iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** X **Month of publication:** October 2022

DOI: https://doi.org/10.22214/ijraset.2022.46887

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

Design and Analysis of a New Image Encryption Algorithm using Hyperchaotic System and Tent Map

Vegesna Girish Varma[1], K. RamaDevi[2]
[1]*Student, M.Tech (CE & SP), UCEK(A), JNTUK, Kakinada, Andhra Pradesh, India*
[2]*Assistant Professor, Deptartment of ECE, UCEK(A), JNTUK, Kakinada, Andhra Pradesh, India*

Abstract: ***Users transfer millions of images every day in the era of information technology. Serious issues could arise if the information included in these photographs is open to unauthorised usage. There are numerous methods for protecting images. One of the most successful and well-known methods is digital image encryption. Confusion and diffusion are the two main phases of an encryption algorithm. This paper proposes a new image encryption technique that uses a hyperchaotic system and a tent chaotic map. With the help of random numbers produced by the 6D hyperchaotic system, the original image gets confused. A tent chaotic map is then used to create a key to diffuse the permuted image. Security analysis and time complexity are used to evaluate the suggested image encryption method's effectiveness. The security is tested using entropy, correlation coefficient, differential attacks, histograms, keyspace, sensitivity, noise, and data cut attacks. Additionally, the outcomes are compared using various encryption methods. The proposed method achieves a high level of security.***
Keywords: Digital image encryption, hyperchaotic system, tent map, chaos, entropy, attacks.

I. INTRODUCTION

The regular process of digital image transmission over various networks involves the transfer of thousands of images every second. In healthcare networks, medical images are sensitive because wrong usage of them could lead to inaccurate diagnoses and subpar medical judgement. To prevent unauthorised access, high security standards are required while transferring military images via numerous networks. Social network users do not want their photographs to be accessible to others. These elements have elevated the importance of securing the data contained in digital images. Through a number of security measures, image secrecy is secured, making it impossible for an unauthorised individual to view the content of an image.

Data hiding, image watermarking, and encryption are the three main categories of image security techniques [1–5]. Data-hiding methods are used to integrate a hidden message that cannot be seen into the cover image. Digital data is inserted into the image when image watermarking techniques are applied, making the watermarked and original copies of the image visible. The key employed in image encryption methods transforms the digital input image into a noisy image that cannot be predicted or understood. Users are unable to access the encrypted image without the key.

A number of techniques are used for digital image encryption, including those based on DNA, the quantum approach, the chaos theory, and compressive sensing. Two crucial processes are used in image encryption methods. Confusion over which pixel arrangements are altered is the first stage. The second step, diffusion, depends on altering the pixel values. Inherent characteristics of chaotic-based approaches include non-periodicity, random behaviour, and sensitivity to initial conditions and control parameters. These characteristics make it possible to encrypt images successfully using chaotic-based techniques.

According to Chai et al. [6], chaotic-based digital image encryption systems can be split into two categories. One-dimensional chaotic maps are an example of a low-dimensional system that fits within this category. The second category includes high-dimensional systems such as hyperchaotic systems. The low-dimensional chaotic maps are comprehensible and practical due to their straightforward structures. Despite these intrinsic characteristics, these maps have a limited keyspace and low security levels. For the confusing procedure, Chen and Hu [7] developed a logistic-sine map-based approach for medical picture encryption. Liu et al. [8] employ a linked hyperchaotic system for pathological picture encryption. Zheng and Liu have created a brand-new technique for encrypting grayscale photos [9]. First, a novel 2D chaotic map system (2D-LSMM), based on both logistic and sine maps is presented. Next, a DNA-based encryption system is used, in which 2D-LSMM chaotic sequences are used to derive the encoding and operation rules for DNA sequences.

There are some limitations on related works, which are as follows:

1) Low sensitivity to the initial conditions and low keyspace.
2) Some encryption techniques are unable to recover the plain image when the encrypted image is subjected to noise and data cuts.
3) Because the histogram of the encrypted image is not flat, some of encryption techniques are vulnerable to statistical attacks.
4) The chaotic map's condition is independent of the plain image, which causes limitations in its ability to resist against differential attacks.

To get beyond the limits of low-dimensional chaotic systems, hyperchaotic techniques are applied. In terms of randomness, unpredictability, nonlinearity, and initial conditions, the hyperchaotic approaches performed better than the low-dimension chaotic methods.

The following is a summary of this paper's contributions:

a) The 6D hyperchaotic system and a chaotic map are integrated to ensure a high level of security.
b) The proposed algorithm offers strong resistance to brute force attacks because to its large keyspace.
c) The proposed algorithm for image encryption is extremely resistant to most attacks.

II. MATHEMATICAL UNDERSTANDINGS

A. Six-Dimensional Hyperchaotic System

According to mathematical analysis, chaotic functions are often nonlinear with dynamic behaviour. They consequently react in ways that are unpredictable. According to past studies, when compared to low-dimension chaotic functions, hyperchaotic functions exhibit far more complicated dynamical behaviour. A hyperchaotic system must have at least four dimensions. Low-dimension chaotic functions only have one positive Lyapunov exponent in contrast to hyperchaotic systems. Wang and Yu [10] define the 6D Hyperchaotic System as follows:

$$\begin{aligned} x_1 &= a\,(x_2 - x_1) + x_4 - x_5 - x_6 \\ x_2 &= cx_1 - x_2 - x_1x_3 \\ x_3 &= -bx_3 + x_1x_2 \\ x_4 &= dx_4 - x_2x_3 \\ x_5 &= ex_6 + x_3x_2 \\ x_6 &= rx_1 \end{aligned} \qquad (1)$$

where a, b, c, d, e, and r are constants; x1, x2, x3, x4, x5, and x6 are state variables of the 6D hyperchaotic system. The constant values chosen for this paper are: a = 10, b = 8, c = 28, d = 1, e = 8, and r = 3. By making this decision, the system is guaranteed to have two positive Lyapunov exponents that satisfy the requirement (sum of all exponents is negative).

B. Tent Chaotic Map

In mathematics, the tent map with parameter μ is the real-valued function f_μ defined by

$$f_\mu := \mu min\{x, 1 - x\} \qquad (2)$$

The graph of f has a tent-like form, therefore the name. f_μ defines a discrete-time dynamical system on it by mapping the unit interval [0, 1] onto itself for parameter values between 0 and 2. (equivalently, a recurrence relation). Specifically, iterating a point x0 in the range [0, 1] results in the sequence x_n:

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu x_n & for\ x_n < \frac{1}{2} \\ \mu(1 - x_n) & for\ \frac{1}{2} \leq x_n \end{cases} \qquad (3)$$

where μ is a positive real constant. Fig. 1 shows the Graph of the tent map function.

III. THE PROPOSED METHODOLOGY

The cutting-edge method employed a Tent Chaotic map and a six-dimensional hyperchaotic system to encrypt the input image. The use of the 6D hyperchaotic system improves encryption performance and security levels due to its complicated, highly dynamic behaviour and two positive Lyapunov exponents. Tent Chaotic map is swift and able to diffuse the permuted image.

A. Encryption

The encryption consists of two phases: confusion and diffusion. The layouts and values of the pixels are altered in accordance with each of these processes. The 6D hyperchaotic system is the foundation of the confusion step. First, a calculation is made to determine the system's initial condition, which is based on the plain image. We then select three sequences after the hyper chaotic system is iterated to create a new vector (x_2, x_4, and x_6). This vector's sorted number order is used to confuse the plain image. After confusing the plain image, the diffusion method is used to obtain the encrypted image. Our method's diffusion is based on a key produced by a Tent Chaotic map.

1) Use the following equation to determine the chaotic tent map's initial value, which depends on the plain image P:

$$Y(1) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} P(i,j)}{MxNx255} \quad (3)$$

2) To create a new sequence S with size MN, iterate the chaotic map (eq. 2) N_0 + MN times, skipping the first N_0 entries.

3) Calculate the key using the following formula:

$$K(i) = mod(floor(S(i) \times 10^{14}), 256) \quad (4)$$

The diffusion process modifies the image's pixel values, which results in the creation of a noisy image. By operating bit-wise exclusively OR operation of the confused image vector with the key K, the encrypted image is produced. In Algorithm section, thorough encryption procedures are described.

B. Decryption

In contrast to encryption, decryption involves the exact opposite steps. The steps listed below can be used to extract the plain image from the encrypted image:

1) To obtain the scrambled image, use a bit-wise exclusive OR operation to the encrypted image vector and key K.

2) A vector W is created from the scrambled image (D′) that is obtained in the previous step.

3) The following equation is used to restore each pixel to its initial place using the vector S created during the encrypting step:

$$ER(S_i) = W_i \text{ , } i = 1 : MN \quad (5)$$

1. To get the decrypted image, convert the vector ER to a matrix (D).

IV. ALGORITHM

The proposed image encryption algorithm is as follows:

Step 1: $i = 1$

Step 2: Create a P vector by converting the input image matrix.

Step 3: Calculate the hyperchaotic system's initial key as follows:

$$X_1 = \frac{\sum_{i=1}^{MN} P(i) + (MxN)}{2^{23} + (MxN)} \quad (6)$$

$x_i = mod\ (x_{i-1} \times 10^6, 1)$, i = 2, 3, …, 6
with the initial conditions; $x_1, x_2, \ldots, x_6$.

Step 4: You can create a new sequence L with dimension M x N by iterating the hyperchaotic system in (eq. 1) N_0 + MN/3 times and then discarding the N_0 values. (We choose three sequences from the system in (eq. 1): x_2, x_4, and x_6).

Step 5: Return the positions of L in vector S after sorting L in ascending order.

Step 6: Permit the image vector P to produce the following newly shuffled sequence

$$R_i = P(S_i),\ i = 1 : MN \quad (7)$$

Step 7: Create the tent map's initial state by utilizing (eq. 3)

Step 8: In order to obtain a new sequence S with size MN, iterate the tent chaotic map (eq. 3) N0 + MN times.

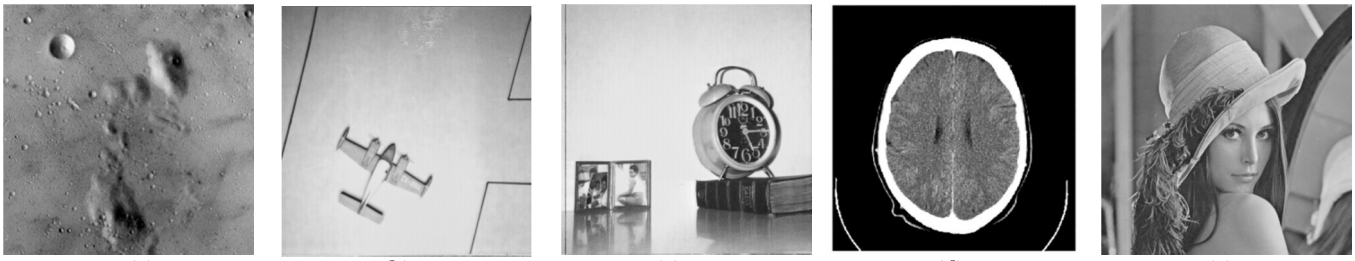
Step 9: Get the sequence K by iterating equation (eq. 4) MN times.

Step 10: Transform the matrix X into the pixel vector of a 1D image, X'.

Step 11: $Enc = R_i' \oplus K$

Step 12: Convert *Enc* into a 2D matrix C.

V. SIMULATION RESULTS



(a) (b) (c) (d) (e)

Fig. 1: The test grayscale images (a) Moon (512x512) [14], (b) Airplane (512x512) [14], (c) Clock (512x512) [14], (d) Img1 (512x512) [12], (e) Lena (512x512) [13]

The effectiveness of the proposed method is evaluated using various grayscale images, as shown in Fig. 1. The proposed algorithm is also evaluated against other image encryption algorithms. All experiments are carried out on a laptop with an 8 GB RAM and Core i5-1135G7 2.4GH CPU running MATLAB (R2020a).

In seven tests, the proposed encryption method is evaluated using entropy, noise and data cut attacks, correlation coefficients, differential attack, histograms, keyspace, and encryption quality. The parameters used in our algorithm is the iteration number N0 = 1000.

A. Entropy

Information entropy calculates the image's randomness. Entropy is described mathematically as follows:

$$H(m) = \sum_{i=1}^{w} P(m_i) log_2 \frac{1}{P(m_i)} \qquad (8)$$

where P(m) is the probability of appearance of m. For grayscale images, the maximum value of entropy is 8. The randomness of the image's pixels is higher when the entropy number is close to 8. As part of this experiment, we encrypt the grayscale test images using the proposed algorithm and calculate the entropy values of the encrypted images, which are shown in Table 1. We can see from the observations that every entropy number is close to 8, which indicates that the encrypted images are truly random. Using our algorithm and the other encryption algorithms described in Table 2, the second test image (i.e., Lena) is encrypted. As can be seen, when compared to the various methods in Table 2, our presented method has a greater entropy value. We draw the conclusion from this test that our proposed technique ensures producing encrypted images with great randomness.

TABLE I: Encrypted Images entropy

Test image	Entropy
Moon	7.9991
Airplane	7.9992
Clock	7.9983
Img1	7.9993
Lena	7.9993

TABLE II: Entropy value of our algorithm and other algorithms

Method	Entropy
Proposed	7.9993
[15]	7.9973
[16]	7.9993
[17]	7.9971
[18]	7.9971

B. Correlation Coefficient

In the input images, the neighbouring pixels frequently show a strong association in the diagonal, horizontal, and vertical axes. This correlation must be reduced for an encryption scheme to be effective. The following formula calculates the correlation coefficient between any two neighbouring pixels, A and B:

$$r_{A,B} = \frac{E((A - E(A))(B - E(B)))}{\sqrt{D(A)D(B)}}$$

$$E(A) = \frac{1}{s}\sum_{i=1}^{s} A_i \qquad (9)$$

$$D(A) = \frac{1}{s}\sum_{i=1}^{s}(A_i - E(A))^2$$

where the integer s referring to the total number of adjacent pixels; D(A) and E(A) stand for the variance and expectation of A, respectively.

In the horizontal (H), vertical (V), and diagonal (D) directions of the grey test images and their encrypted versions, Table 3 lists the correlation coefficient values for each. The correlation coefficient values of the test images are all close to one, whereas the correlation coefficient values of the encrypted images are close to zero. Table 4 provides a comparison of Lena image with other methods.

TABLE III: Correlation coefficient values

Test Image	Direction	Plain image	Encrypted image
Img1	V	0.9848	0.0016
	H	0.9723	0.0008
	D	0.9649	-0.0037
Moon	V	0.9716	0.0002
	H	0.9321	0.0013
	D	0.9212	-0.0021
Airplane	V	0.7589	-0.0031
	H	0.8465	-0.0026
	D	0.7362	0.0028
Clock	V	0.9792	0.0013
	H	0.9768	-0.0006
	D	0.9639	-0.0013

Table IV: Comparison of the Correlation Coefficient Values
Between our algorithm and other algorithms

Method	H	V	D
Proposed	0.0049	0.0004	0.0001
[15]	−0.0053	−0.0012	0.0050
[16]	0.0019	0.0069	0.0200
[17]	-0.0056	0.0006	0.0018
[18]	-0.0059	-0.0064	-0.0003

C. Data Cut and Noise attacks

When images are exchanged over the network, noise or cropping (data cut) attacks are possible. Algorithms for image encryption should be resistant to noise and cropping attacks. The decrypted image quality is assessed using the widely used metric PSNR (peak signal to noise ratio). The PSNR for the original and decrypted images, I_O, and I_D according to mathematics is:

$$PSNR = 10\ x\ log_{10}\left(\frac{255^2}{MSE}\right)\ (db) \qquad (10)$$

where MSE stands for mean square error:

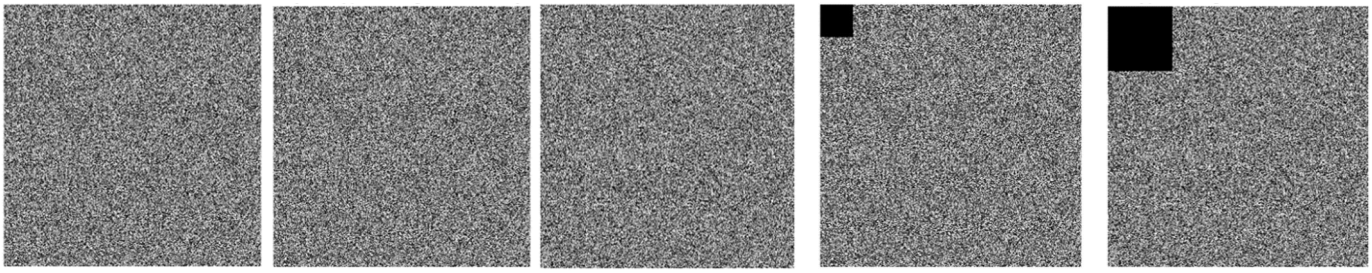
$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|OI(i,j) - EI(i,j)|^2 \qquad (11)$$

High image quality is indicated by a higher PSNR value. Original and decrypted images are indistinguishable for a PSNR > 35. The purpose of this experiment is to evaluate robustness against noise and data cut attacks. In this experiment, the new technique is used to decrypt an encrypted image that has been contaminated with "salt and peppers" noise at two distinct levels, 0.002 and 0.005. Additionally, a data cut of 64 x 64 and 128 x 128 is used to attack the encrypted images before the new approach is used to decrypt them. Table 5 displays the PSNR for the five test images with noise and data cuts.

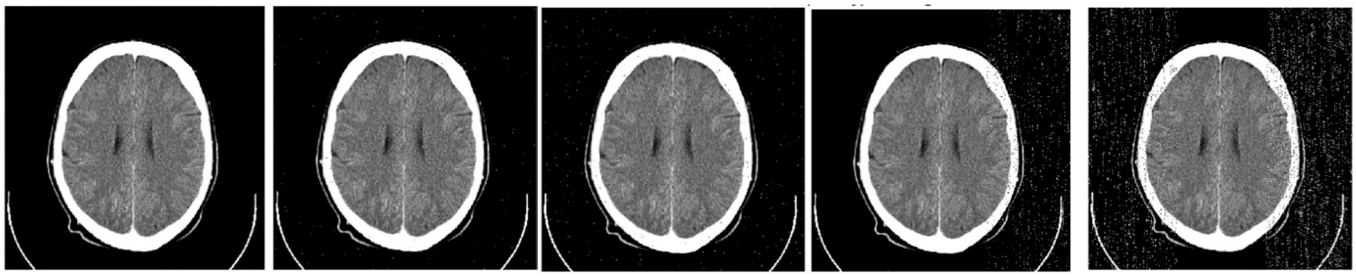
The PSNR is reduced to 20dB when the encrypted image is attacked with a data cut off size of 128 x 128, which is a reasonably large cut off (i.e., the encrypted image lost 1/8 information). The decrypted image is recognizable despite the lower PSNR values. Fig. 2 illustrates the noise and data cut attacks for an encrypted image, showing how the reader can quickly identify the contents of the decrypted images in various scenarios. The new method is therefore robust and resistant to various attacks.

TABLE V: PEAK SIGNAL TO NOISE RATIO (PSNR) (DB) VALUES FOR
NOISE AND DATA CUT ATTACKS

Test Images	Data cut with block size:		Salt and Pepper with noise level:	
	64 x 64	128 x 128	0.002	0.005
Moon	22.3337	17.2738	32.9294	28.5912
Airplane	26.0084	21.2101	35.2736	31.9938
Clock	25.1581	21.3478	36.3196	31.3013
Img1	27.9154	21.6533	35.4043	32.8557
Lena	26.7752	20.7368	35.4221	31.7593



(a) (b) (c) (d) (e)



(f) (g) (h) (i) (j)

Fig. 2: Noise and data cut attacks; (a) The encrypted image of Img2, (b) noisy encrypted image with 0.002, (c) noisy encrypted image with 0.005 and (d) encrypted with 128x128 data cut, (e) encrypted image with 64x64 data cut. (f-j) Images of the decrypted (a-e)

D. Differential Attack

By figuring out the relationship between the original and encrypted images, the attacker hopes to decrypt the encrypted images without needing the key in this attack. Small modifications in the original image's pixels have a big impact on the encrypted version, making it more challenging for hackers to decrypt the encrypted version. This attack must be prevented by strong image encryption methods. Robustness to this attack is evaluated based on the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values obtained from following equations:

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\ x\ 100\ (\%)$$

$$D(i,j) = \begin{cases} 0 & if\ E_1(i,j) = E_2(i,j) \\ 1 & if\ E_1(i,j) \neq E_2(i,j) \end{cases} \qquad (12)$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|E_1(i,j) - E_2(i,j)|}{255}\ x\ 100\ (\%)$$

Symbols E_1 and E_2 refer to two encrypted images i.e., plain image and the modified image (made by changing one pixel in the plain image). The image has a width of M pixels and a height of N.

Here, we compare the NPCR and UACI values between the two encrypted images in Table 6 to examine the effectiveness of our proposed methodology in defending against differential attacks. NPCR should be 99.6094%, and UACI should be 33.4635% with respect to their ideal values. Every value in Table 6 is near to their ideal values. A comparison of our approach and other image encryption algorithms can be seen in Table 7 for the original Lena image. The outcomes demonstrate how well our proposed method can withstand differential attacks.

TABLE VI: NPCR AND UACI PERFORMANCES

Test image	NPCR (%)	UACI (%)
Img1	99.6193	33.4091
Moon	99.5663	33.3844
Airplane	99.6250	33.4544
Clock	99.6124	33.3804

TABLE VII: COMPARISON OF NPCR AND UACI

Method	NPCR	UACI
Proposed	99.6067	33.4449
[15]	99.6216	33.6642
[16]	99.6174	33.4322
[17]	99.6216	33.5848
[18]	99.6197	33.0443

E. Histograms

The distribution of pixels in the image is shown by the histogram. The histogram for an encrypted image should be flat to make it impossible for attackers to predict any image data. Additionally, the histograms of the plain image and the encrypted image shouldn't be same. Using the new approach, three standard grayscale images Moon, Airplane, Clock were encrypted. The histograms of the encrypted images created using our method are uniform and distinct from those of the equivalent plain image histograms, as can be shown in Fig. 3. To ensure that the histogram of the encrypted image is uniform, a further experiment is conducted. The chi-square test (X^2) used in this experiment is calculated by [19]:

$$\chi^2 = \sum_{i=1}^{256} \frac{(O_i - EV)^2}{EV} \qquad (13)$$

where EV = O/256 is the expected frequency of each grey value and O_i is the rate of occurrence of grey value i. The value of $X^2_{(a,d)}$ is 293.2478, where 0.05 is for significance and d is 255 representing degrees of freedom. Table 8 displays the X^2 values of the encrypted image. As all of the values are below 293, the histogram of the images encrypted using our proposed algorithm is uniform. These outcomes validate the effectiveness of the new algorithm.

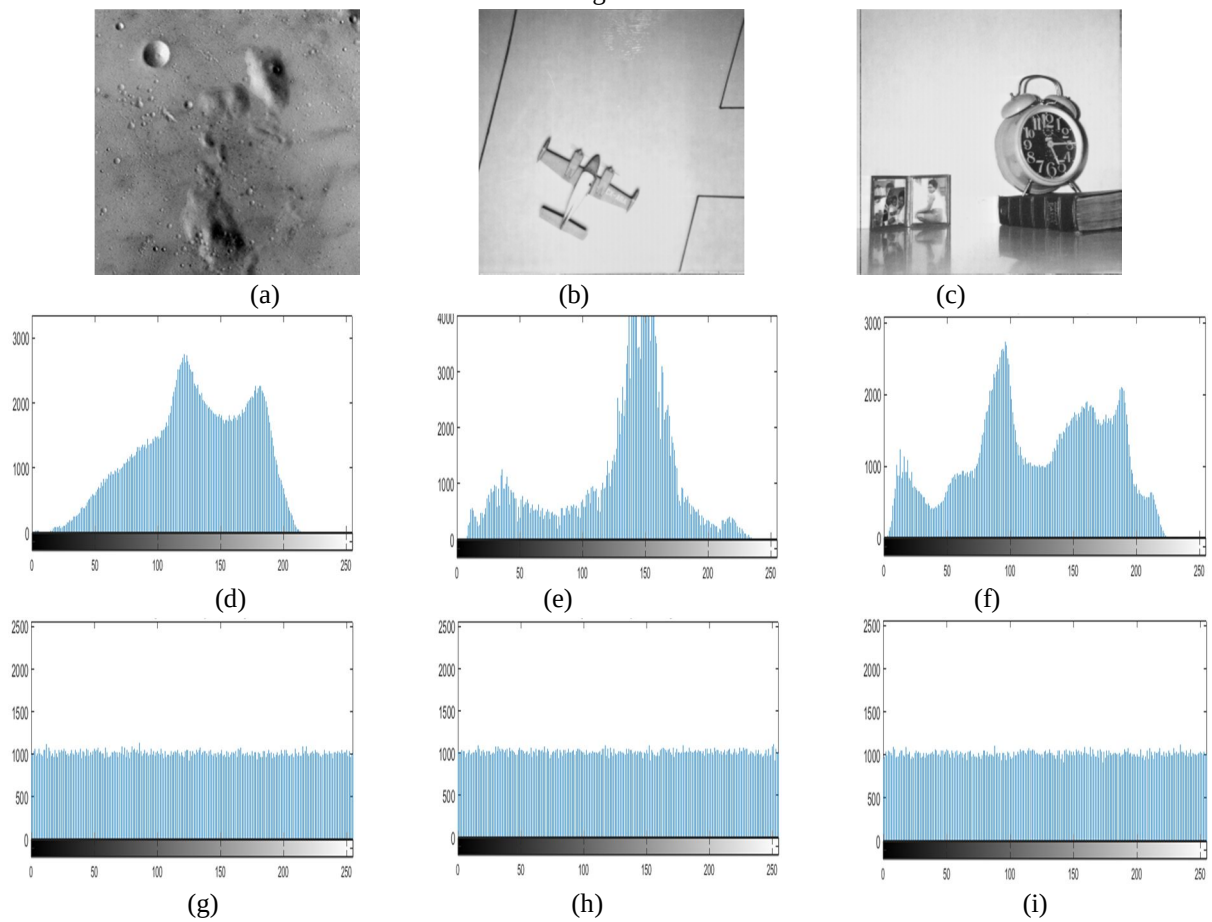


Fig. 3: Histogram analysis; (a) Moon, (b) Airplane, (c) Clock, (d) Histogram of (a), (e) Histogram of (b), (f) Histogram of (c), (g) Histogram of encrypted image in (a), (h) Histogram of encrypted image in (b), (i) Histogram of encrypted image in (c)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue X Oct 2022- Available at www.ijraset.com

TABLE VIII: Chi-Square analysis

Test image	Encrypted Image
Moon	213.2031
Airplane	260.7637
Clock	214.5684
Img1	271.1836
Lena	213.7773

F. Keyspace

The size of the keyspace is important to the encryption process. If the keyspace size is greater than 2^{100}, the encryption technique is resistant to brute force attacks. Different security keys are included in the proposed encryption algorithm: x_1, x_2, x_3, x_4, x_5, x_6, N_0, a, b, c, d, e, and r. If we assume that the precision of the initial value is equal to 10^{16}, then the total keyspace is greater than N_0 x 10^{96}, indicating robustness to a brute force attack.

G. Encryption Quality

1) *Maximum Deviation:* By comparing the pixel values between the plain and encrypted images, the effectiveness of encryption is measured. If this difference is significant, the encryption algorithm is considered to be efficient. Calculating the maximum deviation includes:

$$D = \frac{M_0 + M_{255}}{2} + \sum_{i=1}^{254} M_i \qquad (14)$$

where M_i is the histogram difference between the plain image at index i and the encrypted image at index i. The strong difference between the plain image and the encrypted image is indicated by the high value of D. The maximum values for our proposed methodology are shown in Table 9. Large values show that the images encrypted with the proposed algorithm are completely distinct from the plain image, indicating the excellent security performance of our algorithm.

TABLE IX: Analysis of Maximum deviation

Test image	Maximum Deviation
Moon	221016
Airplane	197492
Clock	153941
Img1	371360
Lena	169850

2) *Deviation from Uniform Histogram:* An encrypted image with a consistent histogram should be produced by a competent encryption technique. The quality of the encryption algorithm evaluated by histogram deviation, which is defined by:

$$H_{C_i} = \begin{cases} \frac{M \, x \, N}{256}, & 0 \leq C_i \leq 255 \\ 0, & elsewhere \end{cases} \qquad (15)$$

$$D_H = \frac{\sum_{C_i}^{255} |H_{C_i} - H_c|}{M \, x \, N}$$

The encrypted image's histogram is referred to as the H_C. The results presented in Table 10 demonstrate low values of D_H that point to strong encryption quality of the proposed technique. A lower value D_H indicates the histogram's uniformity and prove high encryption quality.

TABLE X: Analysis of deviation from a Uniform histogram

Test image	Histogram Deviation
Moon	0.0232
Airplane	0.0250
Clock	0.0234
Img1	0.0253
Lena	0.0223

H. Computational Complexity

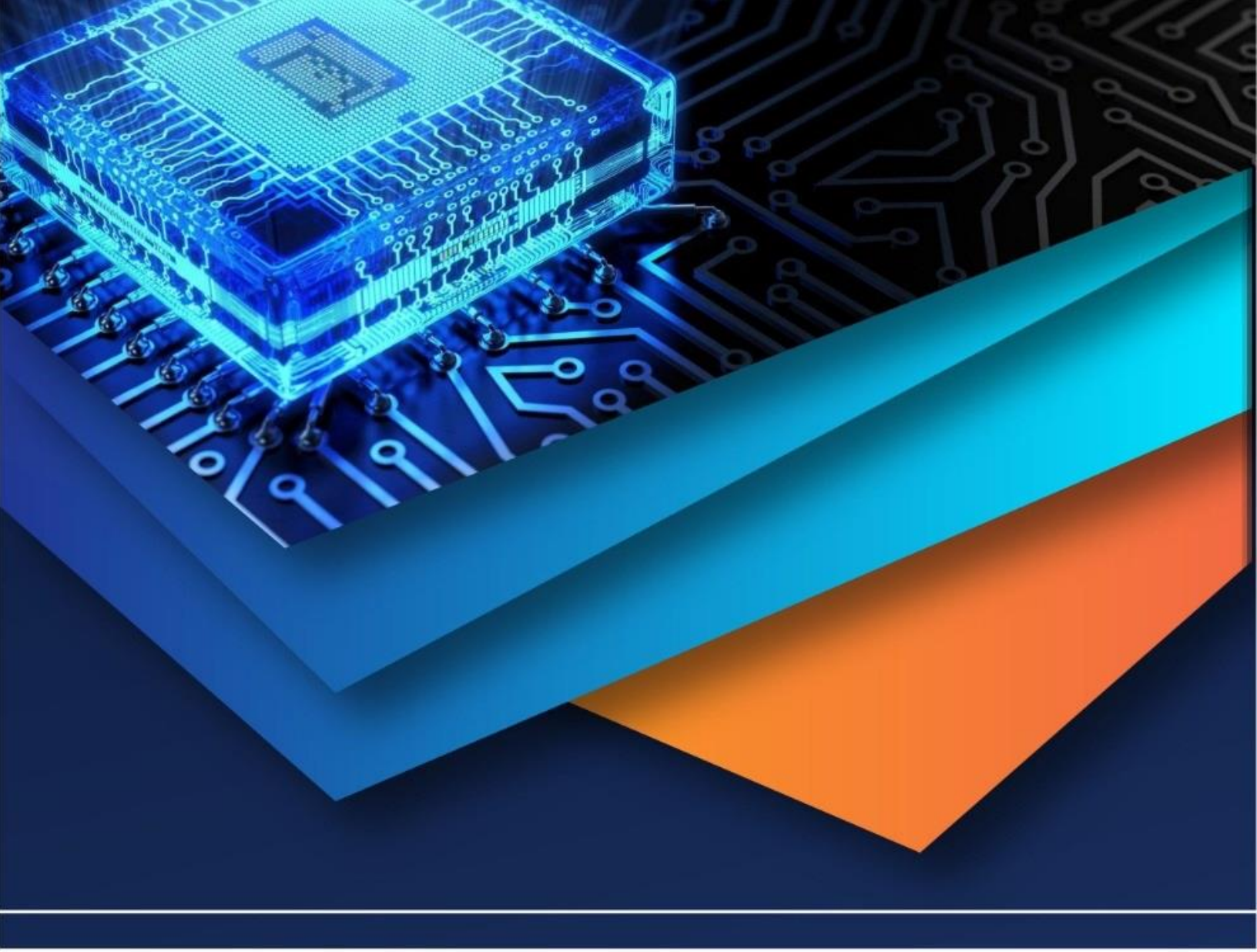
The steps necessary to complete the encryption process are used to evaluate the computational complexity of the algorithm. For a plain image of size M x N, the proposed algorithm's confusion steps have an *O(MxN)* time complexity. The time complexity for the key generation and diffusion stages is *O(MxN)*. As a result, the overall time complexity of our proposed algorithm is *O(MxN)*.

VI. CONCLUSIONS

This paper introduced a new grey image encryption algorithm. The Tent Chaotic map is combined with a 6D hyperchaotic system in this algorithm. First, we choose three sequences from a 6D hyperchaotic system before changing the pixel positions. The Tent chaotic map is then used to change the pixel values of the shuffled image. The new technique is sensitive to small variations in the secret key and pixel distribution, producing a completely different encrypted image. As a result, the proposed algorithm successfully defends against the differential attack. When the keyspace size is large enough, the new algorithm can withstand a brute force attack. Additionally, information entropy, correlation coefficients, noise and data cut attack, and histogram are used to evaluate the security performance of the novel algorithm. The results demonstrate that the proposed algorithm performs well when encrypting grayscale images when compared to other recent encryption algorithms.

REFERENCES

[1] Abdel-Aziz, M.M., Hosny, K.M. & Lashin, N.A. Improved data hiding method for securing color images. Multimed Tools Appl 80, 12641–12670 (2021), doi: 10.1007/s11042-020-10217-9.
[2] K. M. Hosny, M. M. Darwish, K. Li and A. Salah, Parallel Multi-Core CPU and GPU for Fast and Robust Medical Image Watermarking, in IEEE Access, vol. 6, pp. 77212-77225, 2018, doi: 10.1109/ACCESS.2018.2879919.
[3] Hosny, K.M., Darwish, M.M. Robust color image watermarking using invariant quaternion Legendre-Fourier moments. Multimed Tools Appl 77, 24727–24750 (2018), doi: 10.1007/s11042-018-5670-9.
[4] Dolendro Singh Laiphrakpam, Manglem Singh Khumanthem, Medical image encryption based on improved ElGamal encryption technique, Optik, Volume 147, 2017, Pages 88-102, ISSN 0030-4026, doi: 10.1016/j.ijleo.2017.08.028.
[5] Li, Y, Yu, H, Song, B, Chen, J. Image encryption based on a single-round dictionary and chaotic sequences in cloud computing. Concurrency Computat Pract Exper. 2021; 33:e5182, doi: 10.1002/cpe.5182.
[6] Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process, 2019, 155, 44–62.
[7] Chen, X.; Hu, C.-J. Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi J. Biol. Sci. 2017, 24, 1821–1827.
[8] Liu, H.; Kadir, A.; Liu, J. Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system. Opt. Lasers Eng. 2019, 122, 123–133.
[9] Zheng, J.; Liu, L. Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Process. 2020, 14, 2310–2320.
[10] Wang, J.; Yu, W.; Wang, J.; Zhao, Y.; Zhang, J.; Jiang, D. A new six-dimensional hyperchaotic system and its secure communication circuit implementation. Int. J. Circuit Theory Appl. 2019, 47, 702–717.
[11] R Noha, HA HossamEldin, EE Said, and EA Fathi, (2015), Hybrid ciphering system of image based on fractional Fourier transform and two chaotic maps , International Journal of Computer Applications (0975 – 8887), 119 (11) 12–17.
[12] Category: Computed Tomography Images of Mikael Häggström's Brain, Sept. 2022, [online] Available: https://commons.wikimedia.org/wiki/Category:Computed_tomography_images_of_Mikael_H%C3%A4ggstr%C3%B6m%27s_brain.
[13] File:Lenna (test image).png, Sept. 2022, [online] Available: https://en.wikipedia.org/wiki/File:Lenna_(test_image).png.
[14] SIPI Image Database, Sept. 2022, [online] Available: https://sipi.usc.edu/database/database.php?volume=misc.
[15] Tian, P.; Su, R. A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding. Sensors 2022, 22, 5325. doi: 10.3390/s22145325.
[16] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in IEEE Access, vol. 9, pp. 37855-37865, 2021, doi: 10.1109/ACCESS. 2021. 3063237.
[17] Q. Lu, C. Zhu and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," in IEEE Access, vol. 8, pp. 25664-25678, 2020, doi: 10.1109/ACCESS.2020.2970806.
[18] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," in IEEE Access, vol. 9, pp. 120596-120612, 2021, doi: 10.1109/ACCESS.2021.3108789.
[19] A. Banu S and R. Amirtharajan, ''A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach,'' Med. Biol. Eng. Comput., vol. 58, no. 7, pp. 1445–1458, Jul. 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY