Image Encryption Based on Modified Logistic Map and DNA coding

K. Subhashini[1] and R. Amutha[2]
[1]*Department of ECE, Sri Sai Ram Engineering College, Chennai, Tamilnadu, India*
[2]*Department of ECE, Sri Sivasubramaniya Nadar College of Engineering, Chennai,Tamilnadu, India*
[1]subhashini.ece@sairam.edu.in, [2]amuthar@ssn.edu.in

***Abstract*— The proposed image encryption algorithm uses a modified logistic map and DNA coding. The DNA coding method employs the four base pairs of the DNA code. One of the eight DNA encoding rule is selected for encoding. Permutation of image pixel values is then performed. The DNA operation is chosen to achieve diffusion of the image pixel values. The combination of the chaotic system and DNA coding achieves the cipher image. The algorithm is able to withstand statistical and differential attacks. It offers a large key space, increases ciphertext security and improves encoding efficiency, according to theoretical analysis and experimental results.**

Keywords— Logistic Map, Image Encryption, DNA coding, Confusion, Diffusion

I. Introduction

In the digital era, everyone's life is now occupied by digital images. We commonly use public networks to share our vast photo collections with others in addition to storing them. The integrity and privacy of the shared photographs must thus be safeguarded. Nowadays, with the proliferation of multimedia information, data security is a very important issue. A growing number of people are becoming attached to the ongoing advancement and development of human society. The personal information that ought to remain confidential. There may be serious effects if the picture data is obtained illegally. Ensuring image security is crucial. Using a chaotic system to encrypt images is a smart choice, this is because of its high unpredictability, sensitivity to beginning values, all of which are consistent with the avalanche, diffusivity, and confusability of cryptography.

In the proposed operation [1] permutation-diffusion process was done parallel. This overcome the attackers attempt to crack the information. In [2] the diffusion technique was implemented by divide and conquer approach to achieve fast encryption. The image was split into three portions. The key stream was utilized for diffusion. Higher randomness and unpredictability was achieved by conducting an XOR operation between two integer sequences collected from distinct systems. In this work [3] the key sequences generated by a complex system shuffle the pixel values bit-wise, while the chaotic sequences generated by a neural network which was time-delayed, scrambled the pixel positions of dispersed images. In [4] image encryption was performed by implementing 3D bit-scrambling and diffusion operations. The eight bit planes of each grayscale image were extended to a third dimension to provide a 3D bit array. By rearranging all the rows, columns and layers, this 3D bit array was pseudo-randomly jumbled. Subsequently, the jumbled bit planes were employed to reassemble the randomized images. Additionally, the merged and shuffled images undergo a controlled diffusion operation.

To break the strong association between image pixels, the chaotic key was used with the Arnold transformation to scramble the image in [5]. A nonlinear chaotic fractional Mellin transform with apertured chaos and its filter bank was suggested. Two complementary chaotic apertures were added. The issue of repeated data in filter banks was resolved by using a unique method consisting of form filters [6]. The cipher image was obtained using substitution and permutation procedures based on chaos. Bit-level scrambling and block replacement were used in [7]. This work proposed a novel 1D chaotic map that was utilized to build an incoherence rotating chaotic measuring matrix. Confusion and Diffusion was performed using the proposed chaotic map [8]. The proposed encryption scheme used compressive sensing and sparse representation. An over complete learned dictionary combined to create sparse representation of the image [9]. The work suggested an image encryption technique that utilized four chaotic sequences for row wise and column wise confusion and diffusion process [10].

The paper is framed as: preliminaries in Section 2, proposed method is explained in Section 3, Section 4 shows the simulation results and conclusion is presented in Section 5.

II. Preliminaries

A. *Modified Logistic Map*

In this work a modified logistic map is utilized. The mathematical expression of the 1D chaotic map is represented by equation (1)

$$T_j = (abs\left(r * \left(1-\frac{r}{T_0}\right)(1-r^2)\right)mod1$$
(1)

The chaotic system shows a huge chaotic range and exhibits wide chaotic behaviour when the control parameter lies in the range $r \in [0, 100]$.

III. Proposed Encryption method

The proposed encryption method is exhibited in Fig.1. The proposed encryption algorithm encompass different steps. It includes chaotic key generation, DNA coding, permutation and DNA diffusion. The steps implemented in the encryption algorithm are detailed in the subsection.

A. Chaotic key generation

The initial condition T_0 and control parameter r are the two values used by the proposed chaotic map to generate different chaotic sequence. The generated chaotic sequences are of size 4xPxQ.

B. DNA coding

The algorithm is based on DNA coding rule. According to the Watson-Crick base pair rule there are eight rules. The DNA coding rule is chosen based on the chaotic sequence generated.

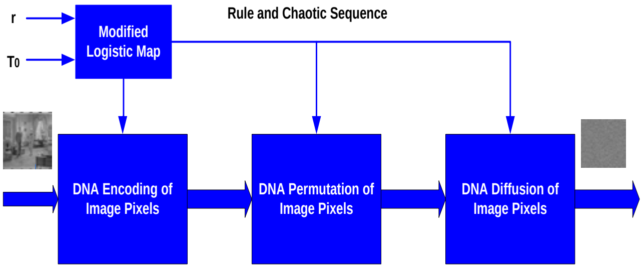

r
To
Modified Logistic Map
Rule and Chaotic Sequence
DNA Encoding of Image Pixels
DNA Permutation of Image Pixels
DNA Diffusion of Image Pixels

Fig.1 Block diagram of Proposed Encryption method

C. Permutation

Permutation operation is performed by using the index values of another chaotic sequence. It is a process where the position of the image pixels are changed.

D. Diffusion

Diffusion operation is performed by implementing one of the following operations $\oplus,\ominus,\oplus, and\ \odot$. It is a process by which the image pixel values are changed.

The Encryption steps are given by:

Step 1: The chaotic sequences of dimension PxQ are generated based on the modified logistic map.
Step 2: One of the eight DNA encoding rule is selected based on one of the chaotic sequence generated.
Step 3: Index value of another key sequence is used for pixel permutation of the image.
Step 4: Select one of the four DNA operation $\oplus,\ominus,\oplus\ and\ \odot$ to perform diffusion utilizing the next chaotic sequence.
Step 5: Arrange the vector into a matrix to obtain the cipher image.

IV. Simulation results

To examine the proposed encryption algorithm the simulation is done. The results obtained are analyzed in this part. The standard images from USC-SIPI database are used to verify the algorithm. The images chosen are of size 512x512 gray scale images. The plain image ‘Couple’ and its cipher image is depicted in Fig.2.

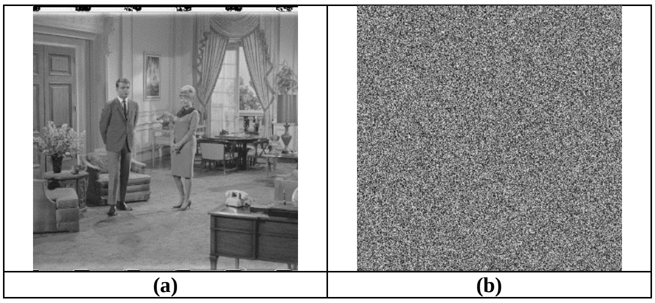

(a) (b)

Fig.2 (a) Couple Plain image (b) Couple Cipher image

A. Entropy analysis

The statistical measure entropy is used to identify the randomness of the cipher image. The theoretical value of information entropy of cipher image is 8 and it is lesser for plain image.

Table 1 Entropy Analysis

Test Image	Plain Image	Cipher Image				
		Proposed	[1]	[3]	[4]	[6]
Couple 512x512	7.2010	7.9993	7.9971	7.9890	7.9993	7.9993

The mathematical expression to calculate information entropy is given in equation (2)

$$H(n) = \sum_{i=0}^{L} p(n_i)\log_2\left(\frac{1}{p(n_i)}\right) \quad (2)$$

$p(n_i)$ is the gray level likelihood occurrence.

The entropy of plain image and cipher image in Table 1 shows that the proposed method ensures randomness as the value is close to 8. The entropy value of the proposed method is better than [1] and [3].

B. Correlation coefficient analysis

The Correlation coefficient gives the degree of similarity between neighbouring pixels of an image. For a good encryption algorithm the correlation coefficient value is equal to one for plain image and zero for cipher image. The correlation coefficient is defined by the equation (3)

$$R_{uv} = \frac{cov(u,v)}{\sqrt{B(u)B(v)}} \qquad (3)$$

where

$$cov(u,v) = \frac{1}{n}\sum_{i=1}^{n}(u_i - m(u))(v_i - m(v))$$

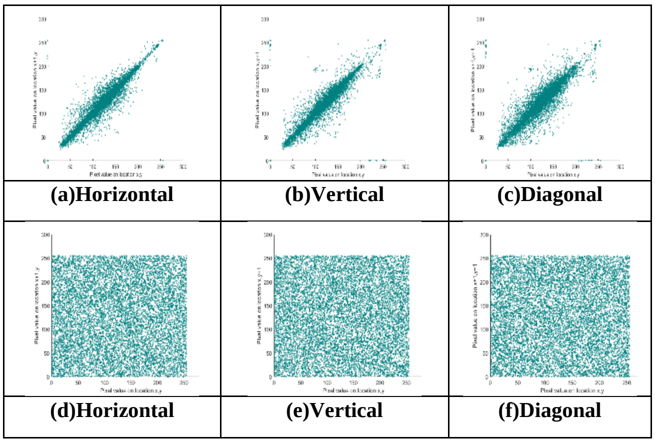
$$B(u) = \frac{1}{n}\sum_{i}^{n}(u_i - m(u))^2$$

$$m(u) = \frac{1}{n}\sum_{i=1}^{n} u_i$$

Table 2 Correlation Analysis

Correlation analysis of Couple Image			
Algorithm	Horizontal	Vertical	Diagonal
Plain Image	0.9422	0.8835	0.8371
Proposed	0.0028	-0.0066	0.0034
[1]	0.0100	0.0114	-0.0025
[4]	0.0082	0.0016	0.0150
[5]	−0.0026	−0.0057	0.0048
[6]	0.0016	-0.0070	0.0001

The image pixel correlation of plain and cipher is calculated by selecting 10,000 pixels in three directions horizontal, vertical and diagonal. The correlation coefficient between plain and cipher image is given in Table 2. The proposed method shows that the adjacent pixel correlation of plain image is high and equal to 1. The pixel correlation of cipher image is low and close to zero. The correlation of Couple cipher image of the proposed method is lesser than [1] and [4]. This shows that the proposed method competes well with the existing encryption algorithm.


(a)Horizontal (b)Vertical (c)Diagonal

(d)Horizontal (e)Vertical (f)Diagonal

Fig.3 a,b,c-Scatter plot of Plain image, d,e,f-Scatter plot of Cipher image

The ‘couple’ original and cipher image correlation is shown in Fig.3. The scatter plot between the pixels of plain image in the all three direction shows high correlation. The cipher image scatter plot shows negligible correlation between the neighbouring pixels in encrypted image.

C. *Histogram analysis*

The image histogram of original image is not uniformly distributed as the variance is large. The image histogram of cipher is uniform as its variance is less. The histogram of plain image is highly irregular whereas the histogram of cipher image is flat in Fig.4. The flat histogram indicates that no information is revealed in secret image. This ensures the information security of plain image.

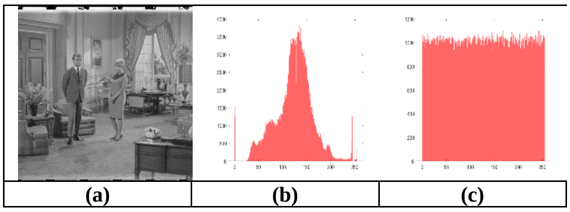

(a) (b) (c)

Fig.4 (a) Plain image (b) Plain Histogram (c) Cipher Histogram

D. *Differential attack analysis*

The encryption algorithm must possess high ability to withstand differential attack. This ability is verified using the unified average change intensity (UACI) and number of pixel changing rate (NPCR). E_1 and E_2 are two encrypted images obtained using the plain image and its one pixel changed image. The differential attack is an attempt to find the secret key which is used to for encryption. The intruder can identify the correlation between plaintext and its cipher text.

Table 3 NPCR Analysis

Test Image	Proposed	[1]	[5]	[6]
Couple 512x512	99.6006	99.6414	99.601	99.6172

The NPCR and UACI are defined using equation (4) and (5) respectively.

$$NPCR = \frac{\sum_{i,j} Difference(i,j)}{PxQ} x100\% \qquad (4)$$

$$UACI = \frac{1}{PxQ}\frac{\sum_{i,j}|E_1(i,j) - E_2(i,j)|}{L} x100\% \qquad (5)$$

where

$$Difference(i,j) = \begin{cases} 0, & E_1(i,j) = E_2(i,j) \\ 1, & Otherwise \end{cases}$$

Table 4 UACI Analysis

Test Image	Proposed	[1]	[5]	[6]
Couple 512x512	33.4840	33.5146	33.372	33.4746

The NPCR and UACI results are tabulated in Table 3 and Table 4. This shows that the values of the proposed method is close to ideal value. For an image of size 512x512 the theoretical value of NPCR is 99.5893%. The theoretical value of UACI for an image of size 512x512 is [33.3730%, 33.5541%]. The NPCR and UACI value of the proposed method passes the test.

V. Conclusion

The proposed image encryption technique is implemented by the modified logistic map and DNA coding. The key sequences are generated using the modified logistic map by varying the initial parameters. The encryption algorithm used the sequences to define a rule to perform DNA coding, Permutation and DNA diffusion. These techniques based on DNA method breaks the relationship between the neighboring pixel values of the image. The input image is converted into a vector and then the encryption process is carried out one by one to produce the cipher image. The experimental results exhibited confirms the improved security provided by the proposed algorithm. The entropy value of cipher image is almost equal to 8, the correlation of cipher is negligible, the histogram analysis of cipher is flat, differential attack analysis ensures to thwart the attack.

References

[1] Liu, L., Lei, Y., & Wang, D. (2020). A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation. *IEEE access*, *8*, 27361-27374. https://doi.org/10.1109/ACCESS.2020.2971759

[2] Ge, B., Shen, Z., & Zhang, J. (2022). Fast chaotic image encryption algorithm using a novel divide and conquer diffusion strategy. *IEEE Access*, *10*, 95986-96005. https://doi.org/10.1109/ACCESS.2022.3204873

[3] Wang, S., Hong, L., & Jiang, J. (2022). An image encryption scheme using a chaotic neural network and a network with multistable hyperchaos. *Optik*, *268*, 169758. https://doi.org/10.1016/j.ijleo.2022.169758

[4] Demirtaş, M. (2022). A novel multiple grayscale image encryption method based on 3D bit-scrambling and diffusion. *Optik*, *266*, 169624. https://doi.org/10.1016/j.ijleo.2022.169624

[5] Wang, J., Jiang, W., Xu, H., Wu, X., & Kim, J. (2022). Image encryption based on Logistic-Sine self-embedding chaotic sequence. *Optik*, *271*, 170075.

https://doi.org/10.1016/j.ijleo.2022.170075

[6] Wang, M. M., Zhou, N. R., Li, L., & Xu, M. T. (2022). A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank. *Expert Systems with Applications*, *207*, 118067.

https://doi.org/10.1016/j.eswa.2022.118067

[7] Ponuma, R., & Amutha, R. J. M. T. (2019). Encryption of image data using compressive sensing and chaotic system. *Multimedia Tools and Applications*, *78*, 11857-11881. https://doi.org/10.1007/s11045-019-00634-x

[8] Ponuma, R., & Amutha, R. (2018). Compressive sensing based image compression-encryption using novel 1D-chaotic map. *Multimedia Tools and Applications*, *77*, 19209-19234. https://doi.org/10.1007/s11042-017-5378-2

[9] Ponuma, R., & Amutha, R. (2019). Image encryption using sparse coding and compressive sensing. *Multidimensional Systems and Signal Processing*, *30*, 1895-1909. https://doi.org/10.1007/s11045-019-00634-x

[10] Subhashini, K., & Amutha, R. (2023, February). A Novel Image Encryption Algorithm Based On Chaotic Map. In *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICECCT56650.2023.10179657