Hyperchaotic image encryption using DNA coding and discrete cosine transform

Umar Hussain Mir
Central University of Jammu
Parveiz Nazir Lone (parveizcuj@gmail.com)
Central University of Jammu https://orcid.org/0000-0001-6578-852X

Research Article

Keywords: Baker map, Discrete cosine transform, DNA coding, Hyperchaotic system

Posted Date: January 24th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2429075/v1

Hyperchaotic image encryption using DNA coding and discrete cosine transform

Umar Hussain Mir [1] and Parveiz Nazir Lone [2]
[1,2]Department of Mathematics, Central University of Jammu, India.
[1]mirumar@cujammu.ac.in; [2]parveizcuj@cujammu.ac.in;

Abstract

The article presents hyperchaos image encryption using DNA (deoxyribonucleic acid) coding and the chaotic maps in discrete cosine transform. The proposed multilayered security system comprises of advanced levels of confusion and diffusion. Initially, the diffusion among the pixels is attained by employing DNA XOR operation between pixel values and the unpredictable sequence generated from hyperchaotic system. Secondly, the pixels of the partially encrypted image is scrambled by Baker map to permute the image pixels. Finally, the partially encrypted image is diffused through the discrete cosine transform. The significant contribution of this algorithm is to improve the quality of encryption through a DNA encoded scheme. The demonstration results and experimental values are in support the robustness of the proposed scheme and have shown resistance against underlying cryptanalytic attacks.

Keywords: Baker map; Discrete cosine transform; DNA coding; Hyperchaotic system.

1. Introduction

Modern day innovation and technology provide secure ways to transmit data over the internet. But still, the security concerns are there for personal and confidential information. Communication through the internet is increasing at an unexpected rate. Despite several ways of communication over the internet, there is a need for quality encryption techniques on which one can rely for private and personal data. The encryption task is an essential aspect of information security, and in particular, image encryption is somehow different due to being bulky in size, correlation among the pixels, and data redundancy. So, the classical cryptosystems like AES, DES, RSA, etc. are not fit for image encryption. Thus, image encryption has become indispensable over the communication channels to secure confidential information. Hence, the need of quality image encryption tasks arises significantly in modern digital communication.

In the last two decades, several chaos based image encryption schemes have been proposed and have got the attention of researchers. Primarily, the image encryption schemes consists

of confusion and diffusion phases. In the confusion phase, pixel values are permuted to a new position, while in the diffusion step, pixel values are substituted depending upon the mathematical functions and operations. Image encryption aims to reduce high correlation among pixels and to increase the entropy level. Chaotic maps has shown their worth in generating chaotic data for encryption methods. Due to its characreristics like ergodicity, unpredictabilty, dependence on initial conditions, aperiodicity, etc., a number of cryptosystem have been designed in the past using chaotic maps [14, 24, 25]. Despite such characteristics of chaotic maps, many chaotic ciphers have been broken down due to the weakness in their implimentation [14, 15]. So one needs to be alert and corrective measures must be taken while designing secure encryption systems.

Some recent chaos based encryption methods in combination with Fourier transform [27], Hartley transform [18, 23], Gyrator transform [1, 28], fractional Fourier transform [9, 10], discrete cosine transform [8, 17] etc., are designed. Most systems were designed using confusion and diffusion at different granularity levels like block level scrambling [4, 20], bit level scrambling [21, 26, 29, 31, 37], pixel level scrambling [2, 16, 33], DNA level scrambling [22], to name a few. In this work, we present a novel type image encryption algorithm using both lower and higher dimensional chaotic maps with DNA coding and discrete cosine transform, which simultaneously forms a DNA level, bit level, and pixel level scrambling technique.

DNA image encryption is among the latest encryption techniques and is well incorporated with image cryptography due to its massive parallelism, low energy consumption, and information density [3, 11]. So, the present method works with DNA encoding rules and Xor operation, the former is employed to convert the image pixels into DNA sequence, while as latter is used over DNA sequences to convert them into a different DNA sequence. Since this type of encryption, not only diffuses image pixels but is combined with different chaotic and hyperchaotic systems to create the complex confusion as well. There are several DNA and chaos based schemes available in the literature. Liua et al. [19] introduced image encryption using a chaotic map and DNA complementary rules. Enayatifar et al. [5] stipulated a chaos based encryption scheme by using a hybrid genetic algorithm and DNA coding. Guesmi et al. [7] also designed a chaotic encryption technique based on DNA operations and a secure Hash algorithm. Kumar et al. [13] provide an encryption technique using DNA encoding and the Diffie-Hellman algorithm over elliptic curves. Sun [30] proposed a chaotic encryption technique using two by two complementary rules of DNA. Recently, Mohamed et al. [24] provided hyper-chaos encryption based on mitochondrial DNA sequences. Further, Jithin and Sankar [12] proposed chaotic RGB encryption combining an Arnold map and a Mandelbrot set by

using DNA operations. Additionally, few DNA schemes having low plaintext sensitivity are vulnerable to chosen and known plaintext attacks. For instance, the scheme [36] was cryp-analyzed through the chosen plaintext attack [38]. Recently, Wang et al. [32] presented an encryption scheme using DNA coding and coupled map lattices to generate the text sensitivity using SHA-256 algorithm. In [34], a cipher was designed by a spatiotemporal chaotic system and DNA operations to code color planes by random rules of DNA encoding. In addition, different RGB planes are combined together to make a single plane on which a DNA encoding was performed by a matrix generated from a non-linear coupled map. So, these schemes suffered from sensitivity and could not resist the chosen plaintext and known plaintext attacks. Hence, new ciphers schemes are required with high plaintext sensitivity to curb the such type of drawbacks. Thus, by considering the above discussion, an efficient encryption scheme has been tried to present in this work.

The remaining part of the article is organized as follows: The DNA sequence, hyperchaotic system, Baker map and discrete cosine transform are briefly described in Section 2. Section 3 present the proposed encryption methodology of the present work. The simulation results and security analysis are presented in Section 4 and Section 5 respectively. Finally, the comparative analysis is presented in Section 6 and the conclusion part in Section 7.

2. Preliminary work

In this section, DNA rules, hyperchaotic system, discrete Baker map, and discrete cosine transform are briefly discussed.

2.1. **DNA coding.** DNA is found in all living organisms consisting of two complementary strands of nucleotide bases that wind around one another to form the shape of the double helix. In 1977, Frederick Sanger developed a process of determining the order of nucleotides in terms of DNA sequences. This process includes any technology or system used to determine the order of the four nucleotide bases Adenine(A), Cytosine(C), Guanine(G) and Thymine(T). This sequencing has wide applications not only in biological research but also in other applied research fields like forensics, biotechnology, medical diagnostics, etc [5]. Nowadays, DNA encoding is the most advanced research domain and secure information carrier in the field of applied cryptography. As per the rule, adenine pairs with thymine, and cytosine pairs with guanine. This imply that A and T, and C and G are complementary to eachother.

As 0 and 1 are complementary, so are 00 and 11, and 10 and 01. Thus in DNA encoding, the binary pairs 00, 01, 10, and 11 of 8-bit pixels are associated with 2-bit nucleotide bases A, C, G and T using Watson-Crick base pairing given in Table 1. As an example, the binary format

TABLE 1. DNA sequencing base pairing rules

Rules	A	T	C	G
1	00	11	10	01
2	00	11	01	10
3	11	00	10	01
4	11	00	01	10
5	10	01	00	11
6	10	01	11	00
7	01	10	00	11
8	01	10	11	00

TABLE 2. DNA XOR operation

$\bigoplus_{\text{DNA}}$	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

of a decimal number 123 is $(01111011)_2$ and the possible DNA codes are GTCT (by rule 1), CTGT (by rule 2), GACA (by rule 3), CAGA (by rule 4), TGAG (by rule 5), TCAC (by rule 6), AGTG (by rule 7), or ACTC (by rule 8).

The developments in DNA computing produced some algebraic and biological operators that are utilized to operate on different DNA sequences through DNA addition, subtraction, exclusive-OR (XOR), and the complementary operations. For every DNA rule given in Table 1, there corresponds to a unique DNA XOR operation given in Table 2. For instance, consider two DNA sequences as 'ATCG' and 'CTGT', then (ATCG) $\bigoplus$ (CTGT) = CATC.

2.2. **Hyperchaotic system.** The hyperchaotic systems are advanced in terms of randomness, uncertainty and dynamical structure compared to the basic chaotic systems. Chaotic systems are primarily in two and three dimensions, but hyper-chaos systems are at least four-dimensional nonlinear systems. The hyperchaotic system is distinguished from a chaotic by simply adding two or more positive Lyapunov exponents to it. Such systems have high nonlinear complexity, more state variables, and a larger key space resulting in providing high security protection than simple chaotic systems with smaller key space and low complexity.

The chosen 4D hyperchaotic system for the proposed encryption technique is given in Equation 1.

$$\begin{cases} \dot{t}_1 = & a(t_2 - t_1) + \lambda_1 t_4, \\ \dot{t}_2 = & bt_1 - t_1 t_3 + \lambda_2 t_4, \\ \dot{t}_3 = & -ct_3 + t_1 t_2 + \lambda_3 t_4, \\ \dot{t}_4 = & -dt_1, \end{cases} \tag{1}$$

where $a, b, c, d, \lambda_1, \lambda_2$ and λ_3 are controlling key parameters of the chosen hyperchaotic system. This system has hyperchaotic behavior when $a = 35,\ b = 3,\ c = 35,\ d = 5,\ \lambda_1 = 1,\ \lambda_2 = 0.2$ and $\lambda_3 = 0.3$ [35].

The defined hyperchaotic system is employed to generate a pseudorandom sequence by iterating desired number of times. For security improvement and cross effect elimination, the system is pre-iterated $N_0 \geq 3000$ times.In the hyperchaotic sequence generation procedure, an equivalent matrix of order $m \times n$ is given in algorithm 1 is generated.

Algorithm 1: Hyperchaotic sequence generation.

Input: $t_1^0, t_2^0, t_3^0, t_4^0$(state values at N_0^{th} pre-iteration), mn(size).

Result: H (chaotic key sequence of size mn)
function $H \leftarrow$ **HyCSG**($t_1^0, t_2^0, t_3^0, t_4^0, mn$)
for $j \leftarrow 1 : \lfloor \frac{mn}{4} \rfloor$ **do**
  $[t_1^j, t_2^j, t_3^j, t_4^j] \leftarrow$ **Store_iter**$[t_1^{j-1}, t_2^{j-1}, t_3^{j-1}, t_4^{j-1}]$; //output stored at each iteration
  for $i = 1 : 4$ **do**
    $z^1(i) \leftarrow \text{mod}\{floor([(|t_i^j| - floor|t_i^j|) \times 10^{15}]/10^8), 256\}$;
    $z^2(i) \leftarrow \text{mod}\{floor(\text{mod}\{[(|t_i^j| - floor|t_i^j|) \times 10^{15}]/10^8\}), 256\}$;
    $k_1(r) = z^1(i)$;
    $k_2(r) = z^2(i)$;
    r=r+1;
  end
end
$K \leftarrow$ **Concate**$(k_1(r), k_2(r))$;
Output:
$H = [z_1^1, z_2^1, z_3^1 \cdots, z_{\frac{mn}{2}}^1, z_1^2, z_2^2, z_3^2 \cdots, z_{\frac{mn}{2}}^2]$.

2.3. **Discrete Baker map.** The map is a bijection of $L \times L$ lattice onto itself and utilized to break the strong correlation among the neighboring pixels of an image by scrambling its pixel positions [**?**]. The working of two dimensional Baker is elaborated in the following steps:

(I) An $L \times L$ image is partitioned into h rectangles vertically of width $\{l_i\}_{i=0}^{h-1}$ and height L such that l_i divides L for each i and $\sum_{i=0}^{h-1} l_i = l_0 + l_1 + \cdots + l_{k-1} = L$.

(II) After that, each l_i rectangle is shrinked vertically and elongated horizontally to obtain h horizontal rectangles. To make this work, the map partitions each vertical rectangle with $L \times l_i$ size into l_i small rectangles with size $\frac{L}{l_i} \times li$ containing exactly L pixels such that each small rectangle is transformed into a row of pixels.

(III) Finally, these transformed rows are piled up to get a shuffled image.

Mathematically, let L_i denote the x-coordinate of left lower corner of each rectangle such that

$$L_i = \begin{cases} 0 & , \quad i = 0, \\ l_0 + l_1 + \cdots + l_{i-1}, & i = 1, 2, \cdots, h. \end{cases} \tag{2}$$

Then the 2D discrete Baker map for scrambling the pixels of an $L \times L$ image is defined in Equation 3

$$B(x, y) = \left(\frac{L}{l_i}(x - L_i) + y \bmod \frac{L}{l_i} \ , \ \frac{l_i}{L}\left(y - y \bmod \frac{L}{l_i} \right) + L_i \right), \tag{3}$$

where $L_i \leq x \leq L_i + l_i$ and $0 \leq y \leq L$.

The inverse of 2D discrete Baker map for reviving the original positions is defined in Equation 4

$$B^{-1}(x, y) = \left(\frac{l_i}{L}\left(x - x \bmod \frac{L}{l_i} \right) + L_i \ , \ \frac{L}{l_i}(y - L_i) + x \bmod \frac{L}{l_i} \right). \tag{4}$$

The 2D discrete Baker map produces a better pixel shuffling with a small iteration number $\tau \geq 2$, and results in a distinct confused image. The iteration number 'τ' and the width values $\{l_i\}_{i=0}^{h-1}$ of h vertical rectangles are the secret key parameters of this map.

Infact, it is easy to understand the concept of Baker map in visual form as shown in Figure 1.

2.4. **Discrete cosine transform (DCT).** The DCT is related to the 2D discrete Fourier transform (DFT) that transforms data from the spatial to the frequency domain. It is a linear transformation utilized for the diffusion phase in the scheme. The definition of 2D-DCT for an image of size mn is given in Equation 5.

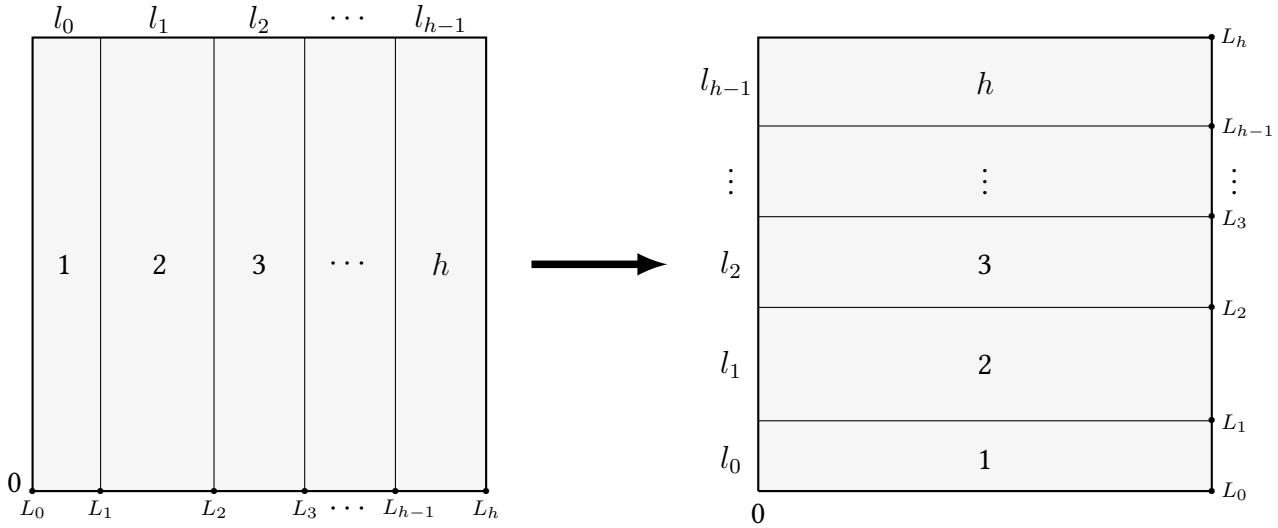

FIGURE 1. The discrete Baker map.

$$\mathcal{D}(u,v) = \alpha_u \alpha_v \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{m}\right] \cos\left[\frac{\pi(2y+1)v}{n}\right], \tag{5}$$

where

$$\begin{cases} 0 \le u \le m-1 \\ 0 \le v \le n-1 \end{cases}, \quad \alpha_u = \begin{cases} \sqrt{\frac{1}{m}}, u = 0 \\ \sqrt{\frac{2}{m}}, 1 \le u \le m-1 \end{cases} \quad \text{and} \quad \alpha_v = \begin{cases} \sqrt{\frac{1}{n}}, v = 0 \\ \sqrt{\frac{2}{n}}, 1 \le v \le n-1 \end{cases}$$

Further the inverse of 2D discrete cosine transform (iDCT) for an image of size mn is given in Equation 6.

$$\mathcal{D}^{-1}(u,v) = f(x,y) = \sum_{u=0}^{m-1} \sum_{v=0}^{n-1} \alpha_u \alpha_v \mathcal{D}(u,v) \cos\left[\frac{\pi(2x+1)u}{m}\right] \cos\left[\frac{\pi(2y+1)v}{n}\right], \tag{6}$$

where

$$\begin{cases} 0 \le x \le m-1 \\ 0 \le y \le n-1 \end{cases}$$

3. Proposed Encryption Methodology

In proposed scheme, the image is encrypted in three phases one confusion phase and two of diffusion phases, as presented in Figure 2. Initially in first phase of diffusion DNA encoded

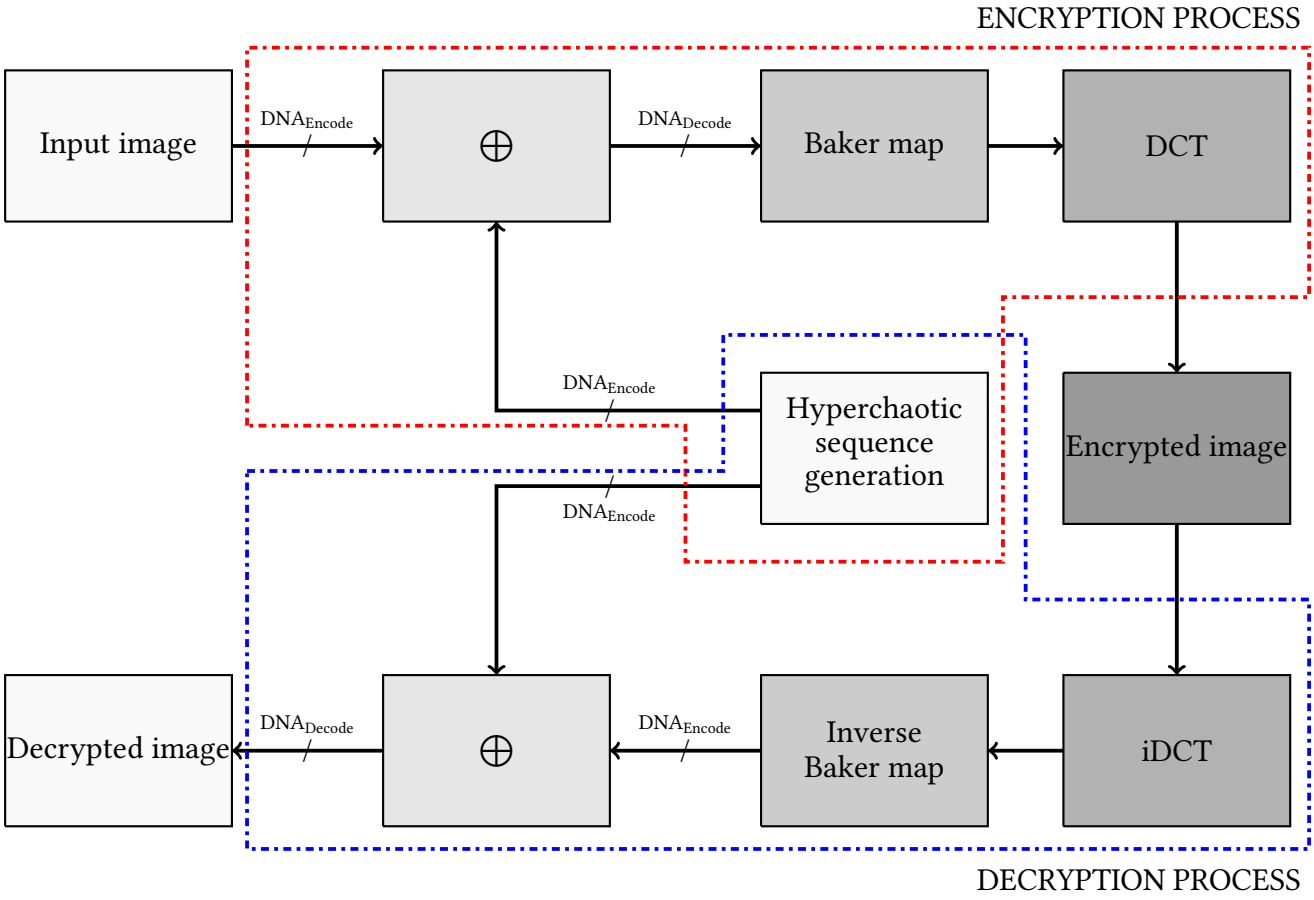

FIGURE 2. Encryption - decryption procedure.

image pixels and hyperchaotic sequence are operated using DNA XOR to partially encrypt the image. After that, the partially encrypted image is gone through the confusion phase where pixel positions are scrambled using Baker map. Finally, the image goes through diffusion phase where the image is treated with two-dimensional DCT to transform the data from spatial domain to frequency domain. The complete encryption method is given in algorithm 2. The decryption process is the inverse of encryption method by using inverse DCT (iDCT) and inverse Baker map respectively.

Algorithm 2: PROPOSED ENCRYPTION ALGORITHM.

Input : I_0(input image of size $m \times n$), $\{t_1^0, t_2^0, t_3^0, t_4^0\}$(state values for chaotic map).

Result: Cipher image
Step (1). $I_1 \leftarrow$ **DNA$_{\text{Encode}}$**(I_0);
Step (2). $H \leftarrow$ **HySg**$(t_1^0, t_2^0, t_3^0, t_4^0, mn)$; //hyperchaotic sequence generation
Step (3). $\hat{H} \leftarrow$ **DNA$_{\text{Encode}}$**(H);
Step (4). $I_2 \leftarrow \bigoplus_{\text{DNA}}(I_1, \hat{H})$;
Step (5). $I_3 \leftarrow$ **DNA$_{\text{Decode}}$**(I_2);
Step (6). Do $s \leftarrow |m - n|$ **then**
$I_n \leftarrow$ **pad_array**$(I_3, s, 0)$; //developing square matrix to I_3
end
Step (7). $I_4 \leftarrow$ **Baker_map**(I_n);
Step (8). $I_5 \leftarrow$ **dct2**(I_4);

Output :
I_5(Cipher image).

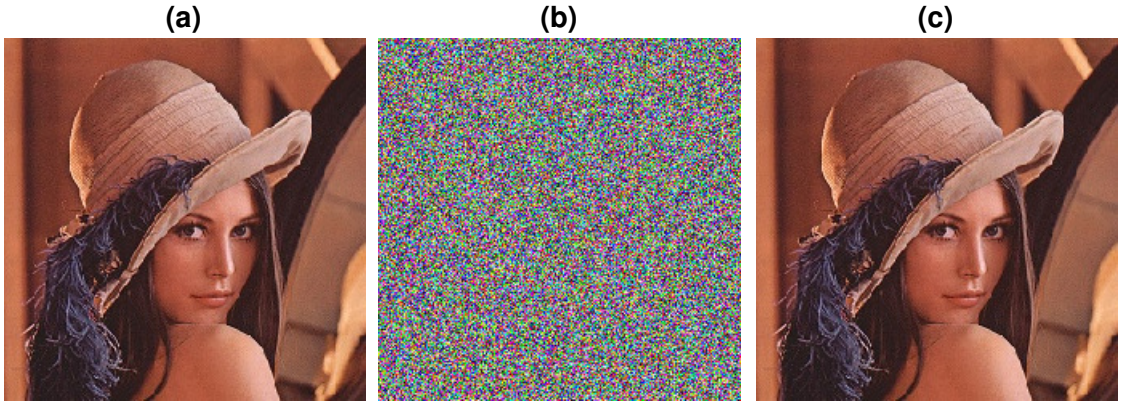

FIGURE 3. Results of lena image: (a) original, (b) encrypted, (c) decrypted.

4. SIMULATION RESULTS

The algorithm is tested on Lena (of size 256×256) and Baboon (of size 512×512) images chosen from a popular USC-SIPI database. The tested results are computed in MATLAB software and are shown in Figure 3 and Figure 4.

5. SECURITY ANALYSIS

A complete extensive analysis is stipulated in this section to analyze the efficiency and robustness of the proposed algorithm against various cryptanalytic attacks like brute-force

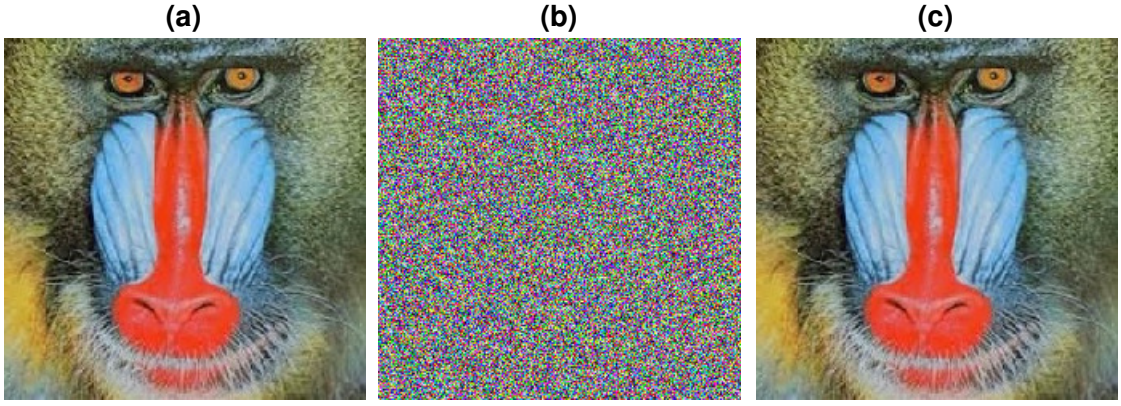

FIGURE 4. Results of baboon image: (a) original, (b) encrypted, (c) decrypted.

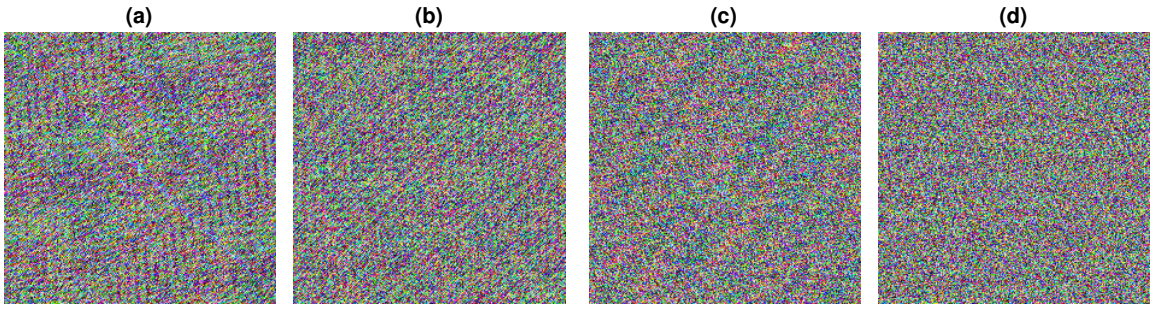

FIGURE 5. Sensitive analysis of Lena image by a $\Delta x = 10^{-15}$change in (a) $t_1^{'}$, (b) $t_2^{'}$, (c) $t_3^{'}$, (d) $t_4^{'}$ respectively in hyper chaotic map.

attack, statistical attacks, differential attacks, noise attacks, entropy attack, cropping attack, etc.

5.1. **Key space and sensitive analysis.** An algorithm is robust against brute-force attack if its keyspace is at least 2^{128} for an 8-bit image [6]. The proposed algorithm has initial conditions of hyperchaotic system as secret keys for the diffusion phase and the values for baker map as secret keys for the confusion phase. Thus, four initial state values of hyperchaotic system are $(t_1, t_2, t_3, t_4) \in \mathbb{R}$ with the computational precision of 10^{-15} as per IEEE floating point standard. So, for an 8-bit image, the keyspace in diffusion phase is approximately $10^{4\times 15} = 10^{60}$ and in confusion phase it is approximately 10^{63}. Thus keyspace of the proposed algorithm is $10^{60} \times 10^{63} = 10^{123}$ which is very large implying that the proposed system is highly resistant to brute force attack.

5.2. **Statistical attack analysis.** This subsection provides a statistical analysis of the algorithm to check resistance against various statistical attacks.

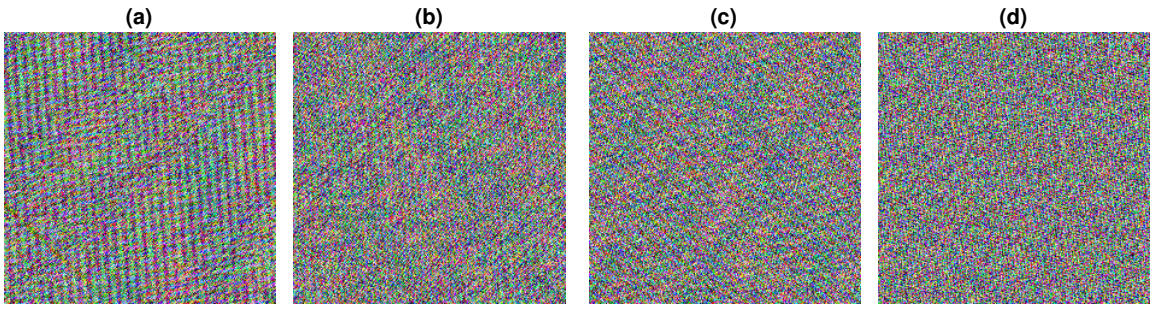

FIGURE 6. Sensitive analysis of Baboon image by a $\Delta x = 10^{-15}$change in (a) t_1^0, (b) t_2^0, (c) t_3^0, (d) t_4^0 respectively in hyper chaotic map.

5.2.1. *Histogram analysis.* Histogram is a statistical distribution of pixel intensity values as input plain image has a non-uniform type of histogram. An efficient algorithm can resist such type of attacks if the histogram of the cipher image is uniformly distributed. The histogram of input images and their cipher images are given in Figure 7 and Figure 8. The uniform histogram distribution of cipher images are different from the histogram of input images that reveal the proposed algorithm conceal the image information while transmission.

Further, uniformity of the data can be verified via chi-square test defined in Equation 7

$$\chi^2 = \sum_{i=0}^{2^n-1} \frac{(O_i - E_i)^2}{E_i}, \tag{7}$$

where O_i is observed and E_i, defined as $E_i = \frac{mn}{256}$ is the expected frequencies respectively. To pass such hypothesis for uniformity at significance level $\alpha = 1\%$ critical value is $\chi^2_{(0.01,255)} = 310.4574$, and at significance $\alpha = 5\%$ critical value is $\chi^2_{(0.05,255)} = 293.2478$ with 255 degrees of freedom. Table 3 shows χ^2 values of test images at significance levels of 1% and 5%.

TABLE 3. χ^2-values

Cipher image	χ^2 values				
	R	G	B	Average	H_0
Baboon	279.2551	267.8251	287.2369	278.1057	accept
Lena	286.1111	276.2865	289.1231	283.8402	accept

5.2.2. *Correlation coefficient analysis.* There is always a good level of correlation between the adjacent pixels of an image in any direction: horizontal (H), vertical (V) or diagonal (D). So, an efficient encryption algorithm is expected to minimize this correlation close to zero between the adjacent pair of pixels. The correlation coefficient between adjacent pixel of an image with size N is computed by Equation 8.

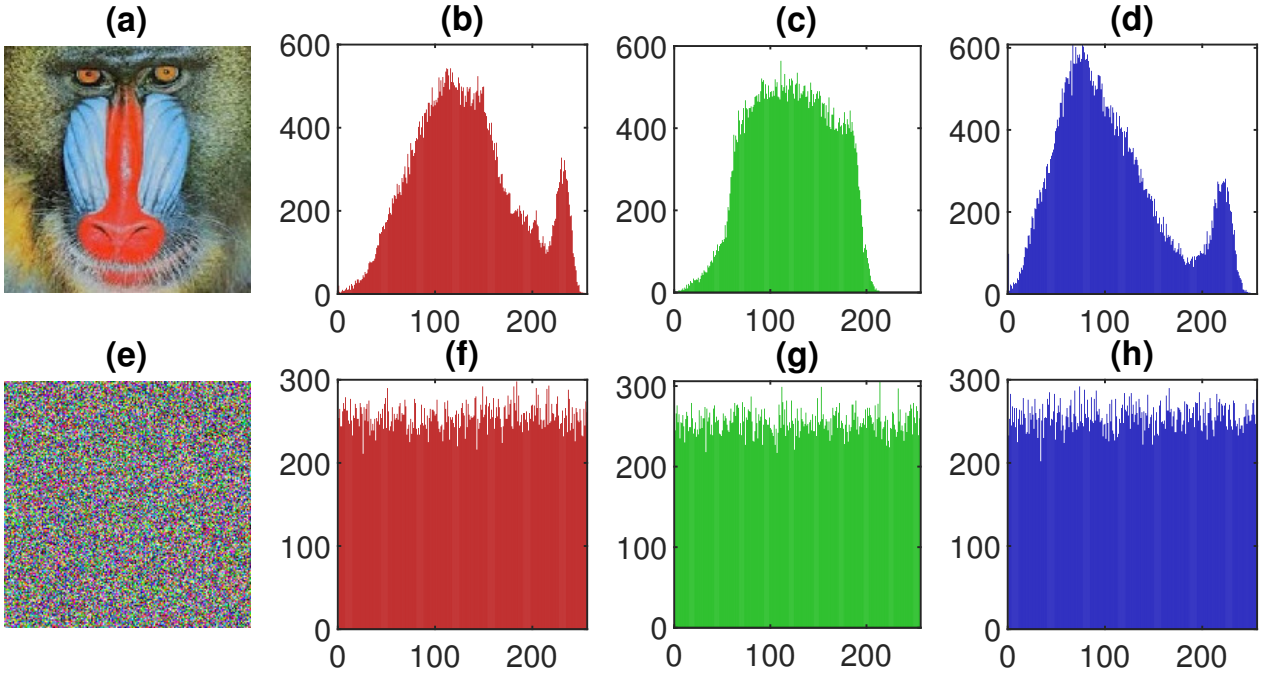

FIGURE 7. Histograms analysis of Baboon image for each color component.

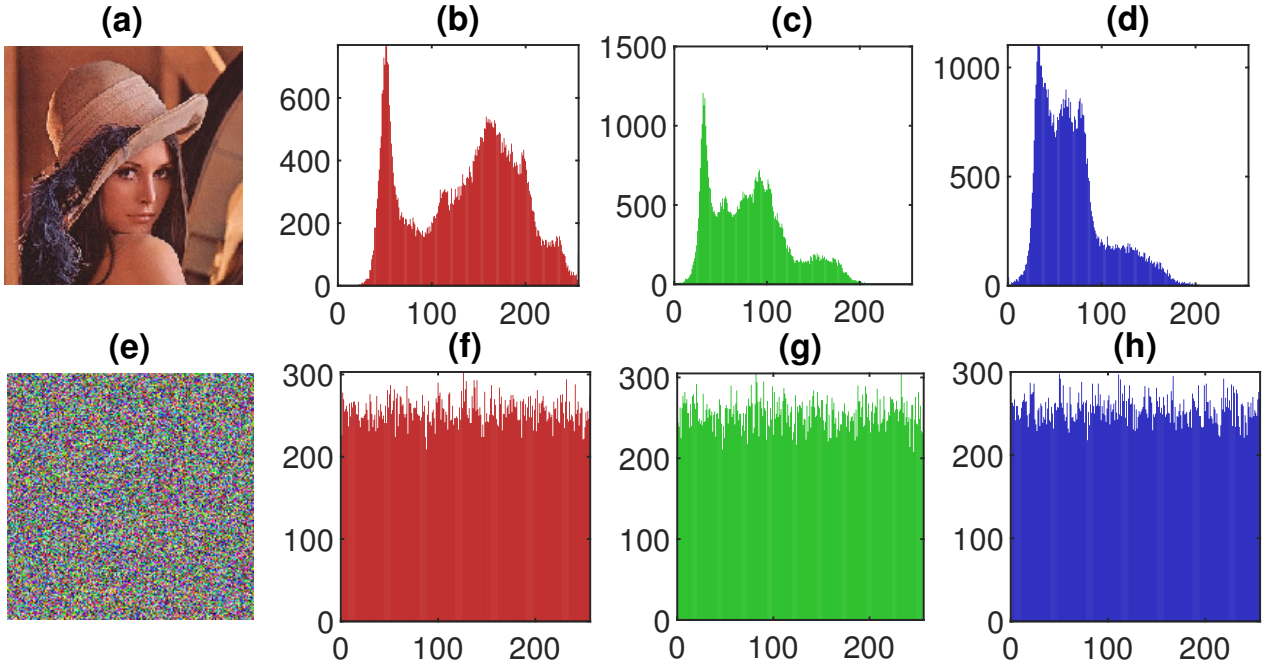

FIGURE 8. Histograms analysis of Lena image for each color component.

$$r_{xy} = \frac{N^2.E[(x - E_x)(y - E_y)]}{\sum_{i=1}^{m}(x_i - E_x)^2.\sum_{j=1}^{n}(y_j - E_y)^2}, \tag{8}$$

TABLE 4. Correlation co-efficient values of the test images

Test images	Component	Plain image			Cipher image		
		H	V	D	H	V	D
Lena (256× 256)	R	0.9475	0.9211	0.8944	0.0005	0.0032	0.0034
	G	0.9359	0.8891	0.9586	0.0025	-0.0065	-0.0016
	B	0.9450	0.9753	0.8639	-0.0024	0.0015	0.0018
Baboon (512× 512)	R	0.8955	0.9358	0.9782	0.0002	-0.0041	0.0035
	G	0.9229	0.9231	0.8836	0.0021	0.0065	-0.0015
	B	0.9648	0.9233	0.9356	-0.0014	0.0022	0.0035

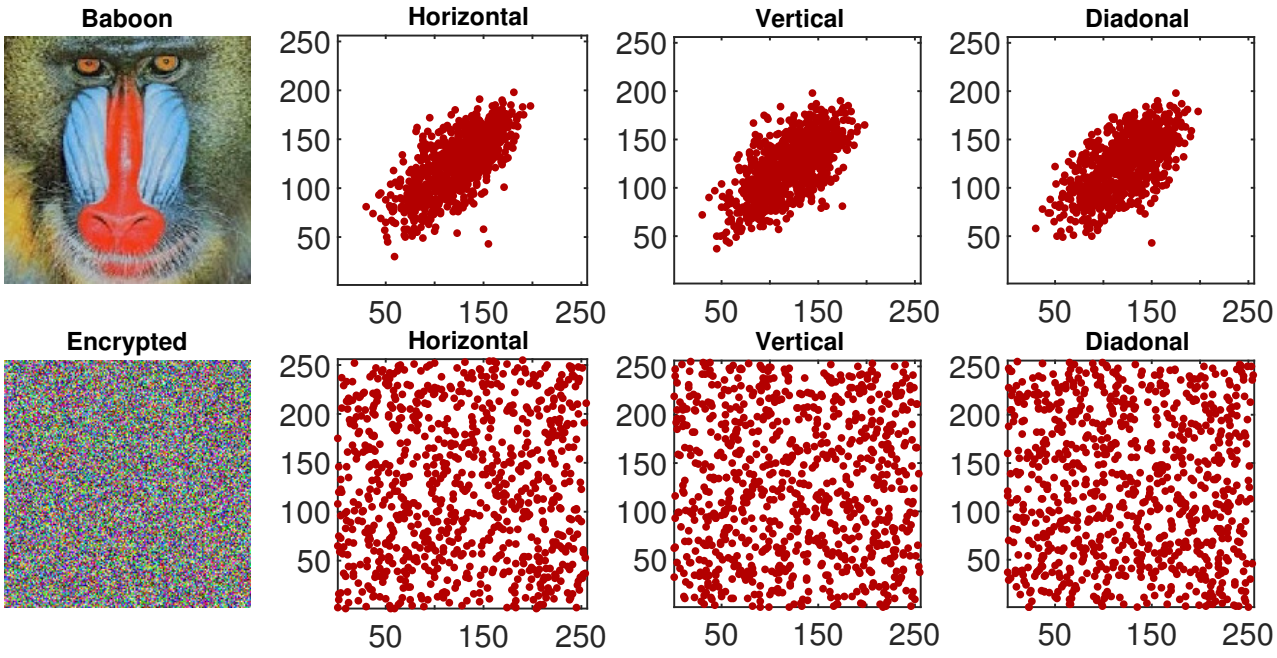

FIGURE 9. Correlation coefficient analysis of red component

where $E_t = \frac{\sum_{i=1}^{N} t_i}{N}$ and x, y are values of adjacent pixels. Figure 9 shows the correlation analysis of adjacent pixels of the input Baboon image and their corresponding cipher images in H, V and D direction of each color component respectively. The pixel distribution of the cipher images shows that the correlation is optimally minimized in all directions that shows the algorithm is robust against such kind of attacks.

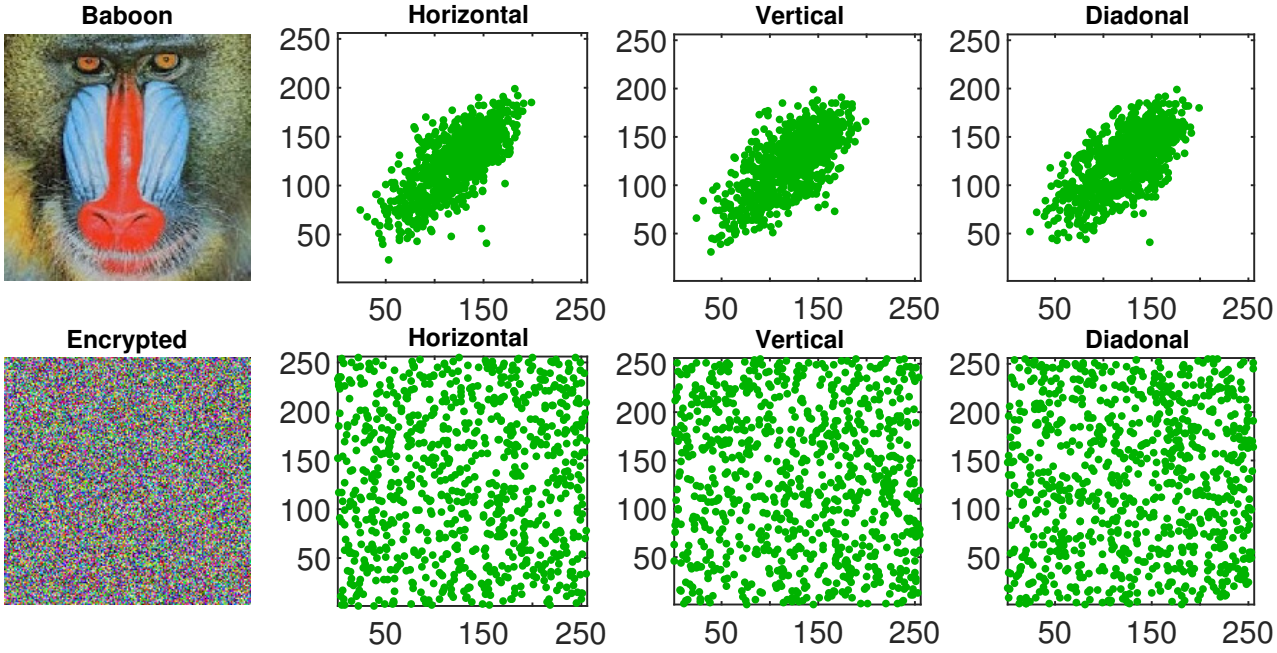

FIGURE 9. Correlation coefficient analysis of green component

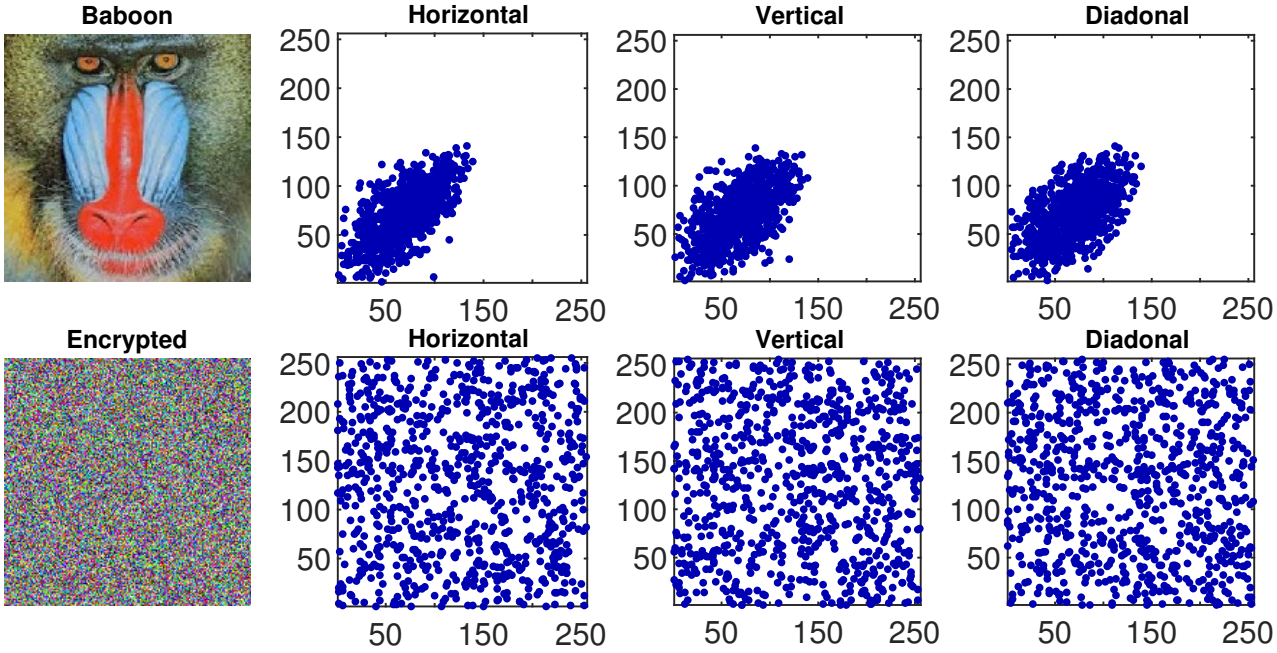

FIGURE 9. Correlation coefficient analysis of blue component

5.3. **Differential attack analysis.** The anti-differential analysis of the presented algorithm is to check the resistance against such attacks. An efficient secure algorithm is anti-differential when it produces encrypted images that has minimum or no relation with the original image. The following two metrics are widely used to check resistance against these attack.

TABLE 5. PSNR analysis

Images	Planes	PSNR	
		Cipher image	Decrypted image
Lena (256× 256)	R	9.1701	∞
	G	8.7589	∞
	B	9.9211	∞
Baboon (512× 512)	R	8.1951	∞
	G	9.5819	∞
	B	8.5361	∞

5.3.1. *UACI.* The theoretical value of Unified Average Changing Intensity (UACI) is equal to 33.4635% to resist the differential attack. In this attack, the attacker tries to reveal the secret keys by using two different cipher images. The UACI value between the images of size mn can be calculated using Equation 9.

$$\text{UACI} = \frac{1}{mn}\left[\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}|C(i,j) - C'(i,j)|}{255}\right] \times 100, \tag{9}$$

where C and C' are cipher image and the image obtained by a negligible change in C respectively.

5.3.2. *NPCR.* The theoretical value of the metric number of changing pixel rates (NPCR) is equal to 99.6094 to resist such kind of attack. The NPCR value between the images of size mn can be calculated by using Equation 10.

$$\text{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} S(i,j)}{mn} \times 100, \tag{10}$$

where

$$S(i,j) = \begin{cases} 0, & if\ C(i,j) = C'(i,j) \\ 1, & if\ C(i,j) \neq C'(i,j) \end{cases}.$$

The NPCR and UACI values of the images are shown in Table 6. Therefore, the experimental results are approximate to ideal values which guarantees that the proposed scheme is safe against such type of attacks.

TABLE 6. UACI and NPCR

Images	Planes	UACI	NPCR
Lena (256× 256)	R	33.6523	99.6123
	G	33.3461	99.6645
	B	33.2983	99.5585
Baboon (512× 512)	R	33.4313	99.6265
	G	33.5238	99.6016
	B	34.0913	99.5952

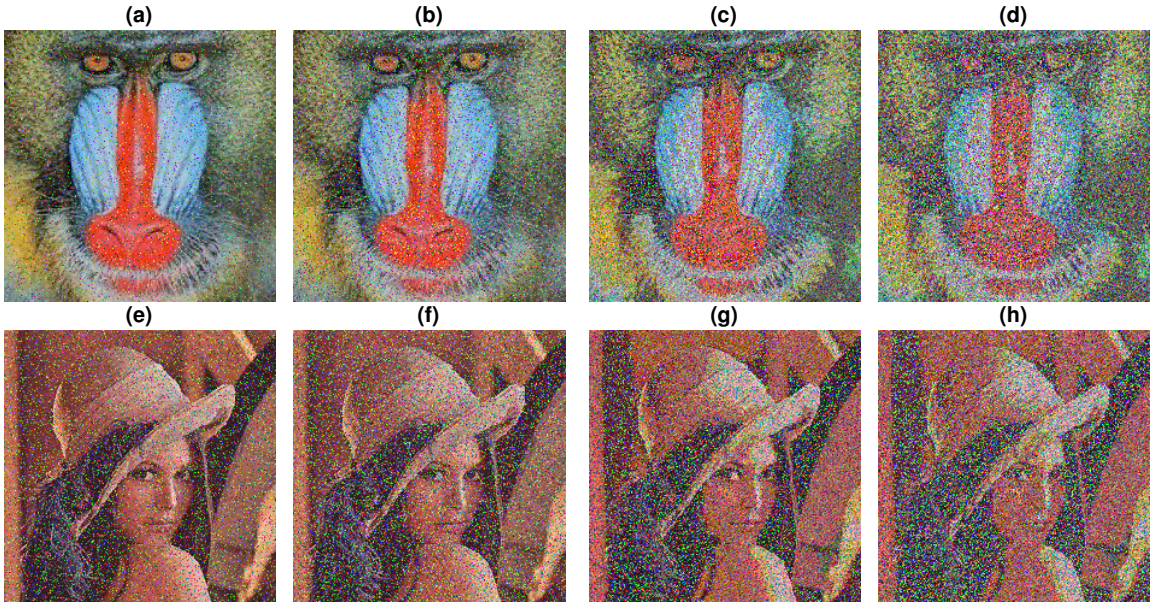

FIGURE 10. Noise result: Salt and pepper noise for (a), (e) and (b), (f) with an intensity levels 0.1 and 0.2 respectively; Guassian noise for (c), (g) and (d), (h) with an intensity levels 0.001 and 0.002 respectively.

5.4. **Noise attack analysis.** The algorithm has gone through the noise attacks as well. The images while transmission may get affected by some type natural noise or noise adding by some intruder. The algorithm successfully visualises the meaningful information even from the affected images after decryption. The Figure 10 shows the results of the affected images after decryption but those are in favor of the stalwaartness of the proposed scheme.

5.5. **Entropy analysis.** This section checks the efficiency of proposed algorithm against the entropy attack. An algorithm is secure against the attack, if the pixels of cipher image are uniformly distributed with high level of randomness. So, the entropy value should be numerically

equal to ideal value 8. Thus entropy of an image of size mn can be calculated by Equation 11

$$H(v) = \sum_{i=1}^{mn} P(v_i).\, log\Big[\frac{1}{P(v_i)}\Big], \tag{11}$$

where v_i represent pixel value and $P(v_i)$ represents probability at v_i . Table 7 shows the values of entropy test.

TABLE 7. Entropy test analysis

Images	Color components	Input image	Cipher image
Lena (256×256)	R	7.1356	7.9972
	G	7.2589	7.9975
	B	6.9982	7.9975
Baboon (512× 512)	R	7.4523	7.9992
	G	7.3564	7.9990
	B	7.2589	7.9991

5.6. **Occlusion attack analysis.** This subsection provides the efficiency of presented algorithm against cropping or occlusion attack. An efficient encryption algorithm is said to resist the occlusion attack if it can decrypt a meaningful image from an affected cipher image. The cipher image can get affected either by some data loss while transmission or an intruder over a public channel manipulates with it.

5.7. **Computation speed analysis.** The computation speed of the encryption algorithm is an essential factor to analyze its efficiency apart from its robustness against various cryptoanalytic attacks. The minimum value of it is an expectation of an efficient system. The running speed of the presented algorithm is computed on Intel(R) 1.80GHz i7-CPU, 8GB RAM, 1TB SSD on MATLAB R2020a software. The average time of the proposed algorithm for images of size (256×256) and (512×512) are 0.5623s and 0.7569s respectively. Evidently, the encryption-decryption execution time being very short and flexible proves the real-time efficiency of the proposed algorithm.

6. Performance comparison analysis

This section analyzes the improvement in security parameters, key space, computation speed, and time complexity of the proposed system compared with some recent similar methods. Table 8 compares the presented algorithm with some recent extant algorithms in terms

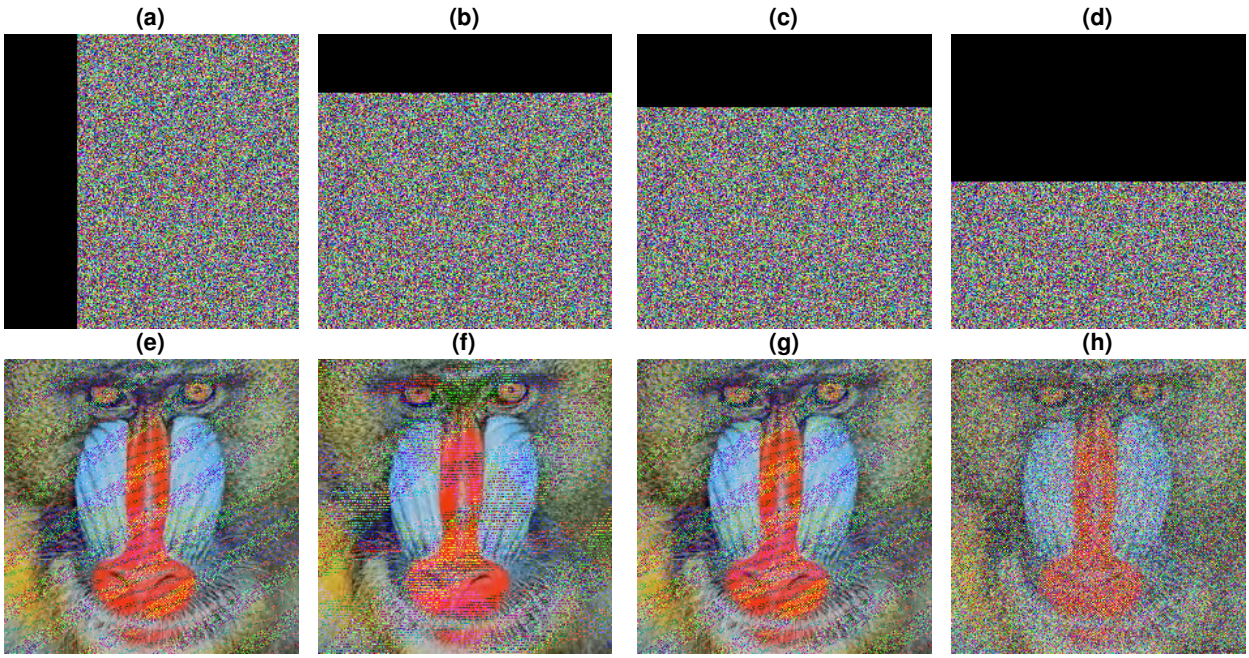

FIGURE 11. Cropping attack analysis with 25%, 20%, 30% and 50% from (a)–(d) and (e)–(h) are the corresponding decrypted results respectively.

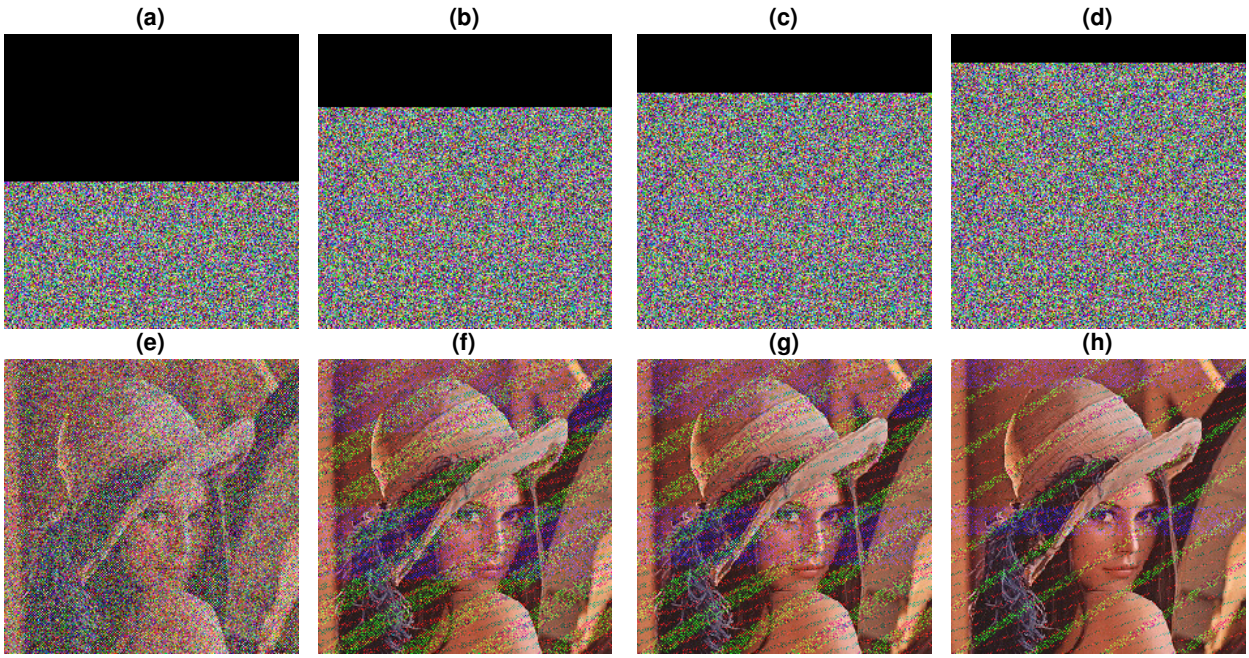

FIGURE 12. Cropping attack analysis with 50%, 30%, 20% and 10% from (a)–(d) and (e)–(h) are the corresponding decrypted results respectively.

of average values of key space, correlation, entropy, NPCR, UACI, and encryption time. The

TABLE 8. Security comparison analysis.

Reference	Key space	Correlation	Entropy	NPCR	UACI	$E_{time}(s)$
Proposed	1.00×10^{123}	0.0002	7.9974	99.6117	33.4322	0.5623
Liua et al.[19]	1.92×10^{126}	-0.0169	7.9874	99.6017	28.1370	—
Enayatifar et al.[5]	1.32×10^{36}	0.0008	7.9997	99.7103	33.6297	3.284
Fu et al.[**?**]	6.61×10^{122}	-0.0169	7.9972	99.5900	33.4500	—
Guesmi et al.[7]	3.40×10^{80}	0.0560	7.9992	99.6155	33.8192	—
Sun[30]	1.30×10^{76}	0.0013	7.9971	99.6100	33.3200	—
Mohamed et al.[24]	1.67×10^{64}	0.0033	7.9974	99.6173	33.4269	—
Jithin and Sankar[12]	—	0.0022	7.9992	99.5700	33.3300	8.2

improvement in key space and security parameters reflects the high security of the presented algorithm.

7. Conclusion

The paper presents a novel and real-time image encryption scheme by using a modified approach to Vigenère cipher and by taking the help of Diffie- Hellman key exchange, Arnold map, and the Baker map. The proposed algorithm has a good security level, as shown by its key sensitivity and resistance against various crypt-analytic attacks. The proposed system is fast, which makes it better for real-time image encryption schemes. Furthermore, the performances of uniform distribution, ideal entropy, de-correlate the adjacent pixels, and able to resist exhaustive attack, statistical attacks, noise attack and the differential attack can provides a sufficient security level. The performed comparison analysis of the scheme is in favor of the robustness of the presented algorithm. The future perspective of this work is to further minimize its computation speed and time complexity by converting the image data from time domain to frequency domain by employing a newer mathematical transformation.

Declaration

There is no conflict of interest among the author(s).

References

[1] M. R. Abuturab. Color image security system based on discrete Hartley transform in Gyrator transform domain. *Opt Lasers Eng.*, 51:317–324, 2013.

[2] H. R. Amani and M. Yaghoobi. A new approach in adaptive encryption algorithm for color images based on dna sequence operation and hyperchaotic system. *Multimedia Tools and Applications*, 78 (15):21537–21556, 2019.

[3] M. Babaei. A novel text and image encryption method based on chaos theory and dna computing. *Natural computing*, 12(1):101–107.

[4] X. Chai, Z. Gan, and M. Zhang. A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimedia Tools and Applications*, 76(14):15561–15585, 2017.

[5] R. Enayatifar, A. H. Abdullah, and I. F. Isnin. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering*, 56:83–93, 2014.

[6] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int Jour. of bifurcation and chaos*, 8(6):1259–1284, 1998.

[7] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet. A novel chaos-based image encryption using DNA sequence operation and secure Hash algorithm SHA-2. *Nonlinear Dynamics*, 83:1123–1136, 2016.

[8] V. Guleria, S. Sabir, and D. C. Mishra. Security of multiple rgb images by RSA cryptosystem combined with FrDCT and Arnold transform. *Journal of Info. Sec. and App.*, 54:102524, 2020.

[9] J. Hahn, H. Kim, and B. Lee. Optical implementation of iterative fractional Fourier transform algorithm. *Opt Express*, 14(23):11103–12, 2006.

[10] B. Hennelly and J. T. Sheridan. Optical image encryption by random shifting in fractional Fourier domains. *Opt Lett.*, 28:269–271, 2003.

[11] A. Jain and N. Rajpal. A robust image encryption algorithm resistant to attacks using dna and chaotic logistic maps. *Multimedia Tools and Applications*, 75(10):5455–5472, 2016.

[12] K. C. Jithin and S. Sankar. Colour image encryption algorithm combining Arnold map, DNA sequence operation and a Mandelbrot set. *Journal of Info. sec. and App.*, 50:102428, 2020.

[13] M. Kumar, A. Iqbal, and P. Kumar. A new image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. *Signal Process.*, 125:187–202, 2016.

[14] C. Li. Cracking a hierarchical chaotic image encryption algorithm based on permutation. *Signal Processing*, pages 203–210, 2016.

[15] C. Li, D. Lin, and J. Lu. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia*, 24:64–71, 2017.

[16] Y. Li, C. Wang, and H. Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 90:238–246, 2017.

[17] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Opt Commun.*, 284(1):123–8, 2011.

[18] Z. Liu, Y. Zhang, W. Liu, F. Meng, Q. Wu, and S. Liu. Optical color image hiding scheme based on chaotic mapping and Hartley transform. *Opt Lasers Eng.*, 51:967–972, 2013.

[19] H. Liua, X. Wanga, and A. Kadir. Image encryption using DNA complementary rule and chaotic maps. *Applied Soft Computing*, 12:1457–1466, 2012.

[20] P. N. Lone and D. Singh. Application of algebra and chaos theory in security of color images. *Optik*, 218:165155, 2020.

[21] P. N. Lone, D. Singh, and U. H. Mir. A novel image encryption using random matrix affine cipher and the chaotic maps. *Journal of Modern Optics*, 68(10):507–521, 2021.

[22] P. N. Lone, D. Singh, and U. H. Mir. Image encryption using dna coding and 3-dimensional chaotic systems. *Multimedia tools and Applications*, 81:5669–5693, 2022.

[23] U. H. Mir, D. Singh, and P. N. Lone. Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain. *Information Security Journal: A Global Perspective*, pages 49–63, 2021.

[24] H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussat. A novel color image encryption algorithm based on hyperchaotic maps and Mitochondrial DNA Sequences. *Entropy*, 22(2):158, 2020.

[25] Y. Niu, X. Zhang, and F. Han. Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database. *Computational Intelligence and Neuroscience*, page 4079793, 2017.

[26] S. F. Raza and V. Satpute. A novel bit permutation-based image encryption algorithm. *Nonlinear Dynamics*, 95(2):859–873, 2019.

[27] P. Refregier and B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding. *Opt Lett.*, 20(7):767–9, 1995.

[28] N. Singh and A. Sinha. Gyrator transform-based optical image encryption using chaos. *Opt Lasers Eng.*, 47:539–546, 2009.

[29] S. Som, A. Kotal, A. Chatterjee, S. Dey, and S. Palit. A colour image encryption based on dna coding and chaotic sequences. *1st International Conference on Emerging Trends and Applications in Computer Science, IEEE*, pages 108–114.

[30] S. Sun. Chaotic image encryption scheme using two by two DNA complementary rules. *Opt Eng.*, 56(11):116117, 2017.

[31] S. Sun. A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photonics Journal*, 10(2):1–14, 2018.

[32] X. Wang, Y. Wang, X. Zhu, and C. Luo. A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and dna level. *Optik*, 125:105851, 2020.

[33] X. Wu, H. Kan, and J. Kurths. A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps. *Applied Soft Computing*, 37:24–39.

[34] K. Xuejing and G. Zihui. A new color image encryption scheme based on dna encoding and spatiotemporal chaotic system. *Signal Processing: Image Communication*, 80:115670, 2020.

[35] K. Zhan, D. Wei, J. Shi, and J. Yu. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *Journal of Electronic Imaging*, 26(1):013021, 2017.

[36] Q. Zhang, L. Guo, and X. Wei. A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik*, 124(18):3596–3600.

[37] X. Zhang, F. Han, and Y. Niu. Chaotic image encryption algorithm based on bit permutation and dynamic dna encoding. *Computational intelligence and neuroscience*, page 6919675, 2017.

[38] Y. Zhang. Cryptanalysis of a novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik*, 126(2):223–229.