A Fast and robustColor Image Encryption Scheme by Huffman Compression, 5D Chaotic Map and DNA Encoding

S. Navaneethan[1,*], G. Kalamathipriya[1],
M. S. Mohamed Keyasudeen[1] and K. Parthiban[2]

[1]*Department of CSE, Shivani Engineering College, Trichy, India*
[2]*Department of AI&DS, Shivani Engineering College, Trichy, India*
E-mail: Ns2066@srmist.edu.in
[*]*Corresponding Author*

Received 02 April 2024; Accepted 07 May 2024

Abstract

In the era of information technology, securing the real-time digital image is the greatest challenge especially colour image. In this paper, a colour image encryption scheme is introduced to secure the image based on compression-then-encryption concept. Theproposed method is a hybrid combination of the Chaos techniques for key generation, Huffman Encoding/compression for compression and avoiding colour decomposition, scrambling for more confusion and DNA Encoding for reducing storage size. In order to enhance security, scrambled data are converted to the Deoxyribonucleic acid (DNA) sequence, make ADD operation and apply the complementary rules to attain the cipher image. Experimental results have been proved as robustness, accurate and high security against attacks, malicious attacks, differential attacks and statistical attacks. Furthermore, results show that the time speed is faster minimum storage space than the existing colour image encryption scheme.

Keywords: DNA, image encryption, 5D chaotic map, Huffman compression, scrambling.

Journal of Graphic Era University, Vol. 12_2, 185–206.
doi: 10.13052/jgeu0975-1416.1221

1 Introduction

Information security is a vast field in IT industry. It would face the greater issue which affects the national security, social media and personal information. Basically, image has some properties such as high redundancy, large date space storage,vivid and high resource allocation compared to text. Due to the larger data space and high redundancy, traditional techniques especially 3-DES, RSA, AES, are not well suited to the image because of its high computational complexity, high resource utilization and low security [1–3]. The various techniques related to images and text are explained to calculate the time consumption of AES, DES, 3-and DES [4, 5]. The conclusion was that the high time complexity while using for images. The another survey paperhas explained the various methods applied to the encryption such as suduko, XOR, Scrambling, permutation, and Chaos Theory [6–8]. Hence, the chaos technique could be far better security and well-suited to key generation especially images. The research work concentrates mainly on the Chaos techniques for key generation, Huffman Encoding for compression and avoiding colour decomposition, DNA Encoding for reducing storage size. Chaotic system is a famous and next generation technique which is sensitive to initial values and high complexity. It has some characteristics such as dynamic, ergodicity, reproduction and PRP to make the encryption strong and avoiding attacks [9]. It provides stronger large key space. Larger key space provides higher security. The chaotic algorithm is generated for image encryption which is used to encrypt the data. It generates the PRP based on the non-linear dynamics [10, 11]. Client Image data and their keys are transmitted over the cloud directly. CSP could take over the data control in the cloud. So, client can face the privacy issues due to the loss of control [2]. Thereafter, some techniques introduced which is passed the partial encrypted image to the cloud. It creates huge complexity while selecting the partial image data [1]. Later, image encrypted by the user and stored to the cloud and minimized the computational complexity to ensure the privacy. Image Owner holdsthemetadata information for privacy assurance. Hence, the proposediPrivacy-Privacy preserving Chaos based Symmetric and Efficient Encryption Technique(SEET) is evaluated by using simple and light-weight method to ensure security and privacy [12, 13]. It assures the confidentiality, integrity and robustness against attacks [14, 15]. Xu et al. generated a novel method which is encrypted the image by bit-level scrambling based on chaotic map and ensures high performance compared with other schemes [16]. Brindha et al. introduced the image encryption technique efficiently and applied a compression algorithm depends on the famous Chinese remainder theorem [17]. Yuan et al. implemented a new encryption with the movement of pixels by diagonal method to encrypt and 5D chaotic map generated the secret keys to achieve the high-level cryptosystem [18]. It has been proved the efficient encryption/decryption with various security analysis and performance metrics. It was proved that the parallel system makes fast and strong. Sun et al. implemented the encryption technique with image which included the different scrambling techniques. Further, DNA encoding are applied to achieve robust against attacks [19, 20]. The 5D hyper-chaotic system generated the secret keys which would be sensitive, reliable, secure and robust from malicious attacks. It was proved that its time speed was minimised compared to other schemes. Wu et al. introduced a colour image encryption based on 1D with multiple improvements and DNA operations [21]. It was proved as robustness, secure from geometric attacks. Samiullah et al. implemented the novel image encryption with the combination of three chaotic systems, chaotic key generator, scrambling technique, SHA Algorithm with DNA sequence [22]. It ensures multilevel security to improve the confusion and diffusion to achieve high security. Mondal et al. implemented image encryption with simple technique (light-weight method) and better security performance by using chaos system and DNA operations [23, 24]. Ravichandran et al. implemented the different chaos based algorithm which is immutable and applied to images [25]. It proved that its algorithm was strong and reliable.

The remaining paper contains: Section 2 introduced the Huffman Compression, 5D hyper chaotic system and DNA coding. Section 3 represents the encipher and decipher of the proposed system. Section 4 briefly explains the experimental results. Section 5 analysis the security and finally conclude the efficiency of the proposed scheme.

2 Contribution

- The colour image are proceed directly to encryption without quality loss instead of not decomposed into three colour formation.
- The proposed colour encryption scheme achieves low time cost compared to related colour and grey-level encryption scheme.
- The proposed scheme minimises storage size because of using DNA technique.
- The proposed scheme has applied the Huffman Compression to colour image and proved as the higher security instead of using text.

3 Preliminary Works

3.1 Huffman Encoding

Huffman Coding is an entropy based technology which is lossless compression and basically applied to the text and well suited too [26, 27]. The sample Huffman tree representation is shown as Figure 1.

Figure 1 shows the Huffman tree of 4*4 pixel values and produces the code conversion based on the counting of values of pixel. Theplain and original colour image is first applied to the Huffman coding without decomposition of three different colours. Even though, it is retrieved thecolour image without any loss. The input image *I* is reduced to ‘n’ number of pixel values based on the size of the image i.e. 4*4 image size = 16 pixel values.

The probability of occurrence of a certain pixel intensity value is as follows. Where $\mathrm{j} = \{1, 2....\mathrm{m}\}$j ‘m’ acts as a distinct pixel intensity in an image. Where prob_ $\mathrm{pixel_j}$ acts as a probability of a specific pixel ‘j’ in an image, freq_$\mathrm{pixel_j}$ represents the number of frequency(tuple) of a specific pixel ‘j’

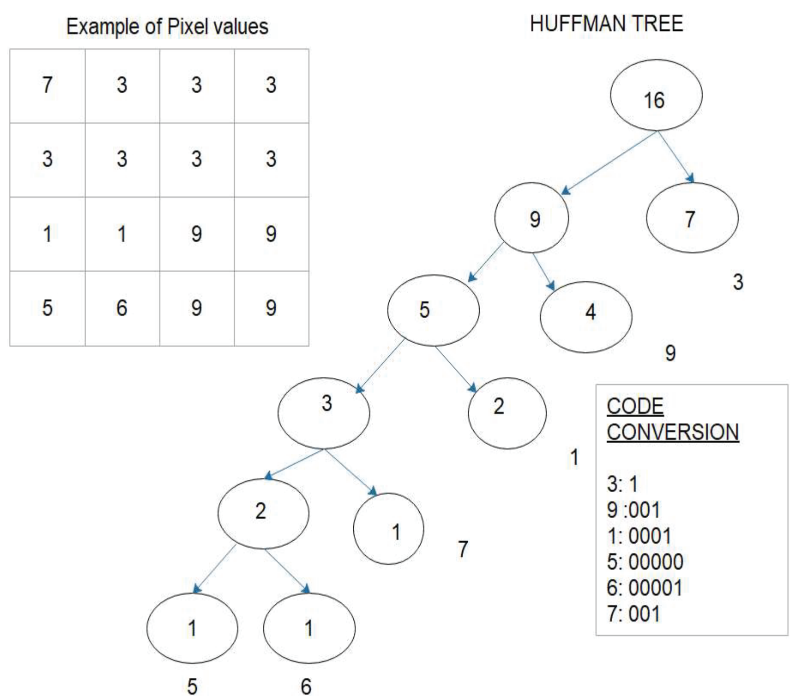

Figure 1 Example of Huffman tree.

with a certain intensity value i.e. '3' pixel value occurs '7'(freq_pixelj) times, tot_pixel represents the total number of pixels in an image (16 values). The req_pixel act as the leaf nodes to construct the Huffman tree. Combine the last two LSB leaf node merge into a new node. Then, sort the nodes based on the new probability nodes in the 'lookup table'. Continue the processes till it gets the single node with probability 1.0. The final node known as 'root'. Thereafter, move to the tree backwards (right to left) and different bits is assigned to the different branches. Thebinary code is calculated from the freq_pixel_j and Huffman tree.

3.2 5D Chaotic System

The following equation of 5D Hyperchaotic system [18] could be generated below

$$\begin{aligned} X &= (a(y-x)) + (yzu) \\ Y &= (b(x+y)) + v - (xzv) \\ Z &= (-cy) - (dz) - (eu) + (xyu) \\ U &= -fu + xyz \\ V &= -g(x+y) \end{aligned} \tag{1}$$

where a,b,c,d,e,f are control parameters. Consider the control parameters value as "$a = 30$, $b = 10$, $c = 15.7$, $d = 5$, $e = 2.5$, $f = 4.45$ and $g = 38.5$" to generate chaotic sequences as Ref(3) [10]. System Trajectories are represented in Figure 2.

3.3 DNA Encoding Scheme

Deoxyribonucleic acid (DNA) [20, 22] molecules made up of nucleotides. It has four types such as A, C, G and T. A-Adenine, C – Cytosine, T – Thymine and, G – Guanine. DNA is two twisted stranded around each other. A, C, G and T indicated as 00,11,10,11. DNA rules, DNA-ADD operation, DNA-SUB operation and rule of complement, shown in Tables 1, 2 and 3, used for encoding/decoding. Table 1 shows the first four rules of DNA sequence.

DNA complementary rule must satisfy the following conditions:

$$X \neq A(x) \neq A(x)) \neq A(A(x))) = A(A(A(A(x)))) \tag{2}$$

where A(x) represents as a base pair of x which differs at least one bit of x.

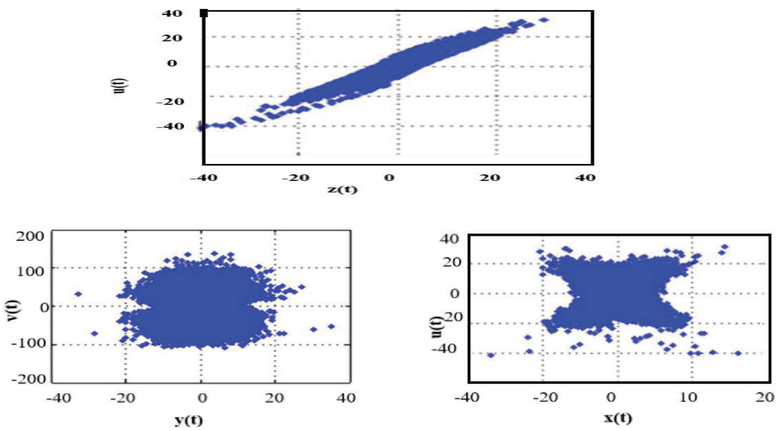

Figure 2 System Trajectories of (3) with initial values and control parameters.

Table 1 DNA sequence rules

Rules	1	2	3	4
00	A	A	C	G
01	C	G	A	A
10	G	C	T	T
11	T	T	G	C

Table 2 DNA-ADD operation

ADD	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 3 DNA-SUB operation

SUB	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

4 Proposed Image Encryption Scheme

The proposed work with different formats such as **JPG, JPEG, GIFF, BMP, PNG,** and so on, are evaluated to show the performance of the technique and time complexity. The collection of more than **1000 images** to test with various attacks such as malicious attacks, exhaustive attacks, brute-force attack to assure the robustness, security analysis to reach the goal.

The proposed scheme is divided into three modules namely Huffman Compression, Scrambling and DNA-based Encryption Module. Each module has different function to attain the cipher image. The 5D Hyperchaotic system are generated the chaotic key sequences which is applied to the encryption process. Consider the image 'P' size as M*N. Then, the original image is entered into the three modules and finally produces the encrypted image.

4.1 5D Hyperchaotic Key Generation

Step 1: Generate the initial values x, y, z, u and v of 5D Hyperchaotic system [18] as follows:

$$\begin{aligned} \mathrm{X} &= \mathrm{mod}(\mathrm{x}+\mathrm{y}+\mathrm{z}+\mathrm{u}+\mathrm{v},1) \\ \mathrm{Y} &= \mathrm{mod}(\mathrm{x}+\mathrm{y},1) \\ \mathrm{Z} &= \mathrm{mod}(\mathrm{y}+\mathrm{z},1) \\ \mathrm{U} &= \mathrm{mod}(\mathrm{z}+\mathrm{u},1) \\ \mathrm{V} &= \mathrm{mod}(\mathrm{u}+\mathrm{v},1) \end{aligned} \tag{3}$$

Where x^0, y^0, z^0, u^0, v^0 are the initial keys, mod(a,b) produces residue of 'a' divided by 'b'.

Step 2: By using the initial keys and control parameters, 5D Hyperchaotic system is iterated MN times to avoid the transient response R_0.

$$\mathrm{R0} = 400 + \mathrm{mod}((\mathrm{x0}+\mathrm{y0}+\mathrm{z0}+\mathrm{u0}+\mathrm{v0}) - [(\mathrm{x0}+\mathrm{y0}+\mathrm{z0}+\mathrm{u0}+\mathrm{v0})] * 1015, 400$$

And generate the five chaotic sequences K_1, K_2, K_3, K_4, K_5. All keys are converted to fixed length float numbers rather than long strings.

$$\begin{aligned} \mathrm{K}_1 &= \{\mathrm{x}^1, \mathrm{x}^2, \ldots \mathrm{x}^{\mathrm{MN}}\} \\ \mathrm{K}_1 &= \mathrm{abs}(\mathrm{x_i}) - [\mathrm{abs}(\mathrm{x_i})] * 10^{-15}, \mathrm{M}-\mathrm{i}) \\ \mathrm{K}_2 &= \{\mathrm{y}^1, \mathrm{y}^2, \ldots \mathrm{y}^{\mathrm{MN}}\} \\ \mathrm{K}_2 &= \mathrm{abs}(\mathrm{y_j}) - [\mathrm{abs}(\mathrm{y_j})] * 10^{-15}, \mathrm{N}-\mathrm{j}) \\ \mathrm{K}_3 &= \{\mathrm{Z}^1, \mathrm{Z}^2, \ldots \mathrm{Z}^{\mathrm{MN}}\} \end{aligned}$$

$$K_3 = \mathrm{abs}(z_i) - [\mathrm{abs}(z_i)] * 10^{-15}, M - i)$$
$$K_4 = \{u^1, u^2, \ldots u^{MN}\}$$
$$K_4 = \mathrm{abs}(u_j) - [\mathrm{abs}(u_j)] * 10^{-15}, N - j$$
$$K_5 = \{v^1, v^2, \ldots v^{MN}\}$$
$$K_5 = \mathrm{abs}(v_i) - [\mathrm{abs}(v_i)] * 10^{-15}, M) \tag{4}$$

Where the range of 'i' from 1 to M and the range of 'j' from 1 to N.

Step 3: Combine and sort out the different key formats from the sequences such as $\{K_1, K_2\}$ for pixel level scrambling, $\{K_3, K_4\}$ for bit level scrambling and $\{K_5\}$ for DNA Encoding.

Module 1: Huffman Compression

Step 4: Consider the equal image(I) size M*N as 256*256,512*512 and 1028*1028. A 2-D image is transferred to the 1D array for fast and easy processing. As refer an Equations [1, 2], generate the Huffman binary tree based on the sorted frequencies of distinct intensity values. Then

$$\mathrm{Codeword} = \{c1, c, 2, c3 \ldots cn\} \tag{5}$$

Where Codeword W (F) is the tuple of binary code values. e_j is the code values for freq_pixel$_j$, $j \in \{1, 2, \ldots m\}$. Convert the binary code to its decimal sequence *P*.

$$p = \{p_1, p_2, \ldots p_{MN}\} \tag{6}$$

Module 2: Scrambling

4.2 Pixel Distribution

Step 5: The decimal sequences are distributed into different blocks as 10*10 pixels. The remaining pixels of the distribution are to be extended with the constant pixel value to make the 10*10 block. Block size $B = 100$. The equation is as follows:

$$\{p_{MN} - \mathrm{tot} \ldots p_{MN}\} = \mathrm{const} \tag{7}$$

Where $\mathrm{tot} = n(p)/100$, Const is the positive integer, const < *M* is the height of an image.

4.3 Pixel-Level Scrambling

Step 6: Combine $\{p_1, p_2 \ldots p_{MN} - tot-_1\}\{p_{MN} - tot \ldots p_{MN}\}$. Suppose the two keys (K_1, K_2) are merged and applied for scrambling [28] by the following equation as

$$Scr(i) = mod(P(i) + \{K_1, K_2\}, M) \tag{8}$$

Where *Scr*(*i*) act as the scrambling based on the pixels, *P* acts as the pixel values $P(i) = \{P_1, P_2, ...P_{MN}\}$ including remaining pixels, $i = 1, 2, \ldots MN$.

4.4 Bit-level Scrambling

Step 7: Transform the decimal sequence Scr, K3, K4 into corresponding binary sequences. The two keys are merged and applied to the following equation

$$Bit\_Scr(i) = circshift[P(i), LSB\{K_3, K_4\}, \{K_3, K_4\}] \tag{9}$$

Where circshift[a,b,c] means c-bit circular shift on the binary sequences *a*, Left/right circular shift are to be decided based on the b value as $b = 0$ or 1, *LSB*(*m*) means the least significant bit of m.

Module 3: DNA Encoding

DNA Encoding [20] is an encoding process which converts into DNA sequence and operation handled on it based on the DNA-ADD, DNA-SUB lookup table. DNA Encoding is divided into five different sections: DNA Sequence, DNA-ADD operation, DNA Rotation, DNA Complement and DNA combination.

4.5 DNA Sequence

Step 8: The binary codes Bit_Scr are converted to DNA sequences based on lookup table, the (DNA rules) and decimal form of Key K_5 converted to the binary form and DNA sequences as refer in Table 1.

$$\text{BKey: Bin\_Key} \leftarrow \text{Bin\_code } (K_5) \tag{10}$$

$$\text{Key: BKey} \leftarrow \text{lookup } (DNA_{rules}) \tag{11}$$

$$\text{C: Bit\_Scr} \leftarrow \text{Bit\_lookup } (DNA_{rules}) \tag{12}$$

Where Bin_code(K_5) denotes the binary code of key K_5 lookup (DNA_{rules}) converts the sequences of DNA (as A, T, G or C) as per the bit represented in Bit_Scr ('00', '01', '10', '00'). Bkey act as the binary code of K_5. Key act as the DNA code key generated after look-up table of DNA rules in Table 1.

4.6 DNA-ADD Operation

Step 9: After the collectively sequence of DNA (as A, T, G or C), perform the DNA-ADD as ref in Table 2, to get the DNA sequence F with the combination of C(i) in Equation (13) and Key in Equation (14).

$$\mathrm{F(i) = C(i) + Key(i)} \tag{13}$$

Where the range of 'i' from $1 \ldots MN$, $C(i)$ acts as a bit scrambling code and $Key(i)$ acts as the Binary form of K_5.

4.7 DNA Complement

Step 10: Consider B*Key* (12) as the key to complement F(i) as shown below.

DNA Rotation

Step 11: Consider every 10*10 blocks to be rotated by 90° degree. Rotation made by two times to get 180°. In Decryption, the same process is to be repeated to attain the original blocks.

$$\mathrm{DNA\_rot = rot(F'(i), 90)} \tag{14}$$

Where DNA_rot denotes the DNA rotation, rot (F' (i),90) denotes to rotate twice (90°) the 10*10 blocks.

4.8 DNA Combination

Step 12: Combine all DNA blocks together to achieve the DNA Sequences. Finally, Decode F' converted to the binary form, convert to decimal sequence H. The Proposedcolour Image Encryption Scheme is shown in Figure 3.

5 Simulation Results/Security Analyses

Experimental simulations are evaluated based on the 5D hyper-chaotic image encryption scheme by the Python 2.7 on a personal computer with YOGA 520 system, 8GB RAM and Intel core i3 processor. The description of Python

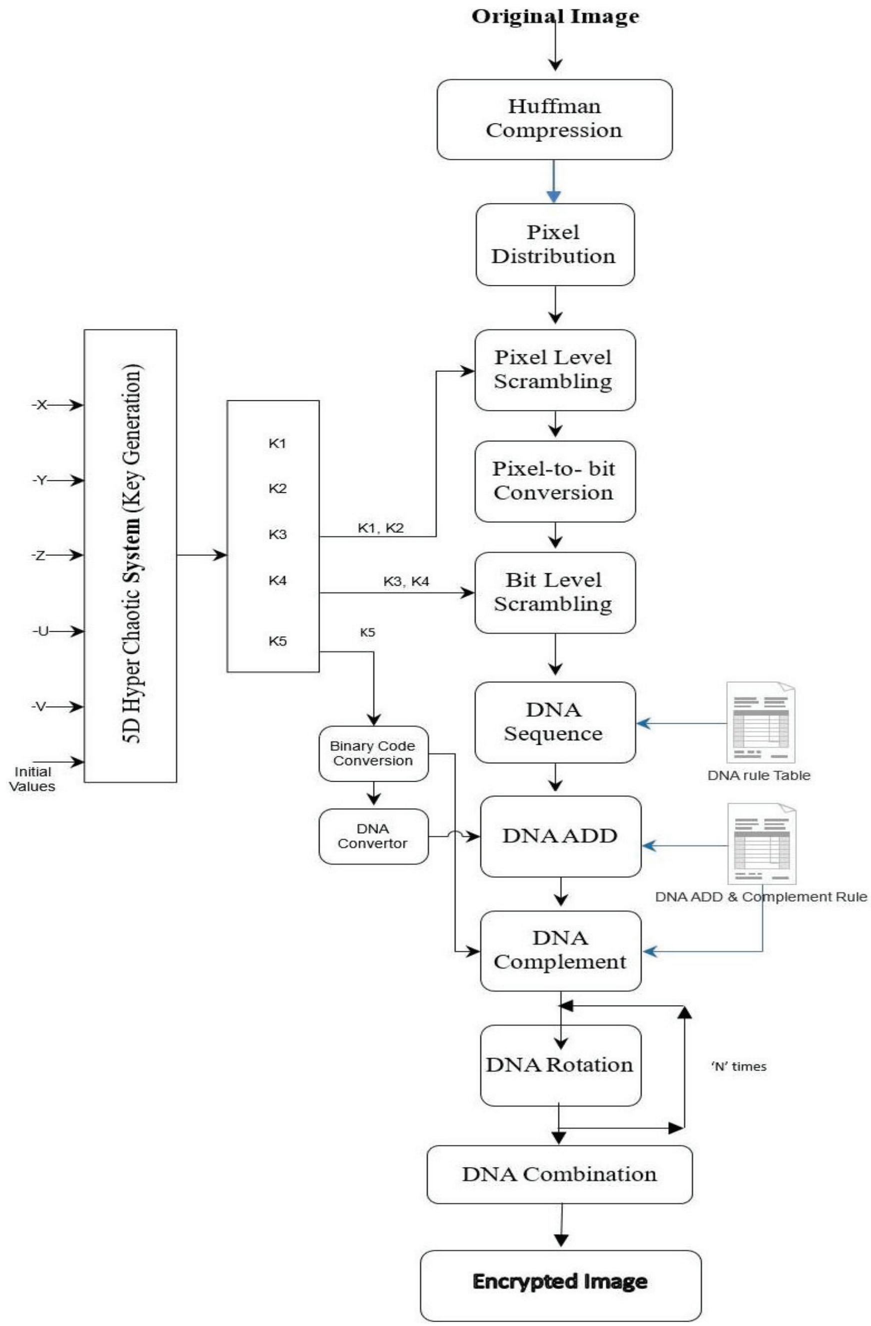

Figure 3 The proposed encryption scheme.

Table 4 Key space analysis

Crypto System	Ours	Ref. [29]	Ref. [28]	Ref. [30]
Keys Space	10^{90} ($\approx 2^{298}$)	10^{56}	10^{60}	2^{128}

as "Python is a high level, scripting language and easy to execute the code. It is simpler code, quick, understandable and open source". Some of the results executed in MATLAB R2016a. The colour plain images such as Lena, baboon, and fruit of different sizes are taken for the proposed scheme as shown in Figure 4.

5.1 Key Space

Key space is the major factors to determine the strength of the proposed image encryption scheme. If it is greater than 2^{100}, it is resist against exhaustive attack. The key calculation of the proposed work based on the initial values as 1.2356, 2.8905, 0.89648, 3.45797 and 0.45723 and rotation key as any character respectively. Thus, the total key space as $(10^{-15)6} = 10^{90}$ which is approximately equal to 2^{298}. If it is more than to 2^{100}, it is proved to resist the exhaustive attacks and brute force attacks.

The key space of existing image encryption scheme compared with the proposedimage encryption scheme are in Table 4. It has shown the proposed cryptosystem is larger while compared to Refs. [28–30] and chaotic properties such as 6 control parameters and key sensitivity. So, it proves to be robust while tested with **exhaustive attacks and brute-force attacks.**

5.2 The Histogram Analysis

Histograms are represented that the data are distributed with pixel/data values. Histogram (plain image) are non-uniformly distributed with pixel values. Histogram (cipher) are uniformly distributed and exhibit exhaustive attacks. The plain images (256*256) image and its Histogram, Encrypted Image and its histogram, Decrypted Image with correct Key are shown as Figure 4. It could be observed that the cipher image is uniformly distributed and flat. Thus, it could withstand several attacks.

5.3 Key Sensitivity Analysis

Key changes to attain encryption

Consider the only 5 initial keys with slight changes of one initial secret key to attain the 0.99% of NPCR in encryption. As observed from calculation below,

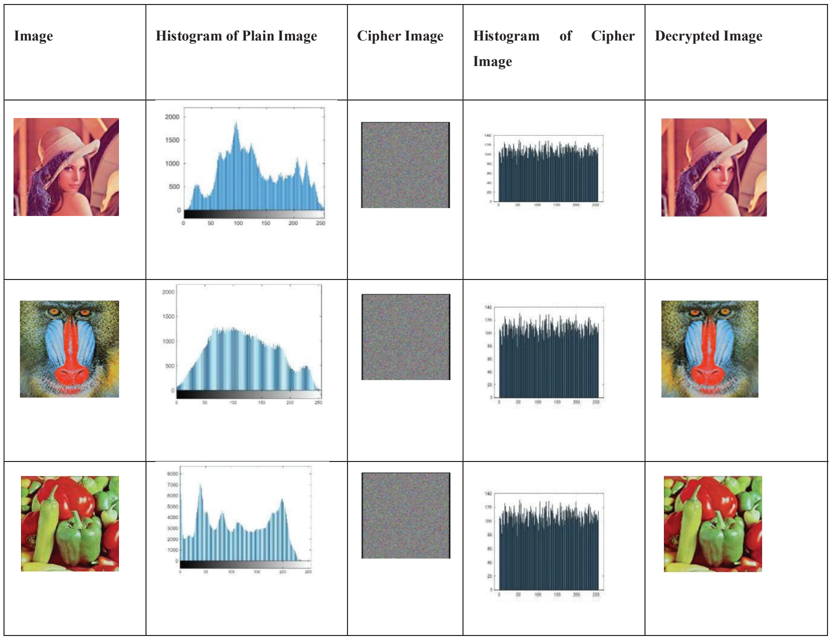

Figure 4 The original image, its Histogram, Encrypted Image and its histogram, Reconstructed Image.

Table 5 NPCR scores between the encrypted image with correct key and changed key

Encryption Keys					
x	y	z	U	v	NPCR(%)
x^0	y^0	z^0	u^0	v^0	–
$x^0 + 10^{-15}$	y^0	z^0	u^0	v^0	99.55
x^0	$y^0 + 10^{-15}$	z^0	u^0	v^0	99.63
x^0	y^0	$z^0 + 10^{-15}$	u^0	v^0	99.57
x^0	y^0	z^0	$u^0 + 10^{-15}$	v^0	99.12
x^0	y^0	z^0	u^0	$v^0 + 10^{-15}$	99.14

encrypted images can cause greater difference because of slight changes of encryption keys. It is shown in Table 5.

Key changes to attain decryption

Consider the only 5 initial keys with slight changes of one initial secret key to attain the 0.99 % of NPCR in decryption. As observed from calculation below, encrypted images can cause greater difference because of slight changes of decryption keys. It is shown in Table 6.

Table 6 NPCR scores between the decrypted image with correct key and changed key

Decryption Keys					
x	y	z	U	v	NPCR(%)
x^0	y^0	z^0	u^0	v^0	–
$x^0 + 10^{-15}$	y^0	z^0	u^0	v^0	0.9941
x^0	$y^0 + 10^{-15}$	z^0	u^0	v^0	0.9931
x^0	y^0	$z^0 + 10^{-15}$	u^0	v^0	0.9934
x^0	y^0	z^0	$u^0 + 10^{-15}$	v^0	0.9963
x^0	y^0	z^0	u^0	$v^0 + 10^{-15}$	0.9912

Table 7 Correlation Coefficient of two adjacent pixels in different images

Image	Image	Plain Image			Cipher Image		
Name	Size	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	256*256	0.9595	0.9810	0.9456	−0.0011	−0.0009	0.0016
Baboon	256*256	0.9976	0.951	0.9610	−0.0009	−0.0014	−0.0015
Lena1	512*512	0.9596	0.9710	0.9656	−0.0011	−0.0010	−0.0015
Baboon1	512*512	0.9755	0.9110	0.9556	−0.0015	−0.0007	0.0014
Lena2	1024*1024	0.9796	0.969	0.9710	−0.0009	−0.0011	−0.0010
Baboon2	1024*1024	0.9467	0.951	0.9556	−0.0010	−0.0015	−0.0012

5.4 Correlation Coefficient

Correlation coefficient is measured the linear relationship between two variables [22]. A secure cryptosystem will reduce the high correlation among two adjacent pixels.

The coefficient of correlation is measured as

From these results, correlation coefficient of plain images with horizontal,vertical and diagonal are 0.9 and with that of cipher images are negative values. So, it was concluded that the correlation of original images and cipher image are different. It was very hard to malicious, exhaustive attacks.

5.5 Information Entropy

It is designed to quantify the image quantity which is evaluated the uncertainty with a random variable. The proposed work is used the entropy-based technique as Huffman coding for initial step for encryption. The image randomness is positively correlated with its entropy.

The information entropy ‘s’ is defined as where $p(S_i)$ denotes the probability at the symbol $S_i, 2^N$ represents to count the total number of possible

Table 8 Information entropies

Image Name	Image Size	Cipher Image
Lena	256*256	7.9973
Baboon	256*256	7.9154
Lena1	512*512	7.9311
Baboon1	512*512	7.9876
Lena2	1024*1024	7.9453
Baboon2	1024*1024	7.9898

Table 9 NPCR and UACI scores between two encrypted Images

Image Name	Image Size	NPCR(%)	UACI(%)
Lena	256*256	99.61	33.46
Baboon	256*256	99.57	33.51
Lena1	512*512	99.25	33.67
Baboon1	512*512	99.45	33.85
Lena2	1024*1024	99.78	33.24
Baboon2	1024*1024	99.12	33.56

symbols. The information entropy represents 8 bits for random image in an ideal situation. Information entropies values of encrypted images are calculated and shown in Table 8. The results in the proposed scheme are closer to 8 bits. So, it proves to resist entropy attacks.

5.6 Differential Attack

It is the existing image cryptosystem attacks which measures changing intensity and changing pixel rate. NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Changing Intensity) are the most common parameters for measuring the plain text sensitivity [30]. It is ability to test against differential attacks. The cipher image is sensitive with the slight change of plain images with respect to the differential attacks. The two parameters are defined as where M represents the image width, 'N' represents the image height; $C1$ and $C2$ represent the ciphered images of the original plain image and its changed image. The expected NPCR and UACI values are 99.6122% and 33.4636%. Table 9 shows the values of NPCR and UACI between two encrypted images. The experimental results concluded that the slight change of plain text can reflect to the cipher image differently even with no other changes in the plain text can lead to a different cipher image. It shows sensitivity to the plain text, which resist to plain attack and differential attack.

Table 10 Speed performance with different schemes

Image	Time(Sec)
Proposed	**3.4**
Ref [32]	3.76
Ref [18]	4.90
Ref [28]	3.826
Ref [22]	22.43

5.7 Encryption Speed

Encryption speed is the major calculation that is to be required to measure the image cryptosystem. The encryption time is calculated with 512*512 are represented in Table 10. It was clearly shown that the proposed colour encryption scheme is faster than the other image cryptosystems.

6 Decryption

The decimal Sequence H converted to binary formand further converted to the DNA Sequence. After the key generation K1, K2, K3, K4 and K5, using the complement rules with K5 to attain intermediate encrypted image. Then, proceed with the DNA- SUB Operation from Table 3. And continue with the DNA sequence, reverse process of scrambling and Huffman coding as ref in equation [1–17]. Finally, original image is retrieved without lossless. Where $\mathrm{i} = 1 \ldots \mathrm{MN}$, H is a final decimal form. ‘I’ acts as the decrypted Image.

7 Conclusion

A fast colour image encryption scheme was introduced by the compression-then-encryption concept to improve speed and secure against attacks. The proposed scheme is the hybrid combination of Chaos techniques for key generation, Huffman Encoding for compression and avoiding colour decomposition, scrambling for more confusion and DNA Encoding for reducing storage size. Security analyses demonstrated to prove the greater NPCR, UACI, robust against attacks and improved the speed performance of the proposed work. For future direction, the proposed work was extended with various images to prove the high security, robustness and reliable.

Declaration

This research paper never has the ethical issues and it is no funded support. There is no conflict of interest. The authors contribution is to implement the encryption in different techniques used.

References

[1] M. Sankari and P. Ranjana, "PLIE- A Light-weight Image Encryption for data Privacy in mobile cloud storage," *International journal of engineering and technology(UAE)*, vol. 7, pp. 368–72, 2023.

[2] M. Sankari and P. Ranjana, "Privacy-Preserving light weight image Encryption in mobile cloud," in *Advances in Intelligent Systems and Computing*, Bangalore, Springer, 2022, pp. 404–414.

[3] S. Swathi and Lahari, "Encryption Algorithms: A Survey," *International journal of Advanced Research in computer science & technology*, vol. 4, no. 2, 2021.

[4] M. M. Ahamad and M. I. Abdullah, "Comparison of Encryption Algorithms for Multimedia," *Rajshahi University Journal of Science & Engineering*, vol. 44, pp. 131–139, 2023.

[5] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33–38, 2022.

[6] P. M. Modak and D. V. Pawar, "A Comprehensive Survey on Image Scrambling Techniques," *International Journal of Science and Research (IJSR)*, vol. 4, 2021.

[7] M. Bahrami and M. Singhal, "A Light Weight Permutation Based Method for Data Privacy in Mobile CloudComputing," in *3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).*, 2015.

[8] M. Bahrami and M. Singhal, " cloudPDB:A light-weight data privacy schema for cloud-based databases," *International Conference on Computing, Networking and Communications, Cloud Computing and Big Data.*, 2016.

[9] N. Holt, "Chaotic Cryptography:Application of Choas Theory to cryptography," 2017.

[10] S. sun, "A Novel Hyperchaotic Image Encryption scheme based on DNA Encoding, pixel level scrambling and bit level scrambling," *IEEE photonics*, vol. 10, no. 2, April 2018.

[11] M. Brindhaa and N. Ammasai, "A chaos based image encryption and lossless compression algorithmusing hash table and Chinese Remainder Theorem," *Applied soft computing*, pp. 379–390, 2016.

[12] M. Sankari and P. Ranjana, "Energy Efficient Symmetric image protection over cloud storage," *International Journal of Advanced Science and Technology*, vol. 29, no. 9s, pp. 4427–4432, 2020.

[13] M. Sankari, P. Ranjana and D. Venkata Subramanian, "Iprivacy-Performance Measurement of Encrypted Image Over Mobile Cloud," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 2919–23, Nov 2019.

[14] M. Sankari, Y. Kalaivani and R. P., "Anomaly Detection in Distributed Denial of Service Attack using Map Reduce Improvised Counter Based Algorithm in Hadoop," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 4, pp. 4668–71, Nov 2019.

[15] A. Muhammad Baqer Mollah, A. Md. Abul Kalam Azad and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, pp. 38–54, 2017.

[16] L. Xu, Z. Li, J. Li and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*,, vol. 78, no. 21, pp. 17–25,, 2016.

[17] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem," *Applied Soft Computing*, vol. 40, pp. 379–390, 2016.

[18] Yuan, Hong-Mei et al., "A new parallel image cryptosystem based on 5D hyper-chaotic system," *image communication*, vol. 52, no. C, pp. 87–96, 2017.

[19] S Sun, et al., "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, April 2018.

[20] Mandrita, Mondal et al., "Review on DNA Cryptography," Cornell University, 2019.

[21] Wua, Xiangjun et al., "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft computing*, vol. 37, pp. 24–39, 2015.

[22] M. Samiullah, et al., “An Image Encryption Scheme Based on DNA Computing and Multiple Chaotic Systems,” *IEEE Access*, vol. 8, pp. 25650–25663, 2020.

[23] B. Mondal and T. Mandal, “A light weight secure image encryption scheme based on chaos & DNA computing,” *Journal of King Saud University – Computer and Information Sciences*, pp. 499–504, 2017.

[24] S. Sun, “Chaotic Image Encryption Scheme using two-by-two DNA complementary rules,” *Optical Engineering*, vol. 56, no. 11, pp. 116117-1-9, 2017.

[25] Ravichandran, D; PraveenKumar, P et al, “Chaos based crossover and mutation for securing DICOM image,” *Computers in biology and medicine*, pp. 170–184, 2016.

[26] Vikas Kumar, “Compression Techniques vs Huffman Coding,” *International Journal of Informatics and Communication Technology*, vol. 4, no. 1, pp. 29–37, 2015.

[27] Islam T Almalkawi, et al., “A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications,” *Journal of Information Security and Applications*, vol. 49, pp. 2214–2126, 2019.

[28] Wu, Jiang et al., “A Novel Image Encryption Approach Based on a Hyperchaotic System, Pixel-Level Filtering with Variable Kernels, and DNA-Level Diffusion,” *Entropy*, vol. 22, no. 1, pp. 1–19, 2020.

[29] Wang, Xingyuan et al., “A novel colour image encryption algorithm based on chaos,” *Signal Processing*, pp. 1101–08, 2011.

[30] Xiuli Chai, et al., “A novel image encryption algorithm based on the chaotic system,” *International Journal of Modern Physics C*, vol. 28, no. 4, p. 1750069 (24 pages), 2017.

[31] Swathi, SV; Lahari, PM et al., “Encryption Algorithms: A Survey,” *International journal of Advanced Research in computer science & technology*, vol. 4, no. 2, 2016.

[32] M. Valander et al., “A fast color image encryption technique based on three dimensional chaotic map,” *Optik- International Journal for Light and Electron Optics*, vol. 183, pp. 1–17, 2019.

Biographies

S. Navaneethan is a research scholar in SRMIST, KTR and working as a Assistant Professor in the department of CSE in Shivani Engineering College Trichy having 13 years of teaching experience and presented 30+ research papers in international conferences and journals & area of interest is WSN, MANET, Mobile Computing, Network Security.

G. Kalamathipriya working as a assistant professor in the department of CSE in Shivani Engineering college. Research area is Machine Learning & Artificial Intelligence.

M. S. Mohamed Keyasudeen doing his graduation in Shivani Engineering College in the department of CSE.

K. Parthiban doing his graduation in Shivani Engineering College in the department of AI&DS.