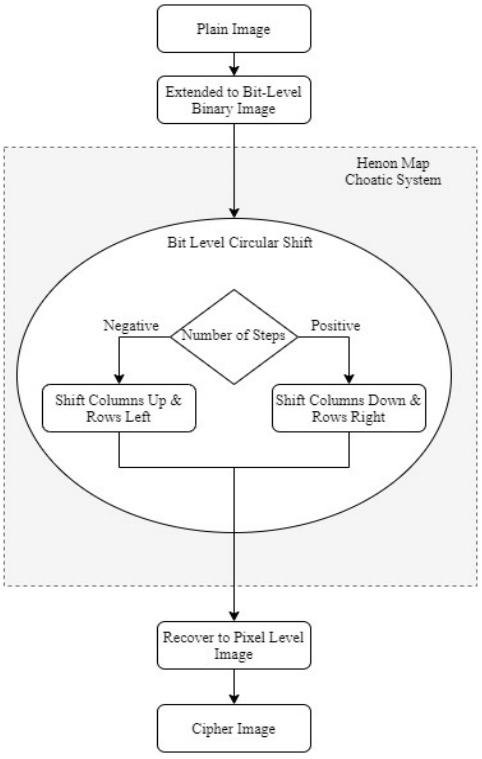


Figure 1: The Proposed Encryption Technique

Journal of Theoretical and Applied Information Technology
31st March 2022. Vol.100. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Encryption Algorithm

Input: Plain Image (P)
Output: Encrypted Image (Q')
Step 1: Read the grayscale plain Image (P) of size M × N
Step 2: Convert the Plain Image (P) to bit-level Binary image (P') by extending every pixel of (P)
Step 3: Using Henon map as a chaotic system. Apply Bit-level circular shift by specific steps to image (P') to obtain shuffled image (Q)
Step 4: Convert shuffled image (Q) obtained in step3 into pixel level to obtain Encrypted image (Q')

3.2 Encryption Working Example

The grayscale Cameraman Image is used to show the working of the Encryption Algorithm. FIGURE 2 shows the grayscale Cameraman Image and its histogram.

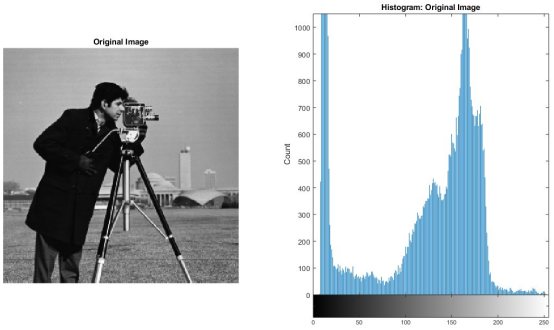


Figure 2: Gray Scale Cameraman Image

The cameraman image(P) is converted from pixel level to bit-level image (P'). This step is done by converting each pixel to 8 bits. Therefore, if we have an M × N pixel image, it will be extended to an M × (N × 8) bits image. The resulting image is a binary image. FIGURE 3 shows the bit-plane image.

Figure 3: Bit-level Binary Image

We shuffle the bits of image (P') using Bit-Level Circular Shift. This circulation is done for rows and columns. The bits of the image are circularly shifted by specific steps. If the number of steps is positive, the bits are shifted down for columns or right for rows. If it is negative, the bits are shifted up for columns or left for rows. The shuffled image (Q) is shown in FIGURE 4.

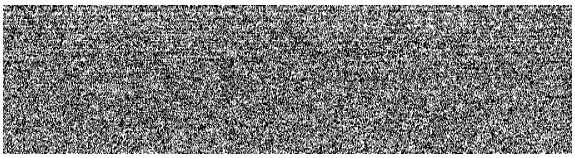


Figure 4: The Shuffled Image

The operations of henon map and bit circular shift are explained as follow:

- The indices of the shifted row or column and the number of steps are generated using Henon map Chaotic System [27] [29] using Eq. 1 and Eq. 2, Where a = 0.3, b ∈ [1.07, 1.4].
- For Henon map, after doing S iterations (for our application S =3000), a new X0 is derived. We continue to generate X1, X2, and X4. X0 and X2 serve as indices of the shifted row/column. X1 and X3 serve as the number of steps used to do the circular shift. These Values are treated using the following formulas [45]:

  ri-= mod(X0 x 1016, N x 8)
  ci= mod(X1 x 1016, M)
  rs= mod((X2 - 0.5) x 1016, N x 8/2)
  cs= mod((X3 - 0.5) x 1016, M/2)

- The values are multiplied by 1016 to enlarge the keyspace size. rs and cs are the values of the steps, thus 0.5 is subtracted first to provide positive and negative values. The output range is controlled using the mod function which returns the remainder after division. The image is in bit-plain thus the upper limit of ri is N x 8. The circular shift is done in both directions thus the upper limits of rs and cs are divided by 2.
- The circular shift is done for one row and one column using ri as an index for the shifted row and rs as shifted steps. The same for ci as an index for the shifted column and cs as shifted steps.

Finally, we convert the shuffled image(Q) from bit-level to pixel level to produce the encrypted image (Q'), which is depicted in FIGURE 5.

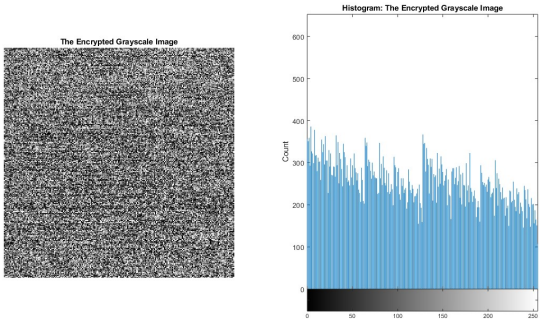


Figure 5: The Encrypted Gray-scale Image and its Histogram

3.3 Decryption

For decrypting the image (Q') we do the same steps backward. First, we read the encrypted image(Q'). Then the encrypted image is converted from pixel-level to bit-level binary image. After that, the image is de-shuffled with the same keys. Finally, we can get the original image(P) by converting the image from bit-level to pixel level.

4. PERFORMANCE ANALYSIS

The performance and quality level of an encryption method depend on its ability to resist known attacks of all kinds. The capability of the proposed system against known attacks is measured in the following section.

4.1 Differential Analysis

The Differential Attack is used to test the sensitivity of the algorithm for encryption against the slight changes in a plain image. We measured the number of Pixel Change Rate (NPCR) and the Unified Average Change Intensity (UACI) parameters for our scheme.

4.1.1 Number of Pixel Change Rate (NPCR)

This calculates the percentage of different pixel numbers between two encrypted images, the plain images of which differ by a single pixel only. It can be computed as:

$$NPCR = \frac{\sum_{j,k} D(j,k)}{M \times N} x\ 100 \quad (3)$$

Here,

$$D_{j,k} = \begin{cases} 0 & if\ E(j,k) = E'(j,k) \\ 1 & if\ E(j,k) \neq E'(j,k) \end{cases} \quad (4)$$

where M and N represent the width and height of the image, respectively. D(j, k) indicates the difference between corresponding pixels of the encrypted image obtained by encrypting the original image (E'(j, k)) and the encrypted image of the changed image (E(j, k)).

4.1.2 Unified Average Changing Intensity (UACI)

It measures the mean difference in intensity between two encrypted images, which corresponds to plain images varying by one pixel. It can be calculated by using the formula:

$$UACI = \frac{\sum_{j,k} E(j,k) - E'(j,k)}{255 \times M \times N}\ x\ 100 \quad (5)$$

where E(j, k) and E'(j, k) is the encrypted images of original and changed images, respectively.

UACI and NPCR measurements were used to test 11 different input images. The results of the two indicators are close to the ideal value. The encryption algorithm is performed on the modified original image, then the results of NPCR and UACI tests are computed as shown in Table 1. The results show that a small change in the original image will result in a great change in the encrypted image; this implies that the proposed algorithm has an excellent ability to resist the differential attack.

Table 1: Results of NPCR and UACI Tests on Different Input Images

Sr	Input Image	NPCR	UACI
1	Female (NTSC Test Image)	99.6094	33.4110
2	Couple (NTSC Test Image)	99.2310	33.8476
3	Female	99.4202	33.0522
4	House	99.5255	33.5820
5	Tree	99.5087	33.5764
6	Jellybeans	99.4720	33.8353
7	Moon surface	99.5956	33.8507
8	Aerial	99.5560	33.9836
9	Airplane	99.5087	33.8626
10	Baboon	99.5762	33.4470
11	Peppers	99.6223	33.4445

4.2 Statistical Analysis

The encryption techniques may also be broken by the statistical analysis of an encrypted image. Confirming the robustness of our scheme against the most important statistical attacks that are key space analysis, histogram analysis, key sensitivity analysis, entropy analysis of information and correlation of adjacent pixels

4.2.1 Keyspace analysis

The secret key in our encryption process is the combination of initial values of Henon map X_0, a, and b, with the precision of 10^{-14}, resulting in a keyspace size of 10^{70}. This main space is enormous enough to make brute-force attacks ineffective.

4.2.2 Keyspace analysis

In examining histograms, we want to show how pixels are distributed in an image. This is done by plotting the pixel count for the grayscale level. FIGURE 6 shows the histogram of plain and encrypted cameraman images.

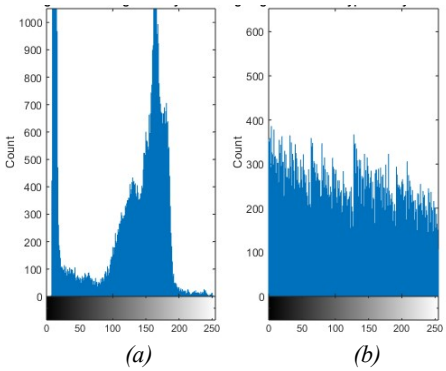
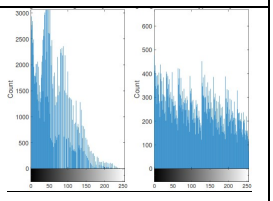
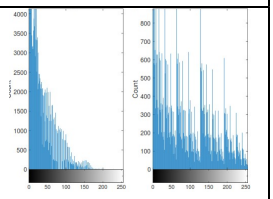
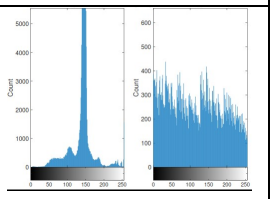
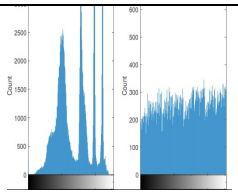
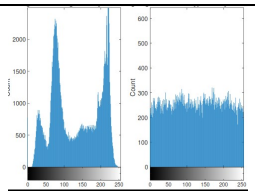
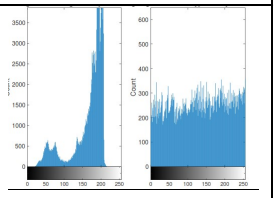
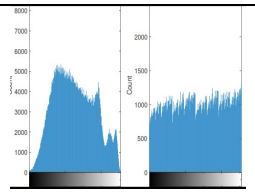
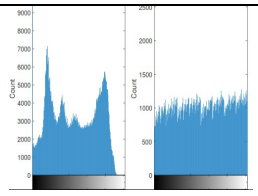
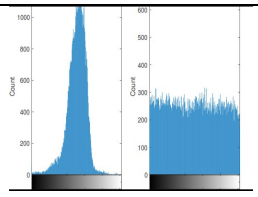
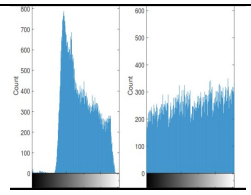
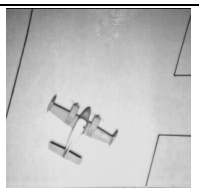
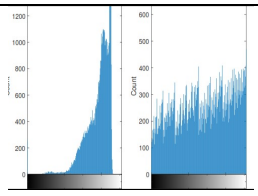


Figure 6: Histogram of (a) the original image (b) the encrypted image

Table 2 shows the original grayscale encrypted image histogram of the different input images. We can see that the encrypted image's histogram is efficient in achieving and far from the original. Thus, statistical attacks are not applicable here.

Table 2: Histogram analysis of the proposed Scheme on Various Input Images

Sr	Input Image	Histogram Grayscale & Encrypted Image
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

4.2.3 Information entropy analysis

To calculate the randomness information entropy is one the most significant measure. Information entropy is calculated. Information entropy is calculated using the following formula;

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i) \quad (6)$$

Here, N denotes the number of bits needed to represent a symbol $s_i \in ss_i \in s$ and $P(s_i)P(s_i)$ denotes the probability of symbol s_i of expressing the entropy in bits. If we have 2N symbols, then N is the ideal entropy. In our scheme, the grayscale image has 256 gray levels. Information entropy of various input images is depicted in Table 3. Each entropy result is close to the perfect estimation of the cipher entropy information, which is 8. This indicates that the attacker will derive less information of the plain image from the grey value distribution in the encrypted image. As a result, the proposed cipher algorithm has a high level of security, which is necessary for an encryption algorithm.

Table 3: Results of entropy analysis of the proposed Scheme on Different Input Images

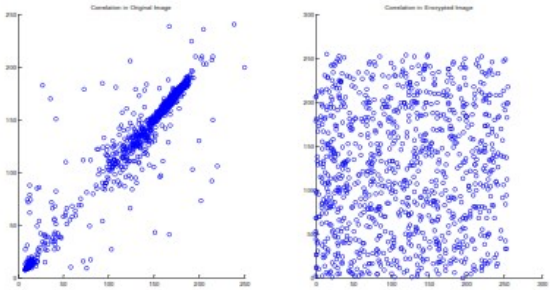
Sr	Input Image	Grayscale Image	Encrypted Image
1	Female (NTSC Test Image)	9.8981	7.9345
2	Couple (NTSC Test Image)	6.2945	7.9547
3	Female	5.9709	7.9547
4	House	7.0686	7.9829
5	Tree	7.5371	7.9940
6	Jellybeans	6.5835	7.9834
7	Moon surface	6.7093	7.9946
8	Aerial	7.3118	7.9845
9	Airplane	6.4523	7.9464
10	Baboon	7.7624	7.9916
11	Peppers	7.6698	7.9911

4.2.4 Correlation of adjacent pixels analysis

To do the correlation analysis 1000 pixels were selected randomly. For each pixel, we find it's adjacent (vertically, horizontally, and diagonally). The person correlation coefficient was used using the following formula in Eq. (7):

$$r_{xy} = \frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (7)$$

where x and y are gray values of the adjacent pixels. The correlation distribution of horizontally adjacent pixels shows a strong correlation for the original image Figure.7a. On the other hand, there is no correlation for the encrypted image Figure.7b.



(a) (b)

Figure 7: Correlations in (a) the original image (b) the encrypted image

The correlation coefficients for other adjacent pixels are shown in the following Table 4.

Table 4: Correlation Coefficients for Adjacent Pixels

Sr	Input Image	Plain Image			Encrypted Image		
		Ver	Hor	Dia	Ver	Hor	Dia
1	Female (NTSC test image)	0.9715	0.9610	0.9511	0.0293	0.007	0.047
2	Couple (NTSC test image)	0.9356	0.9573	0.9084	0.0448	0.0152	0.0112
3	Female	0.9831	0.9408	0.9319	0.0616	0.0224	0.0374
4	House	0.9659	0.9206	0.9054	0.0833	0.0413	0.0076
5	Tree	0.9612	0.9316	0.9415	-0.0072	-0.0227	-0.0111
6	Jellybeans	0.9775	0.9776	0.9524	0.0568	-0.0114	0.0005
7	Moon surface	0.9088	0.9332	0.901	-0.0246	-0.067	-0.0492
8	Aerial	0.8964	0.8625	0.8055	0.0216	-0.0211	0.0025
9	Airplane	0.9629	0.9387	0.9033	0.0173	-0.0331	-0.0041
10	Baboon	0.9186	0.8663	0.86	-0.0078	-0.0202	0.027
11	Peppers	0.9581	0.9639	0.9522	0.0701	0.0048	-0.0099

4.2.5 Key sensitivity test

As mentioned before, the secret key is composed of the initial values of Henon map X0, a, and b. When using the same parameters as in the encryption algorithms, the original image will be retrieved as shown in FIGURE 8.

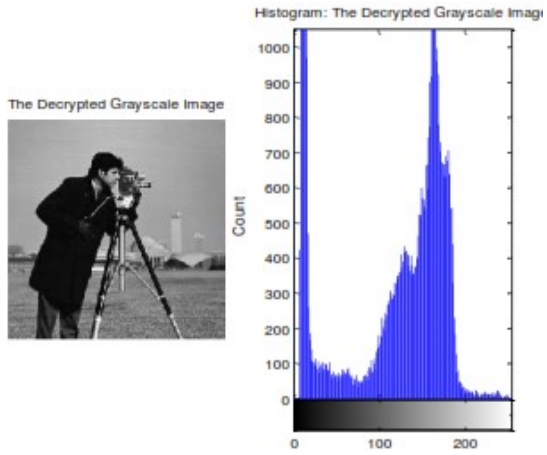
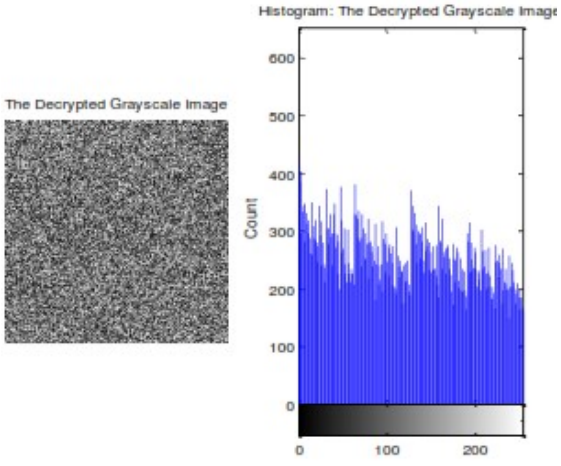


Figure 8: Decrypted Cameraman image and Histogram using the same

We see that for the initial value of henon map X_0 our method of encryption is very sensitive.FIGURE 8 shows the decrypted image with all the parameters to be same except a = 1.40000000001. For all initial parameters our encryption method is very sensitive to, a minor alteration in these parameters will result in a completely different image as shown in FIGURE 9.



(a) *(b)*

Figure 9: Decrypted Cameraman image using a=1.40000000001 (a) Decrypted image (b) Histogram

5. COMPARATIVE ANALYSIS

This section provides a comparative analysis using seven different parameters of the proposed technique as shown in Table 5. Lena's image is used as the input image for comparison purposes as most of the existing techniques are evaluated using Lena's image. The size of the input image was 256 x 256, the value of NPCR and UACI for the proposed scheme are 99.89092657 and 33.316276 respectively are higher than the existing techniques. This shows the robustness of the techniques proposed against different forms of Differential Attacks. The value of the statistical parameters - Keyspace is 1070 which is wide enough to render a brute force attack ineffective. The proposed scheme's Information Entropy value of 7.9997 is also marginally higher than the existing schemes and closer to the optimal value of 8. Furthermore, the coefficient of correlation of the ciphered image displays a random behavior like that of the original images demonstrating that the ciphered image is completely different from the original.

Thus, a comprehensive comparative analysis of the proposed technique has been carried out on basis of seven different parameters to validate its robustness. Table 5 shows a comparison of existing techniques with the proposed method. It is observed that in contrast to the existing techniques, the proposed technique shows promising results on Lena's image as compared to the cameraman image because Lena's image has smooth blocks, clear and detailed patterns, gradual changes in lights and shades.

6. CONCLUSION

We present a new image encryption algorithm based on a chaotic system and bit-level circular shift. According to experimental results, the proposed algorithm shows promising performance. The keyspace is large enough to resist brute-force attacks. The histogram of the encrypted image is fairly uniform and far away from the original one. Thus, the statistical attack is not applicable here. There is no correlation between adjacent pixels (vertically, horizontally, and diagonally) for the encrypted image. The proposed algorithm is very sensitive to the keys; a tiny change key will end up with a completely different image. We can conclude that this method is suitable for image encryption and transmission over public networks

Table 5: Comparative Analysis

Sr	Reference	Input Image	Dimensions	NPCR	UACI	KA	Correlation Coefficient-Ciphered Image			IE
							Horizontal	Vertical	Diagonal	
1	[51]	Random	256 x 256	99	-	2^{80}	0.0041	-0.0337	-	-
2	[52]	Barbara	256 x 256	41.962	33.25	2^{260}	0.0038	0.0023	0.0004	7.9968
3	[53]	Lena	512 x 512	99.5*	33.3	-	0.000707	0.002165	0.014886	7.9994
4	[54]	Lena	512 x 512	99.6051788	33.3999634***	10^{-14}	.000550055	0.00165017	-0.00459011	7.999342
5	[55]	Girl	512 x 512	-	-	2^{96}	-0.0893	0.0034	0.001	7.9993
6	[56]	Random	-	99.55	33.39	-	0.002909	-0.01503	-0.012901	7.9997
7	[57]	Lena	256 x 256	99.6537	37.6825	-	0.0037	0.0109	0.0287	7.9961
8	[58]	Lena	256 x 256	99.6203917**	33.4970309	10^{120}	.000533462	.000286785	0.00210009	-
9	[59]	Lena and Lion	256 x 256	99.82	33.39	8^{256} x256	0.009642154	0.03421542	0.020574261	7.998446
10	[60]	Lena	256 x 256	99.6228	33.7041	$>2^{624}$	-0.0048	-0.0112	-0.0045	7.9985
11	[61]	Lena	256 x 256	99.41	33.26	2^{256}	0.003	-0.0024	-0.0034	7.9976
12	[62]	Lena	512 x 512	99.524	33.434	2^{60}	0.0085	0.0097	0.0092	7.9976
13	[63]	Lena	256 x 256	99.61	33.46	-	-0.0015	-0.0032	0.0008	7.9972
14	Proposed Scheme	Lena	256 x 256	99.89092657	33.316276	10^{70}	0.0065	0.0478	-0.0142	7.9997
		Cameraman	256 x 256	99.58	33.32		-0.0125	0.0649	-0.03	7.9717

REFERENCES

[1] J. FRIDRICH, "SYMMETRIC CIPHERS BASED ON TWO-DIMENSIONAL CHAOTIC MAPS," International Journal Of Bifurcation And Chaos, Vol. 8, No. 6 (1998) 1259–1284, Vol. 8, 1998.

[2] W.-H. M. Y.-F. Z. Z.-L. Z. F. C. L. K. T. C. C. Fu, ""“An Efficient And Secure Medical Image Protection Scheme Based On Choatic Maps," ” Computers In Biology And Medicine, , Vol. 43, 2013.

[3] Z.-L. Z. C. F. H. Y. A. Y. Z. J.-X. Chen, ""“Reusing The Permutation Matrix Dynamically For Efficient Image Cryptographic Algorithm,," Signal Processing, Vol. 111, 2015.

[4] B. S.-H. K. A. W.-S. L. K.-W. Wong, "A Fast Image Encryption Scheme Based On Chaotic Standard Map,”," Physics Letters A, P. 372, 2008.

[5] B.-B. L. Y.-S. M. X. L. A. J.-J. C. C. Fu, "A Novel Chaos Based Bit-Level Permutation Scheme For Digital Image Encryption,," Optics Communication, Vol. 284, 2011.

[6] Y. Z. S. A. A. J. P. N. Y. Wu, ""“A Symmetric Image Cipher Using Wave Perturbations,," Signal Processing, , Vol. 102, 2014.

[7] H. Y. Y.-L. Z. A. Z.-L. Z. W. Zhang, "Image Encryption Based On Three-Dimensional Bit Matrix Permutation,," Signal Processing, Vol. 118, 2016.

[8] O. B. H.-Y. J. L.-H. G. A. H.-F. M. C. Fu, "A New Chaos Based Image Cipher Using A Hash Function,," In International Conference On Computer And Information Science (ICIS)., 2016.

[9] Z.-L. Z. C. F. H. Y. A. L.-B. Z. J .-X. Chen, “A Fast Chaos-Based Image Encryption Scheme With A Dynamic State Variables Selection Mechanism, ” Communications In Nonlinear Science And Numerical Simulation,, Vol. 20, 2015.

[10] Z.-K. W. Z.-L. Z. A. H. Y. C. Fu, “A Security Improved Image Encryption Scheme Based On Chaotic Baker Map And Hyperchaotic Lorenz System," International Journal Of Computational Science And Engineering,, Vol. 12, 2016.

[11] S. L. A. K.-T. L. C. Li, "Breaking A Modified Substitution–Diffusion Image Cipher Based On Chaotic Standard And Logistic Maps,”," Communications In Nonlinear Science And Numerical Simulation, , Vol. 16, 2011.

[12] L. Y. Z. R. O. K.-W. W. A. S. S. C. Li, "Breaking A Novel Colour Image Encryption Algorithm Based On Chaos,," Nonlinear Dynamics,, Vol. 70, 2012.

[13] T. X. Q. L. A. G. C. C. Li, "Cryptanalyzing Image Encryption Using Chaotic Logistic Map,," Nonlinear Dynamics, , Vol. 78, 2014.

[14] Y. L. L. Y. Z. A. M. Z. C. C. Li, "Breaking A Chaotic Image Encryption Algorithm Based On Modulo Addition And Xor Operation,”," International Journal Of Bifurcation And Chaos, , Vol. 23, 2013.

[15] K.-W. W. X. L. T. X. A. G. C. Y. Wang, ""“A Chaos-Based Image Encryption Algorithm With Variable Control Parameters,," Chaos, Solitons & Fractals, , Vol. 41, 2009.

[16] J.-B. H. N.-N. W. Q.-B. H. A. W.-M. L. C. Fu, ""“A Symmetric Chaos-Based Image Cipher With An Improved Bit-Level Permutation Strategy,”," Entropy, , Vol. 16, 2014.

[17] K.-W. W. A. X. L. T. Xiang, "Selective Image Encryption Using A Spatiotemporal Chaotic System,”," An Interdisciplinary Journal Of Nonlinear Science, , Vol. 17, 2007.

[18] B. S.-H. K. A. C.-H. Y. K.-W. Wong, ""“An Efficient Diffusion Approach For Chaos-Based Image Encryption,," Chaos, Solitons & Fractals,, Vol. 41, 2009.

[19] Z.-L. Z. C. F. L.-B. Z. A. Y. Z. J.-X. Chen, ""“An Efficient Image Encryption Scheme Using Lookup Table-Based Confusion And Diffusion,”," Nonlinear Dynamics, , Vol. 81, 2015.

[20] J.-J. C. H. Z. W.-H. M. Y.-F. Z. A. Y.-W. Y. C. Fu, "A Chaos-Based Digital Image Encryption Scheme With An Improved Diffusion Strategy," Optics Express, , Vol. 20, 2012.

[21] W. Z. K.-W. W. A. H. Y. Z.-L. Zhu, ""“A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation,”," Information Sciences, , Vol. 181, 2011.

[22] Z.-L. Z. C. F. L.-B. Z. A. Y. Z. J.-X. Chen, ""“An Image Encryption Scheme Using Nonlinear Inter-Pixel Computing And Swapping Based Permutation Approach,," Communications In

Nonlinear Science And Numerical Simulation, Vol. 23, 2015.

[23] Z.-L. Z. L.-B. Z. Y. Z. A. B.-Q. Y. J. Chen, "Exploiting Self-Adaptive Permutation–Diffusion And Dna Random Encoding For Secure And Efficient Image Encryption,"," Signal Processing, , Vol. 142, 2018.

[24] S. H. T. L. H. Y. A. X. K.]F. Qi, "2d Henon-Chebyshev Chaotic Map For Image Encryption,"," In 2019 IEEE 21st International Conference On High Performance Computing And Communications; , 2019.

[25] M. Sharma And A. Sharma, ""A Secret file Sharing Scheme With Chaos Based Encryption,," In 10th International Conference On Computing,Communication And Networking Technologies (ICCCNT). , 2019.

[26] F. H. A. W. G. Z.-H. Guan, ""Chaos-Based Image Encryption Algorithm,," Physics Letters A, , Vol. 346, 2005.

[27] A. S. A. P. I. R. R. Kumar, "Enhancement And Analysis Of Chaotic Image Encryption Algorithms,," In First International Conference On Computer Science, Engineering And Applications (CCSEA 2011), , 2011.

[28] G. C. A. S. L. Y. Mao, "A Novel Fast Image Encryption Scheme Based On 3d Chaotic Baker Maps,"," International Journal Of Bifurcation And Chaos, , Vol. 14, 2004.

[29] M. Sonis, ", "Once More On Hénon Map: Analysis Of Bifurcations,," Chaos Solitons & Fractals, , Vol. 07, 1996.

[30] T. Gao And Z. Chen, ""A New Image Encryption Algorithm Based On Hyper Chaos,," Physics Letters A, , Vol. 372, 2008.

[31] B.-B. L. Y.-S. M. X. L. A. J.-J. C. C. Fu, "A Novel Chaos Based Bit-Level Permutation Scheme For Digital Image Encryption,"," Optics Communications, , Vol. 284, 2011.

[32] S. Li And X. Zheng, "Cryptanalysis Of A Chaotic Image Encryption Method,"," In IEEE International Symposium On Circuits And Systems. Proceedings (Cat. No. 02CH37353), , 2002.

[33] M. Baptista, "Cryptography With Chaos,, Physics Letters A, , 1998..

[34] K.-W. Wong, "A Fast Chaotic Cryptographic Scheme With Dynamic Look-Up Table,," Physics Letters A, , Vol. 298, 2002.

[35] V. P. A. K. S. N. K. Pareek, "Discrete Chaotic Cryptography Using External Key,," Physics Letters A, , Vol. 309, 2003.

[36] U. Q. I. G. A. D. J. F. Belkhouche, "Binary Image Transformation Using Two-Dimensional Chaotic Maps,," In 7th International Conference On Pattern Recognition, , 2004.

[37] J. S. A. Z. W. S. Lian, ""A Block Cipher Based On A Suitable Use Of The Chaotic Standard Map,," Chaos, Solitons & Fractals, Vol. 26, 2005.

[38] L. L. A. F. H. Y. Feng, "A Symmetric Image Encryption Approach Based On Line Maps,," In IEEE, 2006.

[39] ". H. Cheng And X. Li, ""Partial Encryption Of Compressed Images And Videos,," IEEE Transactions On Signal Processing, , 2000.

[40] Y. M. A. C. K. C. G. Chen, "A Symmetric Image Encryption Scheme Based On 3d Chaotic Cat Maps,," Chaos, Solitons & Fractals, , Vol. 21, 2004.

[41] B. D. A. X. L. T. Li, "Image Encryption Algorithm Based On Logistic And Two-Dimensional Lorenz,," IEEE Access, , Vol. 8, 2020.

[42] H. M. A. M. E. N. R. I. Abdelfattah, "Secure Image Encryption Scheme Based On Dna And New Multi Chaotic Map,," In Journal Of Physics: Conference Series, .

[43] X. D. H. H. Z. J. A. W. Z. N. Jiang, "Quantum Image Encryption Cryption Based On Henon Mapping," International Journal Of Theoretical Physics, , Vol. 58, 2019.

[44] M. Khan And F. Masood, "A Novel Chaotic Image Encryption Technique Based On Multiple Discrete Dynamical Maps,"," Multimedia Tools And Applications, , Vol. 78, 2019.

[45] R. Durstenfeld, "Algorithm 235: Random Permutation, Communications Of The ACM, .

[46] V. P. A. K. K. S. N. K. Pareek, "Image Encryption Using Chaotic Logistic Map,"," Image And Vision Computing, , Vol. 24, 2006.

[47] A. A. H. M. A. A. A. S. Behnia, "A Novel Algorithm For Image Encryption Based On Mixture Of Chaotic Maps,"," Chaos, Solitons & Fractals, , Vol. 35, 2008.

[48] K.-W. W. X. L. A. G. C. “. Y. Wang, "A New Chaos-Based Fast Image Encryption Algorithm,," Applied Soft Computing, , Vol. 11, 2011.

[49] ∗. Z. H. H. Zhongyun Huaa, "Cosine-Transform-Based Chaotic System For Image Encryption," Information Sciences Elsvier, Vol. 480, 2018.

[50] "Export.Arxiv.Org," [Online]. Available: Http://Www.Export.Arxiv.Org. [Accessed 25 04 2020].

[51] N. K. A. P. V. A. S. K. K. Pareek, "Image Encryption Using Chaotic Logistic Map," Image And Vision Computing, Vol. 24, 2006.

[52] S. A. A. A. A. M. H. A. A. A. Behnia, "A Novel Algorithm For Image Encryption Based On Mixture Of Chaotic Maps," Chaos, Solitons \& Fractals, Vol. 35, 2008.

[53] Y. A. W. K.-W. A. L. X. A. C. G. Wang, "A New Chaos-Based Fast Image Encryption Algorithm," Applied Soft Computing, Vol. 11, 2011.

[54] Z.-L. A. Z. W. A. W. K.-W. A. Y. H. Zhu, "A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation," Information Sciences, Vol. 181, 2011.

[55] O. A. Y. M. A. I. H. Mirzaei, "A New Image Encryption Method: Parallel Sub-Image Encryption With Hyper Chaos," Nonlinear Dynamics, Vol. 67, 2012.

[56] A. A. G. M. Kanso, "A Novel Image Encryption Algorithm Based On A 3D Chaotic Map," Communications In Nonlinear Science And Numerical Simulation, Vol. 17, 2011.

[57] X.-Y. A. W. T. A. X. D.-H. A. C. F. Wang, "A Selective Image Encryption Based On Couple Spatial Chaotic Systems," International Journal Of Modern Physics , Vol. 28, 2014.

[58] Y.-Q. A. W. X.-Y. Zhang, "A Symmetric Image Encryption Algorithm Based On Mixed Linear--Nonlinear Coupled Map Lattice," Information Sciences, Vol. 273, 2014.

[59] X.-Y. A. G. S.-X. A. Z. Y.-Q. Wang, "Novel Image Encryption Algorithm Based On Cycle Shift And Chaotic System," Optics And Lasers In Engineering, Vol. 68, 2015.

[60] A. A. E.-L. A. A. A. A. B. S. Belazi, "A Novel Image Encryption Scheme Based On Substitution-Permutation Network And Chaos," Signal Processing, Vol. 128, 2016.

[61] W. A. S. K. A. Z. C. Liu, "A Fast Image Encryption Algorithm Based On Chaotic Map," Optics And Lasers In Engineering, Vol. 84, 2016.

[62] M. A. E. A. S. A. D. O. Farajallah, "Fast And Secure Chaos-Based Cryptosystem For Images," International Journal Of Bifurcation And Chaos, Vol. 26, 2016.

[63] Y. A. W. C. A. C. H. Li, "A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation And Bit-Level Permutation," Optics And Lasers In Engineering, Vol. 90, 2017.

[64] W. Z. K.-W. W. A. H. Y. Z.-L. Zhu, " A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation,," ” Information Sciences, , Vol. 181, 2011.

[65] M. Y. A. H. I. O. Mirzaei, "“A New Image Encryption Method: Parallel Sub-Image Encryption With Hyper Chaos," Nonlinear Dynamics,, Vol. 67, 2012.

[66] A. Kanso And M. Ghebleh, "A Novel Image Encryption Algorithm Based On A 3d Chaotic Map,”," Communications In Nonlinear Science And Numerical Simulation, , Vol. 17, 2012.

[67] T. W. D.-H. X. A. F. C. X.-Y. Wang, "“A Selective Image Encryption Based On Couple Spatial Chaotic Systems,”," International Journal Of Modern Physics B, , Vol. 28, 2014.

[68] Y.-Q. Zhang And X.-Y. Wang, "“A Symmetric Image Encryption Algorithm Based On Mixed Linear–Nonlinear Coupled Map Lattice," Information Sciences, , Vol. 73, 2014.

[69] S.-X. G. A. Y.-Q. Z. X.-Y. Wang, "Novel Image Encryption Algorithm Based On Cycle Shift And Chaotic System,”," Optics And Lasers In Engineering, , Vol. 68, 2015.

[70] A. A. A. E.-L. A. S. B. A. Belazi, "“A Novel Image Encryption Scheme Based On Substitution-Permutation Network And Chaos,," Signal Processing, Vol. 128, 2016.

[71] K. S. A. C. Z. W. Liu, "“A Fast Image Encryption Algorithm Based On Chaotic Map,," Optics And Lasers In Engineering, Vol. 84, 2016.

[72] S. E. A. A. O. D. M. Farajallah, "Fast And Secure Chaos-Based Cryptosystem For Images,," Nternational Journal Of Bifurcation And Chaos, , Vol. 26, 2016.

[73] C. W. A. H. C. Y. Li, "A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation And Bit-Level Permutation,," Optics And Lasers In Engineering, , Vol. 90, 2017.

[74] Z.-L. A. Z. W. A. W. K.-W. A. Y. H. Zhu, "A Chaos-Based Symmetric Image Encryption Scheme Using A Bit-Level Permutation," Information Sciences, Vol. 181, 2011.

[75] G.-Y. Z. M. Z. Z. W.-M. L. Chong Fu, ""A New Chaos-Based Color Image Encryption Scheme With An Efficient Substitution Keystream Generation Strategy"," Security And Communication Networks, 2018.

[76] Tarasvi Lakum, Prof.B. Tirapathi Reddy, " An Efficient File Access Control Technique For Shared Cloud Data Security Through Keysignatures Search Scheme ", Journal Of Theoretical And Applied Information Technology 15th January 2022. Vol.100. No 1 Pp 127-136.

[77] Sangapu Venkata Appaji, Dr. Gomatam V S Acharyulu, " Image Encryption Using Enhanced Four Stage Encryption ", Journal Of Theoretical And Applied Information Technology 15th December 2017. Vol.95. No 23 Pp 6523-6533.

[78] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed, " An Image Encryption Approach Using Stream Ciphers Based On Nonlinear Filter Generator", Journal Of Theoretical And Applied Information Technology 15 July 2012. Vol. 41 No.1 Pp 1-10.