Multimedia Tools and Applications (2023) 82:28769–28796
https://doi.org/10.1007/s11042-023-14542-7

HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing

Shaista Mansoor[1] · Shabir A. Parah[1]

Received: 22 February 2021 / Revised: 6 April 2022 / Accepted: 31 January 2023 /
Published online: 22 February 2023

Abstract

In this paper, a distinctive Hybrid Adaptive Image Encryption (HAIE) scheme is proposed that utilizes some statistical parameters of the plain image like mean and variance to modify the initial conditions and control parameters of the chaotic system. The proposed scheme involves two one-dimensional chaotic maps; logistic map and tent map to generate the pseudo-random sequences. The reason for the scheme being distinctive is that the outcome of the confusion phase, i.e. the permuted image is a hybrid one. Half of the plain image is permuted using the logistic map and the other half using the tent map. The two half-permuted images are concatenated after being encoded into DNA sequences using a DNA coding rule. Another random sequence generated using the logistic map is also encoded into a DNA sequence using the same rule. Finally, in the diffusion phase, the two DNA sequences are operated using the DNA addition operation and then decoded using the same DNA decoding rule followed by a XOR operation. The various experimental results like NPCR (Number of Pixel Changing Rate), UACI (Unified Average Changing Intensity), entropy, and correlation coefficients are calculated. For all the test images used, NPCR and UACI values are closer to their ideal values of 99.61% and 33.46%, respectively, entropy is also approximately equal to 8, and likewise, correlation coefficients are closer to zero in the encrypted images. Some other parameters like SSIM (Structural Similarity) and PSNR (Peak Signal to Noise Ratio) are also calculated and lie in their expected range. The scheme is also subjected to noise and cropping attacks. It is observed that the scheme is highly robust against these attacks. Additionally, being adaptive, the proposed algorithm is resilient to chosen and known plaintext attacks. All these experimental observations indicate that the proposed scheme has not only a good encryption effect but can resist various attacks as well.

Keywords Adaptive image encryption · Chaotic maps · DNA computing · Logistic map · Tent map

✉ Shabir A. Parah
shabireltr@gmail.com

[1] Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, Jammu and Kashmir 190006, India

1 Introduction

Nowadays, digital images and video information transmission across the Internet or over some wireless networks and other kinds of innovative technologies has become an important task [10]. It is a major problem to ensure the protection of such data content. The rapid advancement in computer and network technology necessitated the security of data transmission and storage. Images are one of the most important carriers of information and can vividly depict the scene that may be linked to personal information, or some crucial information about the military, medical, commercial, and political affairs. Therefore, it is very important to secure image transmission and storage and more and more attention among the public and researchers has been drawn to it.

One of the most significant methods to provide security and also at the same time assure confidentiality of image information is image encryption. However, the digital images have some intrinsic characteristics such as data redundancy, adjacent pixels are strongly correlated, have less sensitivity in comparison to the text data (i.e. there is not a drastic degradation in the image quality and bulk capacity of data, etc. upon a small change in any of the image pixel attribute). As a consequence, for real-time image encryption, the traditional ciphers like IDEA (International Data Encryption Algorithm), RSA (Rivest Shamir Adleman), AES (Advanced Encryption Algorithm), and DES (Data Encryption Algorithm), etc. are not appropriate as a huge computational time and power is required by these ciphers [25].

The study of chaotic image encryption is becoming the focus of more and more researchers because of the natural connection of chaos with secret communication and cryptography, and as such, many encryption algorithms based on chaos are proposed [5, 15, 24, 27, 29, 32–34]. The main reason for using chaos is because of its certain properties like pseudo-randomness, ergodicity, and extreme sensitivity to initial state and control parameters. Some traditional cryptographic properties like confusion and diffusion can be associated with these inherent properties of chaotic systems and make chaotic maps a suitable choice for designing a cryptosystem. However, from the point of view of modern cryptography, few of these algorithms have been found insecure and broken down in cryptanalysis.

Since for images, there is a huge storage requirement in addition to security because of the bulk data in them. For such data, a newly emerging field is DNA-based cryptography. The first experiment on DNA computing was performed by Adleman in 1991 [1], due to which a new stage in the information era began. Afterward, DNA computing found its way into the field of cryptography [14]. Owing to certain properties of DNA like extremely high storage, massive parallelism, high speed, ultra-low power consumption, a lot of researchers have combined chaos-based encryption techniques with Deoxyribonucleic acid (DNA) computing to further enhance the security and efficiency of image cryptosystem and many image encryption schemes based on chaos and DNA computing have been put forward [6, 9, 11, 13, 16, 18, 19, 22, 28, 30, 35–37].

Since speed and security are the key concerns for a good encryption algorithm; it should be computationally less complex and at the same time should be able to withstand various attacks like chosen plaintext attacks, known-plaintext attacks, etc. A lot of encryption schemes have been put forward that involve utilizing high dimensional chaotic maps to increase the keyspace and thus security. However, they have high computational complexity in terms of time, power, and other resources, like in schemes [11, 13, 24, 27, 33, 35, 36]. Similarly, various encryption algorithms have their secret keys independent of plain images. As a result of which, same chaotic sequences or keystreams are employed for different plain images, making them

vulnerable to chosen and known plain text attacks, such as the schemes like [13, 15, 16, 18, 28, 29, 36, 37].

In light of the above discussion, we propose an HAIE (Hybrid Adaptive Image Encryption) algorithm. The proposed algorithm is based on two discrete one-dimensional chaotic maps namely logistic map and tent map and involves adaptive image encryption by using statistical characteristics of the plain image like mean and variance to calculate the initial conditions and control parameters for both of the maps. This makes the secret keys dependent on the plain image, thus, reducing the chances of known and chosen attacks. The permuted image in this scheme is a hybrid image; the first half is permuted using logistic map and the other half using tent map, which further enhances its security. The use of low dimensional maps makes the algorithm computationally less complex. The overall efficiency of the scheme is further improved by using DNA computation.

Following points elucidate novel contributions of the proposed work:

- It involves utilizing low-dimensional chaotic maps for generating PRN (Pseudo Random Number) sequences, which significantly reduces the computational complexity of the algorithm. At the same time, besides being less complex, the proposed algorithm performs much better than several recently presented state-of-the-art schemes.
- All the preliminary conditions and control parameters of the chaotic maps are made plain image dependent by adaptively modifying them using statistical characteristics of the plain image. As a result of which, the secret keys change every time the plain image is changed i.e. different secret keys will be generated for different plain images [4, 20, 27]. This makes the algorithm robust against chosen and known plain text attacks.
- In the permutation phase, the image is not permuted entirely using a single map. Half of the image is permuted using logistic map and the other half using tent map. This makes the final permuted image a hybrid of two half-permuted images, which increases the security to a further extent. Additionally, the use of two chaotic maps adds more keys to the encryption and decryption process, thus, making the scheme resilient to brute force attacks.

The rest of the paper is organized as follows: In Section 2, some related work done in the field of chaos-based image encryption is discussed. Section 3 gives an overview of various concepts involved in the proposed scheme. Section 4 presents the proposed image encryption algorithm. Section 5 shows the decryption algorithm. Section 6 gives the experimental results and security analysis. Finally, the conclusion of the proposed scheme is presented in Section 7 of the paper.

2 Related work

Numerous image encryption methods based on chaotic systems, DNA computing, fractional transform, etc. have been proposed. Luo et al. in [16] proposed an improved baker map and logistic map based novel chaotic image encryption algorithm. In the proposed scheme, baker map is used to control the logistic map system parameters and state variable. The algorithm consists of two main processes; shuffling and substitution, based on the improved chaotic map.

Bhaskar et al. and Tarni et al. in [18] have used a lightweight image encryption scheme based on chaos and DNA computing. In this scheme, first, the plain image is permuted using a PRN sequence and then encrypted by DNA computation. A Pseudo-Random Number

Generator (PRNG) is used to generate two PRN sequences based on the chaotic logistic map using two sets of keys. One PRN sequence is used in the permutation of the plain image whereas a random DNA sequence is generated using the second sequence.

In [11], Farah et al. proposed a novel method for optical image encryption by using fractional Fourier transform, chaos theory, and DNA sequence operation. Iterative Lorenz map is used for generating random phase masks and the transformation of a plain image into a DNA matrix is done. This matrix and the random phase mask are combined and then three times transformed using the fractional Fourier transform. In [13], Huang et al. proposes 2D Logistic-Sine-Cosine Map (2D-LSCM) and Double Random-Phase Encoding (DRPE)-based novel image encryption scheme. The algorithm makes use of 2D-LSCM, Discrete Wavelet Transform (DWT), and DRPE. In this scheme, firstly DWT is performed on the original image, the wavelet coefficients obtained are then scrambled using 2D-LSCM, and the scrambled result is encoded using DRPE. Afterwards, Inverse Discrete Wavelet Transform (IDWT) is applied on the encoded sequence. Lastly, the chaotic sequences generated from 2D-LSCM are used to perform diffusion and confusion of the result obtained after IDWT. In [30], Kang et al. have presented a new color image encryption algorithm based on spatiotemporal chaotic systems and DNA operations. In the scheme, mixed linear-nonlinear coupled map lattices (MLNCML) system is used to enhance the security of the image encryption algorithm.

Niu et al. [19] proposed an image encryption scheme based on chaotic maps and genetic operations. Firstly, the initial conditions of the chaotic map are obtained as the plain image hash values using the Keccak algorithm. The logistic map is used for pixel shuffling of the plain image and then genetic operations at bit level are performed combined with Henon map and DNA coding technique to achieve pixel selection, crossover, and mutation along with further pixel diffusion and scrambling. Finally, bidirectional XOR operations with chaotic sequences are used to bring more enhancements in the diffusion and confusion features of the scheme.

Sravanthi et al. in [22] presented a bit-plane operation based secure image encryption algorithm. In this scheme, PWLCM (Piecewise Linear Chaotic Map) and 2D-LASM (Logistic Adjusted Sine Map) are used. PWLCM system is employed to perform bit-plane diffusion operation and then 2D-LASM is used to perform the row-shuffling and column-shuffling operations. The bit-plane operation simultaneously performs the confusion as well as diffusion of the pixels. Chai et al. [9] used a 2D-LASM (Logistic Adjusted Sine Map) and a new 1D chaotic system. DNA encoding/decoding rule matrix is produced using the chaotic sequences from 2D-LASM and according to it, the image is encoded into a DNA matrix. Then, on this matrix, DNA level row and column permutation is performed. Next, the two 1D chaotic systems are combined and a key matrix is obtained that is used to perform DNA XOR operation on the permuted DNA matrix.

Wu et al. in [28] proposed a 2D-HSM (Henon Sine Map). Plain image is diffused using the DNA approach and is permuted from the sequences generated. The DNA rules, DNA XOR operation, and the permutation sequence are controlled by 2D-HSM.

Babaei et al. [6] proposed a permutation-diffusion-based image encryption scheme using cellular automata and DNA sequence. In the permutation phase, a cellular shift is performed in the rows and columns of the image using a logistic map. Then the gray level of the pixels is changed in the diffusion phase using DNA and RCA (recursive cellular automata). Zhang et al. in [37] presented a new image encryption algorithm using quantum chaotic map, lorenz chaotic map and DNA coding. In the algorithm, pixel position scrambling, and DNA coding

and decoding rule selection is done by the quantum chaotic map. For pixel diffusion, lorenz chaotic map is used to select the DNA addition and XOR rules.

Zhan et al. [36] have used hyper-chaotic sequence and DNA sequence for image encryption. This scheme has proposed a new global bit scrambling method due to which the encryption performance is significantly improved. The proposed GBS algorithm simultaneously realizes the pixel position scrambling and pixel value substitution. Zarei et al. [35], have proposed a novel image encryption algorithm using a hybrid model of hyper-chaos, DNA computing, and hash functions. DNA level permutation and diffusion are used in this method. Two new DNA operators; DNA left circular shift and DNA right circular shift have also been used.

However, there are certain shortcomings in the above-mentioned schemes like in [13, 16, 18, 28, 36, 37], the key streams are independent of the plain image, making the schemes prone to chosen and known-plaintext attacks. Schemes like [11, 13, 35, 36] involve high dimensional maps and transform operations, etc. making the overall encryption algorithm a computationally complex one in terms of time, power, and other resources.

Although there are some disadvantages associated with the low dimensional maps when used in encryption, they are still widely used for the generation of pseudorandom key sequences in image cryptosystems because more computational time, power, and resources are required by the high dimensional maps. Low dimensional maps become more attractive for image cryptosystems because of their properties like discreteness, fewer arithmetic operations, simple structure, high output processing and relatively having easier implementations in digital systems. Consequently, it is beneficial for the low dimensional systems when used in encryption to involve approaches that enhance its efficiency.

In the proposed HAIE scheme, two different one-dimensional maps are used; the logistic map and the tent map to increase the security of the system, and also more keys are added to the encryption and decryption process. The initial conditions and the control parameters for both the maps are controlled dynamically using statistical parameters like mean and variance of the plain image, making the scheme robust against the chosen and known attacks. Half of the plain image is permuted using a logistic map and the other half using a tent map making the permuted image a hybrid one, thus, improving security. DNA computation is used in the substitution phase to further increase the security and efficiency of the algorithm.

3 Preliminaries

Chaos is used to generate the pseudo-random sequences (key streams) because of its extraordinary feature of sensitivity to initial conditions and control parameters. The function's subsequent values will be tremendously changed upon bringing a slight change in the original values of the primary conditions.

In the proposed model, two chaotic maps are used to generate pseudo-random sequences.

3.1 Logistic map

Proposed in 1967, a logistic map is the most popularly used chaotic equation to generate the pseudo-random sequences.

The logistic map iterative expression is given by the Eq. (1) below:

$$x(k) = \mu * x(k-1) * (1 - x(k-1)) \tag{1}$$

Where k is the iteration index, x (0) is the initial condition and lies in the range (0, 1). μ is the control parameter and ϵ (0, 4). However, for the logistic map to exhibit chaotic behavior, μ ϵ (3.5699456, 4).

3.2 Tent map

The tent map is a piecewise linear chaotic map. It shows chaotic orbits along with other typical dynamical behavior.

Mathematically, the tent map is defined as per Eq. (2) given below:

$$x(n) = f(x(n), r) = \begin{array}{ll} r * x(n-1), & 0 < x(n-1) \leq 0.5 \\ r * (1 - x(n-1)), & 0.5 < x(n-1) \leq 1 \end{array} \tag{2}$$

Where n is the iteration index, x(n-1) is the initial condition, and ϵ [0, 1]. The interval [0, 1] is transformed by the map onto itself and has only one control parameter r ϵ [0, 2]. However, the map exhibits chaotic behavior when r ϵ [10, 25] or more precisely, when its value is closer to 2.

3.3 DNA coding

In living organisms, the function of DNA (deoxyribonucleic acid) is to store, transmit and copy the genetic information. Four nucleotides constitute the DNA; Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). These four nucleotides are also known as bases. Just like any digital computer operates on 0 s and 1 s, these four bases are operated upon in the DNA operations. In the DNA, A pairs with T, and G pairs with C. It can be said in other words that A and T are complementary; likewise, G and C are also complementary. Generally, the four bases represent the two-bit binary numbers i.e. 00, 01, 10, and 11. Since binary numbers 0 and 1 are complementary, likewise, 00 and 11 are complementary and 01 and 10 are also complementary.

If the four DNA bases are used to represent the binary numbers 00, 01, 10, 11, then there exist 4! = 24 DNA encoding combinations. However, only 8 of these combinations satisfy what is known as the "Watson-crick complementary rule" as given in Table 1.

Table 1 8-kinds of DNA map rules

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

3.4 DNA computation

Based on the DNA encoding and decoding rules, some biological and arithmetic operations can be applied to the DNA sequences like addition, subtraction, and XOR listed in Tables 2, 3, and 4, respectively (as per encoding rule 3).

4 Proposed encryption scheme

In this section, a new Hybrid Adaptive Image Encryption (HAIE) scheme based on the two chaotic maps (i.e. logistic map and tent map) and DNA computation is presented. The block diagram of the proposed encryption scheme involving different phases is shown in Fig. 1. The various phases comprise of key generation phase, permutation phase, DNA encoding phase, substitution phase, and finally DNA decoding phase.

4.1 Key generation phase

In the proposed HAIE algorithm, the initial conditions and the control parameters i.e. the secret keys of the two chaotic maps are controlled dynamically using certain plain image statistical characteristics, so that if there is a change in the plain image, the secret keys, and thus the key stream generated also change accordingly.

In this scheme, a random 8 × 8 pixel block of the plain image is taken. The arithmetic mean and variance of the block is calculated and then normalized as well. The normalized mean is used to get the initial conditions of both maps. On the other hand, the normalized variance is used to get the control parameters i.e. μ and r of the logistic map and the tent map, respectively.

4.2 Permutation phase

Permutation refers to scramble the plain image pixels i.e. changing the pixel positions. In the permutation phase, the plain image having a size of MxN is taken as the input. On giving the

Table 2 DNA addition rule

+	A	G	C	T
A	T	A	G	C
G	A	G	C	T
C	G	C	T	A
T	C	T	A	G

Table 3 DNA subtraction rule

–	A	G	C	T
A	G	A	T	C
G	C	G	A	T
C	T	C	G	A
T	A	T	C	G

Table 4 DNA XOR rule

⊕	A	G	C	T
A	G	A	T	C
G	A	G	C	T
C	T	C	G	A
T	C	T	A	G

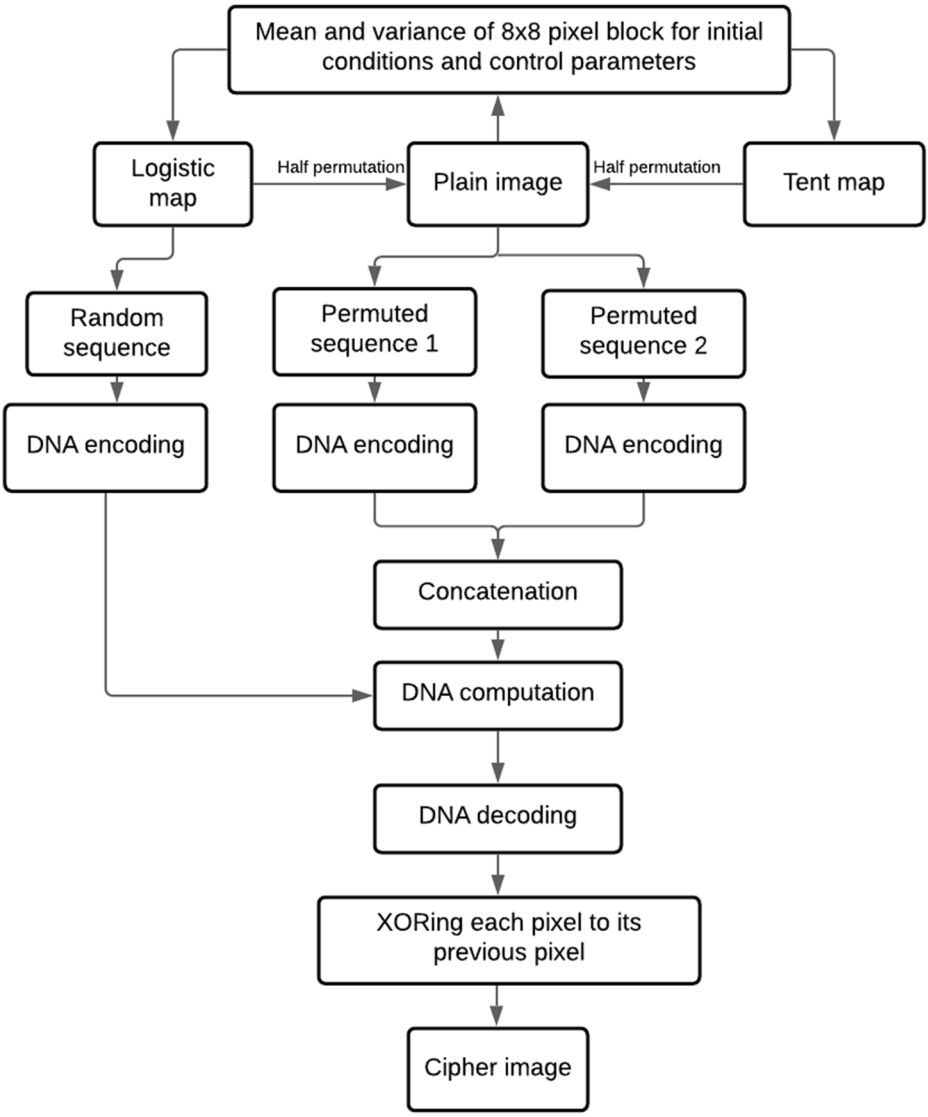


Fig. 1 Block diagram of the proposed encryption algorithm

initial condition and control parameter values, the logistic map is iterated (MxN)/2 times and a pseudo-random keystream is generated. Similarly, the tent map is also iterated (MxN)/2 times to generate another pseudo-random keystream. The first half of the plain image i.e. from 1 to (MxN)/2 pixels, is permuted using the keystream generated by the logistic map, and the second half of the plain image i.e. from (MxN)/2 + 1 to MxN pixels, is permuted using the keystream generated by the tent map. In this manner, two half permuted images are obtained at the end of the permutation phase which are then concatenated to form a final hybrid permuted image.

4.3 DNA encoding

In this phase, the two half permuted images obtained in the permutation phase are converted into DNA bases ATGC according to one of the DNA encoding rules. In the proposed scheme,

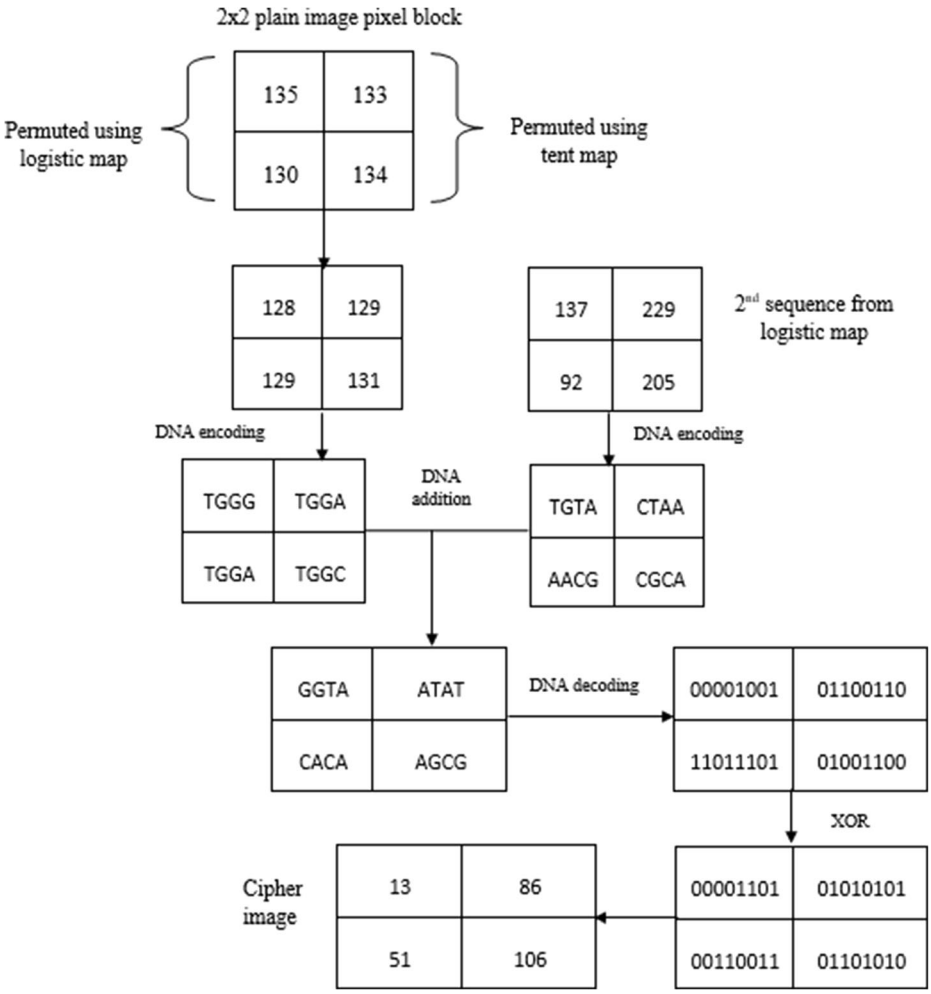


Fig. 2 Illustration of the proposed method using an example

the sequences are encoded as per rule 3. The two DNA sequences obtained are concatenated to get a DNA sequence of size 4xMxN. Also, the logistic map is again iterated MxN times after giving different values of the initial condition and control parameter, to get another pseudo-random sequence. This sequence is also encoded into a DNA sequence as per the same rule.

4.4 Substitution phase

The substitution part is of much importance in any encryption algorithm and is used to modify the pixel values. In this phase, DNA computation is carried out by performing some operation between the two DNA sequences. In the proposed scheme the two DNA sequences are added together according to DNA addition rule 3.

4.5 DNA decoding

The DNA sequence obtained in the substitution phase is decoded into a binary stream according to the same decoding rule. The binary stream is then converted into decimal numbers.

Finally, each element is XORed with the elements previous to that index in the decoded sequence, thus, giving the cipher image.

Figure 2 illustrates the proposed method using an example. In the example a random 2×2 plain image pixel block is taken and the proposed algorithm is applied to it.

The pseudo-code of the proposed encryption scheme is given in Algorithm 1.

Algorithm 1 pseudo-code for image encryption

Input: Plain MxN image P, and its characteristics like mean (α) and variance (β). **Output:** Encrypted MxN image E.

BEGIN

1. **FOR** $i \leftarrow 5$ **to** 12 **do**
   FOR $j \leftarrow 5$ **to** 12 **do**
   A(i-4, j-4) ← P(i, j)
   END FOR
   END FOR
   α ← mean (A(:))/255
   β ← var(double(A(:)))/255
2. $u_1 \leftarrow \beta + \beta_1$
   x_1 (1) ← α-α_1
   $chaotic\_seq_1$ ← generate x_1 using =n (1)
3. $u_2 \leftarrow \beta + \beta_2$
   x_2 (1) ← α-α_2
   $chaotic\_seq_2$← generate x_2 using =n (2)
4. P_{perm1}← permutation(P, x_1 , (MxN)/2)
   P_{perm2}← permutation(P, x_2 , (MxN)/2)
5. DNA_{seq1} ← encode P_{perm1} with rule 3.
   DNA_{seq2}← encode P_{perm2} with rule 3.
   DNA_{seq3}← [DNA_{seq1} DNA_{seq2}]
6. v ← $\beta + \beta_3$
   y(1) ← α-α_3
   $chaotic\_seq_3$ ← generate y using =n (1).
7. DNA_{seq4} ← encode $chaotic\_seq_3$ with rule 3.
8. $Diffused_{seq1}$←DNA_{seq3} + $DNA_{seq4}$with rule 3.
9. $Decoded_{seq}$ ← decode $Diffused_{seq1}$with rule 3.
10. $Decimal_{seq}$← convert $Decoded_{seq}$ to decimal.
11. E ← XOR each pixel in $Decimal_{seq}$ to its previous pixel.

END Algorithm 1

5 Decryption scheme

The image decryption process is similar to the image encryption process. It is the reverse version of the encryption process. The block diagram of image decryption for the proposed scheme is shown in Fig. 3.

The pseudo-code of the decryption process is shown in Algorithm 2.

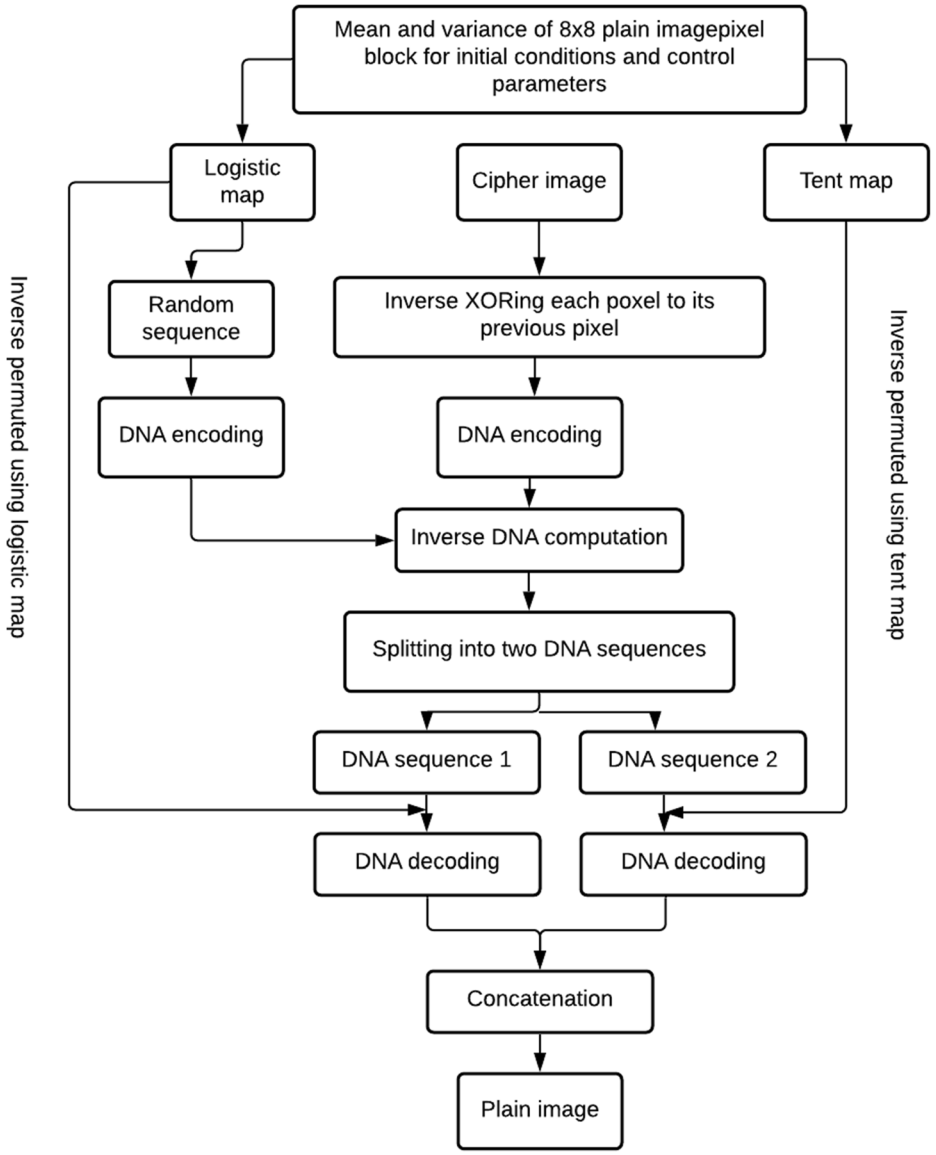


Fig. 3 Block diagram of image decryption

Algorithm 2 Pseudo-code for image decryption

Input: Encrypted MxN image, E. **Output:** Plain MxN image, P.

BEGIN

1. $E_1 \leftarrow$ Inverse XOR each pixel in E to its previous pixel.
2. $DNA_{seq5} \leftarrow$ encode E_1 with rule 3.
3. $Diffused_{seq2} \leftarrow DNA_{seq4} - DNA_{seq5}$ with rule 3.
4. **FOR** $i \leftarrow 1$ **to** 4x(MxN)/2 **do**
   $DNA_{seq6}(i) \leftarrow Diffused_{seq2}(i)$
   END FOR
   FOR $j \leftarrow$ 4x(MxN)/2 **to** 4xMxN **do**
   $DNA_{seq7}(j - \frac{4x(MxN)}{2}) \leftarrow Diffused_{seq2}(j)$
   END FOR
5. $Decoded_{seq1} \leftarrow$ decode DNA_{seq6} with rule 3.
6. $Decimal_{seq1} \leftarrow$ convert $Decoded_{seq1}$ to decimal.
7. $Decoded_{seq2} \leftarrow$ decode DNA_{seq7} with rule 3.
8. $Decimal_{seq2} \leftarrow$ convert $Decoded_{seq2}$ to decimal.
9. $P_{invPerm1} \leftarrow$ InversePermutation ($Decimal_{seq1}$, x_1 , MxN/2).
10. $P_{invPerm2} \leftarrow$ InversePermutation ($Decimal_{seq2}$, x_2, MxN/2).
11. P $\leftarrow [P_{invPerm1}\ P_{invPerm2}]$.

END Algorithm 2

6 Experimental results and security analysis

In this section, experimental results and performance analysis of the proposed HAIE scheme in terms of the keyspace, key sensitivity, histograms, information entropy, correlation coefficients, and differential attack analysis are given.

In the proposed algorithm, various standard grayscale images have been used as plain images and their corresponding cipher images are shown in Fig. 4.

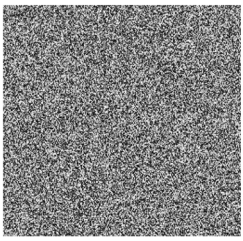
6.1 Keyspace analysis

For the encryption algorithm, all the digital space that can be used as the encryption/decryption key is known as the keyspace of the algorithm. The more its value, the better it is. For a good cryptosystem, the keyspace should be at least equal to 2^{100} ($\approx 10^{30}$), to resist the brute force attacks [3].

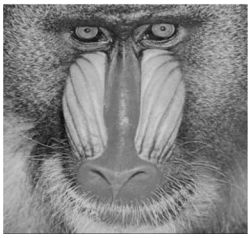
In the proposed scheme, since two maps are used each having two parameters i.e. one initial condition and one control parameter and the logistic map is used twice, so a total of 6 parameters are used. If the precision of each parameter is up to10^{-10}, the keyspace becomes $(10^{10})^6 = 10^{60}$ ($\approx 2^{200}$). Also out of 8 DNA encoding rules one rule is used and the encoding process is done three times. Likewise, DNA addition and DNA decoding is also performed.

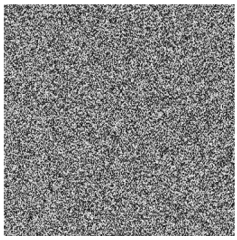
So, the total keyspace of the scheme = (2^{200}) x $(2^3)^5 = 2^{215}$, which is greater than 2^{100} and is sufficiently large enough to withstand the brute force attacks.

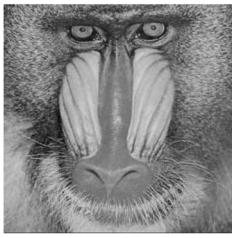

(a) Lena(256x256)


(a_1) Lena encrypted

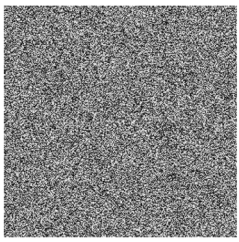

(a_2) Lena decrypted


(b) Baboon (256x256)


(b_1) Baboon encrypted

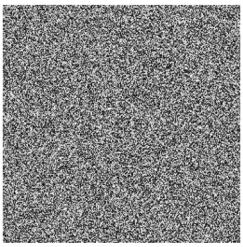

(b_2) Baboon decrypted


(c) Airplane (256x256)


(c_1) Airplane encrypted

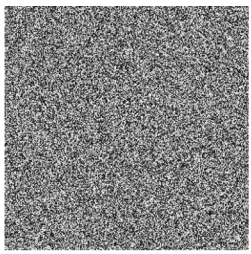

(c_2) Airplane decrypted


(d) Cameraman (256x256)


(d_1) Cameraman encrypted


(d_2) Cameraman decrypted

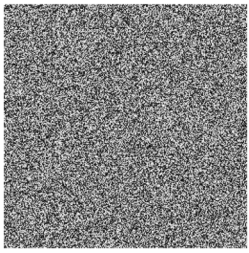

(e) Peppers (256x256)


(e_1) Peppers encrypted


(e_2) Peppers decrypted

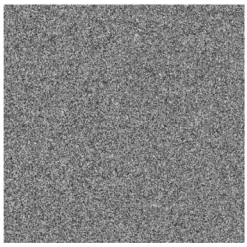
Fig. 4 **a-i** Plain images, (a_1)-(i_1) Corresponding encrypted images, (a_2)-(i_2) Corresponding decrypted images


(f) Boat (256x256)

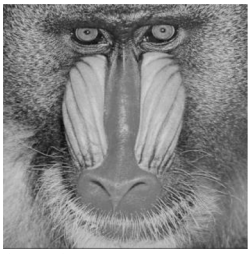

(f_1) Boat encrypted

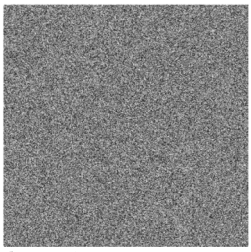

(f_2) Boat decrypted

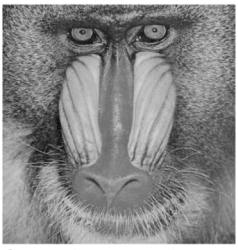

(g) Lena (512x512)


(g_1) Lena512 encrypted

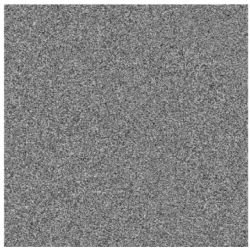

(g_2) Lena512 decrypted


(h) Baboon (512x512)


(h_1) Baboon512 encrypted


(h_2) Baboon512 decrypted


(i) Airplane (512x512)


(i_1) Airplane512 encrypted


(i_2) Airplane512 decrypted

Fig. 4 continued.

6.2 Key sensitivity analysis

For a cryptosystem, the key sensitivity analysis shows how much the system is sensitive to even the slightest change in one of the secret key values. A cryptosystem should be extremely sensitive to any change in the secret keys. The key sensitivity is analyzed by encrypting the plain image using a correct set of keys and then decrypting the image by bringing a very slight

change in at least one of the keys. In such a case, the decrypted image should not leak any kind of information about the plain image, failing which; the algorithm can be easily attacked by the adversary using any set of keys.

To test the sensitivity of the proposed HAIE algorithm to the secret keys, image Lena is first encrypted using a correct set of keys and then decrypted by slightly changing one of the keys. Here, we decrypt the image by taking y(1) = 0.1555999998 instead of the correct key 0.1555999999. In other words, a variation of only a single decimal place in the key produces an entirely noisy or unrecognizable image. Figure 5 shows the key sensitivity analysis of the proposed scheme. Figure 5c shows decrypted Lena using the correct key and Fig. 5d shows decrypted Lena using the incorrect key. It is evident from Fig. 5d that the proposed HAIE algorithm is extremely sensitive to the secret keys.

6.3 Statistical attack analysis

6.3.1 Histogram analysis

A histogram depicts the frequency of image intensities i.e. for each gray intensity level, it gives the number of pixels and is used to analyze the performance of a cryptosystem. A good encryption algorithm should have a uniform cipher image histogram so that no meaningful information is available to the attacker and the algorithm is protected against statistical attacks.

Figure 6 shows the various plain image & cipher image histograms. One can clearly see that the cipher image histograms are very uniform, thus keeping the actual content of the plain images hidden and making the algorithm safe against statistical attacks.

6.3.2 Information entropy analysis

Information entropy is used to measure the degree of randomness or uncertainties in a system. In images, it reflects the distribution of gray values and is large when the gray value distribution is more uniform. The ideal value of the information entropy for a random image having 256 Gray levels is 8. It can be calculated using the expression given below:

$$H(S) = \sum_{i=0}^{2^N-1} P(S_i) * \log(1/P(S_i)) \tag{3}$$

Where, N, in bits is the length of a pixel value and the probability of symbol S_i in a message, S is given by $P(S_i)$. Table 5 lists the various standard grayscale images along with the corresponding information entropy of their cipher images as obtained using the proposed scheme.

Fig. 5 Key sensitivity analysis. **a** Original Lena image, **b** Encrypted Lena, **c** Decrypted Lena using correct keys. **d** Decrypted Lena using a slight change in one key

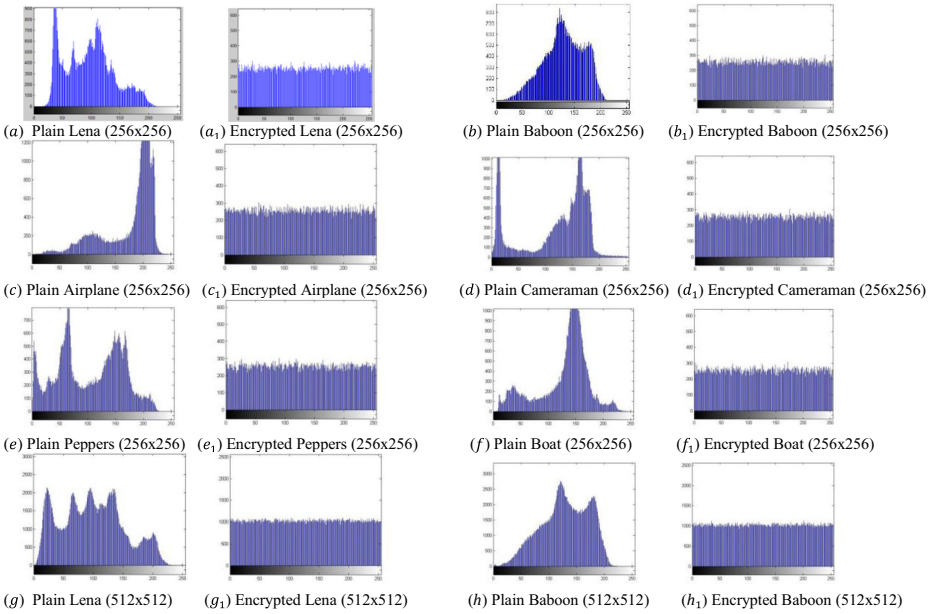


Fig. 6 Histogram analysis

The results are also compared with several recently presented state-of-the-art algorithms. As it can be seen that all cipher images have entropy values very close to the ideal value of 8, so, there is a very small probability of information leakage which makes a statistical attack on these images difficult.

In addition, it is observed that entropy values of the proposed scheme are either comparable with most of the other schemes or better than these schemes.

6.3.3 Correlation coefficient analysis

The correlation coefficient depicts the relation between the adjacent pixels of an image. In a plain image, the pixels are extremely related to each other along the various directions i.e. horizontal, diagonal, and vertical, thus, having a high value of correlation coefficient. This high correlation should be minimized by the encryption algorithm. A good encryption

Table 5 Information Entropy analysis

Images	Proposed	[9]	[28]	[37]	[26]	[31]
Lena(256×256)	7.9973	–	7.9976	7.9973	7.9976	7.9976
Baboon(256×256)	7.9972	–	7.9971	–	7.9974	–
Airplane (256×256)	7.9971		7.9970	–	–	–
Cameraman(256×256)	7.9973	7.9969	7.9975	–	–	7.9971
Peppers (256×256)	7.9972	–	7.9974	–	7.9973	7.9980
Boat (256×256)	7.9970	–	7.9971	–	–	–
Lena (512×512)	7.9993	7.9993	7.9994	–	–	–
Baboon (512×512)	7.9993	7.9994	7.9992	–	–	–
Airplane (512×512)	7.9994	–	7.9992	–	–	–
Peppers (512×512)	7.9992	–	7.9993	–	–	–

algorithm is the one giving a completely uncorrelated image i.e. an image with a very small value of correlation coefficients, closer to zero. It is calculated using Eq. (4).

$$\begin{aligned} r_{xy} &= cov(x,y)/\sqrt{D(x)*D(y)} \\ cov(x,y) &= 1/N \sum_{i=1}^{N} (x_i - E(x))*(y_i - E(y)) \\ D(x) &= 1/N \sum_{i=1}^{N} (x_i - E(x))^2 \\ \mathrm{E}(x) &= 1/N \sum_{i=1}^{N} (x_i) \end{aligned} \tag{4}$$

where number of pixel pairs are given by N, the two adjacent pixels have gray values of x & y, E(x) is the mean, the variance is given by D(x), and covariance is given by Cov(x,y).

Table 6 shows the values of correlation coefficients of various cipher images along horizontal, vertical, and diagonal directions. The values are very close to zero indicating that the proposed scheme is fairly secure against statistical attacks.

The correlation coefficient plot for the image Lena is shown in Fig. 7. It can be clearly seen that there is a high correlation between the adjacent pixels of the plain image whereas, the correlation is very weak in the encrypted image. Hence, the claim of adjacent pixels being uncorrelated in the encrypted image is also verified.

The correlation coefficients obtained using the proposed scheme are also compared with other recent state-of-the-art schemes as shown in Table 7. It is evident that the correlation coefficient values of the proposed scheme are better than most of the schemes being compared with. Thus, it implies that the encrypted images are completely uncorrelated and shows better security against statistical attacks.

6.4 Peak signal to noise ratio (PSNR)

The peak signal to noise ratio is used as a tool to assess the quality of an image encryption algorithm. It indicates the closeness between the original image and the encrypted image. If there is a large difference between the two images is, it means there is large noise between the two. Thus, for a good encryption algorithm, the PSNR value between the original and the

Table 6 Correlation coefficient analysis

Image	Cipher Image		
	Horizontal	Vertical	Diagonal
Lena (256×256)	0.0042	−0.0890	0.00086
Baboon (256×256)	0.0027	−0.1457	−0.00030
Airplane (256×256)	0.0033	0.0085	0.00065
Cameraman (256×256)	0.0047	−0.0379	0.0029
Peppers (256×256)	0.0022	−0.0185	−0.00058
Boat (256×256)	0.0074	−0.0079	0.0020
Lena (512×512)	−0.0013	−0.0511	0.0042
Baboon (512×512)	0.0041	−0.1271	0.0020
Airplane (512×512)	0.0022	−0.0015	0.00078
Peppers (512×512)	0.0047	−0.0171	0.000093

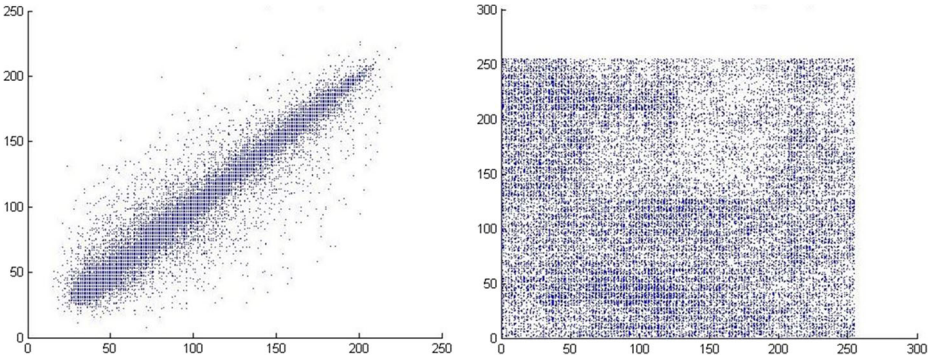


Fig. 7 Correlation coefficient plot

encrypted image must be low. PSNR between the original and the encrypted images should be 7 to 9 for most of the good image encryption schemes [2].

Equation (5) gives the expression to calculate PSNR:

$$\mathrm{PSNR} = 10*\log(P)^2/MSE \tag{5}$$

Where P is the highest pixel intensity for an 8-bit image and is equal to 255, MSE is the mean square error given by Eq. (6):

$$\mathrm{MSE} = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}(O(i,j)-E(i,j))^2 \tag{6}$$

where O is the original image and E is the encrypted image.

Table 7 Comparison of Correlation coefficients with other schemes

Image	Scheme	Cipher Image		
		Horizontal	Vertical	Diagonal
Lena (256×256)	Proposed	0.0042	−0.0890	0.00086
	[9]	–	–	–
	[28]	0.0056	0.0037	0.0032
	[37]	0.0054	−0.0011	−0.0038
	[17]	0.0018	0.0040	−6.0096e-4
	[26]	−0.0017	−0.0004	0.0028
Peppers (256×256)	Proposed	0.0022	−0.0185	−0.00058
	[9]	–	–	–
	[28]	0.0016	0.0059	0.0034
	[37]	0.0066	−0.0026	0.0041
	[17]	0.0054	0.0045	−0.0038
	[26]	−0.0029	0.0003	0.0021
Lena (512×512)	Proposed	−0.0013	−0.0511	0.0042
	[9]	0.0139	0.0177	0.00067
	[28]	0.0032	0.0016	0.0023

6.5 Structural similarity (SSIM)

The structural similarity is a perceptual metric that helps in quantifying degradation in the image quality caused by any processing. SSIM cannot determine the better image among the two images but simply measures the perceptual difference between the two by assessing their visual impact of structure, contrast, and luminance. In encryption domain, the measure of similarity between the original image and the cipher image is given by the SSIM index. It depends on how much the structural information has been modified in the plain image. SSIM is calculated using the formula given in Eq. (7):

$$SSIM(o,e) = [l(o,e)]^{\alpha}[c(o,e)]^{\beta}[s(o,e)]^{\gamma} \tag{7}$$

Where, $[l(o,\ e)] = (2\mu_o\mu_e + C_1)/(\mu_o{}^2 + \mu_e{}^2 + C_1)$ is the image luminance, $[c(o,\ e)] = (2\sigma_o\sigma_e + C_2)/(\sigma_o{}^2 + \sigma_e{}^2 + C_2)$ is the image contrast, and. $[s(o,\ e)] = (\sigma_{oe} + C_3)/\sigma_o\sigma_e + C_3$ is the image structure.

α, β, γ are all >0 and control each term's relative significance, μ_o = Original image mean, μ_e = encrypted image mean, $\sigma_o{}^2$ = original image variance, $\sigma_e{}^2$= encrypted image variance, σ_{oe} = covariance between original and encrypted images. C_1, C_2, C_3 are constants with $C_1 = (h_1L)^2$, $C_2 = (h_2L)^2$, $C_3 = C_2/2$, L = 255, h_1= 0.01 and h_2 = 0.03. The value of the SSIM index between the original image and the encrypted image should be as low as possible indicating low similarity between the two and more modified information in the original image.

Table 8 gives the SSIM and PSNR results obtained using the proposed HAIE algorithm. The SSIM values are close to zero, thus showing a good modification of the information in the original images. PSNR values are also low indicating a large noise between the original and the encrypted images.

Table 9 gives the comparison of PSNR values of the proposed scheme. The results of the proposed scheme are better than those given in [31] signifying greater difference between the

Table 8 SSIM index and PSNR

Images	SSIM	PSNR
Lena(256×256)	0.0090	9.2736
Baboon(256×256)	0.0129	10.1361
Airplane (256×256)	0.0112	8.6688
Cameraman(256×256)	0.0082	8.5116
Peppers (256×256)	0.0085	8.6143
Boat (256×256)	0.0098	9.7935
Lena (512×512)	0.0093	8.8175
Baboon (512×512)	0.0096	9.8491
Airplane (512×512)	0.0108	8.6437
Peppers (512×512)	0.0101	8.6090

Table 9 Comparison of PSNR

Image	Proposed	[31]
Lena (512×512)	8.8175	9.2392
Baboon (512×512)	9.8491	9.5248
Peppers (512×512)	8.6090	8.8811

plain and encrypted images. Consequently, it is more difficult to predict the plain image form the encrypted image.

6.6 Differential attack analysis

There should be a very high sensitivity to the plain image in an image encryption algorithm such that even if a minute change is brought in the plain image, the corresponding cipher image should significantly change. Such an algorithm is said to resist the differential attacks wherein, the attacker makes a small change in the original image and then encrypts both the images before and after the change to determine any sort of statistical pattern in their distribution.

There are two criteria to determine the resistance against differential attacks; NPCR (number of pixel change rate) and UACI (unified average changing intensity) defined by Eqs. (8), (9), (10) [8].

$$NPCR(C_1, C_2) = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)*100\% \tag{8}$$

$$UACI(C_1, C_2) = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j)-C_2(i,j)|}{255}*100\% \tag{9}$$

$$D(i,j) = \begin{cases} 0, if\ C_1(i,j) = C_2(i,j) \\ 1, if\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{10}$$

Where the width and height of the original image are given by M and N, and cipher images before and post changing the pixel value at location (i, j) are given by $C_1(i, j)$ and $C_2(i, j)$, respectively. The ideal values of NPCR and UACI are 99.61% and 33.46%, respectively [21].

In the proposed scheme, various grayscale images are taken and one bit of the plain images is changed. NPCR and UACI are calculated and the results are given in Table 10. The results obtained from the proposed scheme are either equal or close to the ideal values implying that, it is extremely sensitive to the plain image.

A comparison of NPCR and UACI values of the proposed scheme with other schemes is given in Table 11. The results of the proposed scheme outperform most of the results of other schemes. It is because the proposed scheme is adaptive in nature. So, any change in the plain

Table 10 NPCR and UACI analysis

Image	NPCR	UACI
Lena (256×256)	99.61	33.46
Baboon (256×256)	99.61	32.45
Airplane (256×256)	99.66	32.93
Cameraman (256×256)	99.61	33.07
Peppers (256×256)	99.61	33.17
Boat (256×256)	99.61	32.33
Lena (512×512)	99.61	33.44
Baboon (512×512)	99.60	32.64
Airplane (512×512)	99.61	32.87
Peppers (512×512)	99.60	33.20

Table 11 Comparison of NPCR and UACI with other schemes

Image	Proposed		[37]		[28]		[9]		[26]		[31]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena (256×256)	99.61	33.46	99.59	28.54	99.62	33.41	–	–	99.60	33.45	99.60	33.45
Cameraman (256×256)	99.61	33.07	–	–	99.61	33.53	99.61	33.46	–	–	99.60	33.40
Peppers (256×256)	99.61	33.17	99.60	29.60	99.60	33.49	–	–	99.60	33.47	99.61	33.43
Lena (512×512)	99.61	33.44	–	–	99.60	33.50	99.58	33.43	–	–	–	–

image pixels produces an entirely different encrypted image. Thus, this algorithm is capable of resisting the differential attacks extremely well.

6.7 Chosen plaintext and known plaintext attacks

The proposed encryption algorithm resists both the chosen plaintext attack as well as the known plaintext attack. This is because, in the proposed algorithm, the secret keys i.e. the initial conditions and control parameters of the chaotic maps are plain image dependent. Thus, for different plain images, diverse secret keys and hence diverse keystreams will be generated in the encryption process. As a result of which, attackers will not be able to extract any useful information by encrypting some pre-designed special images, because the encrypted outcome is related to those selected images only. This concludes that the proposed algorithm is plain image dependent and capable of effectively withstanding the chosen plaintext and known plaintext attacks.

6.8 Robustness analysis

It is inevitable in real-world applications that some noise gets added to the information or it suffers some losses during transmission over a communication channel. Robustness is the ability of an encryption algorithm to recover original image from a cropped or noisy cipher image.

6.8.1 Noise attack analysis

To check the robustness of the proposed scheme against noise attacks, we add salt and pepper noise of different densities to the encrypted image of Lena, as shown in Fig. 8. The noise densities used are 0.01, 0.05, and 0.1 in Fig. 8a, 8b and 8c, respectively. The corresponding

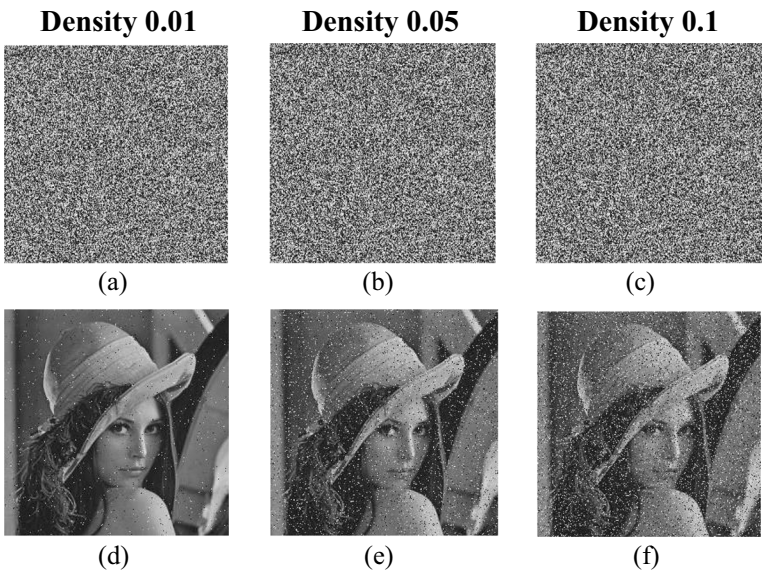


Fig. 8 Noise attack analysis. **a**-**c** Noisy cipher images **d**-**f** Corresponding decrypted images

decrypted images are shown in Fig. 8d, 8e, and 8f. As it is evident from the figure that the despite the cipher images being noisy, corresponding decrypted images are still perceivable. This shows robustness of the proposed scheme against noise attacks.

6.8.2 Cropping attack analysis

In order to test robustness of the proposed scheme against cropping attack, we use different cropping levels like 1/8, 1/4, and 1/2, as depicted in Fig. 9a, 9b, and 9c, respectively. We find out in Fig. 9d-f that the corresponding decrypted images can still be recognized. Thus, the proposed algorithm succeeds in resisting the cropping attack as well.

One of the most important index to measure the quality of encryption is PSNR. A low PSNR value signifies good encryption quality and a high value signifies better perceptual security. We evaluate the robustness of the proposed algorithm against salt and pepper noise attack and cropping attack in terms of PSNR and MSE, defined in Eqs. 5 and 6, respectively. The results obtained for the image Lena are presented in Table 12 (noise attack analysis) and Table 13 (cropping attack analysis).

From the Tables 12 and 13, it is observed that both PSNR and MSE have good values, which indicates that the proposed scheme has good perceptual security and is robust against noise and cropping attacks.

6.9 Computational complexity analysis

The chaotic sequence generation, permutation operations and diffusion operations in any chaos-based image encryption algorithm constitute its time consumption part. The computa-

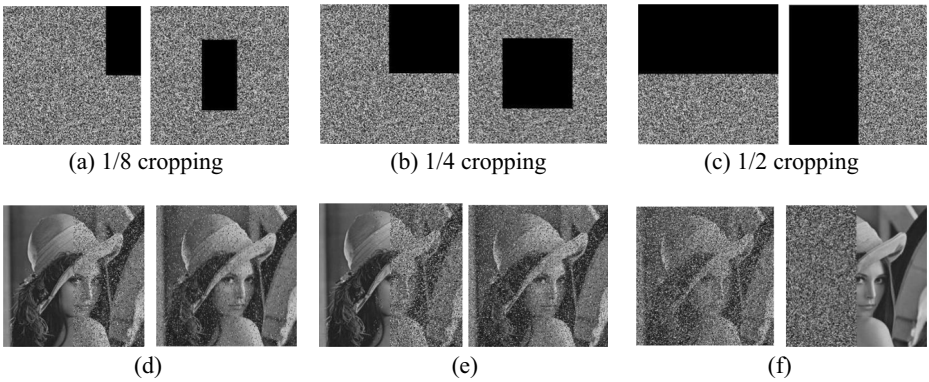


Fig. 9 Cropping attack analysis. **a**-**c** Cropped cipher images **d**-**f** Corresponding decrypted images

Table 12 Noise attack analysis

Salt and pepper noise density	PSNR	MSE
0.01	26.0792	160.3826
0.05	19.0492	809.3903
0.1	16.1265	1586.5

Table 13 Cropping attack analysis

Cropping level	PSNR	MSE
1/8 (Upper right corner)	18.3096	959.6727
1/8 (Centre)	18.5029	917.8980
1/4 (Upper right corner)	15.3177	1911.2
1/4 (Centre)	15.4647	1847.6
1/2 (Horizontal)	12.4716	3680.6
1/2 (Vertical)	12.6096	3565.5

tional complexity is described by the number of times each operation is repeated in various stages based on plain image pixels MxN.

The key generation phase in the proposed algorithm involves generating the two sequences using logistic map and tent map, each sequence equal to half the number of image pixels. So, the time complexity is O(MxN). Another chaotic sequence is generated using logistic map and thus the complexity is O(MxN).

Table 14 shows the number of times various other operations are repeated in the proposed algorithm.

On aggregating all of these operations, the computational complexity of the proposed algorithm is O(20xMxN) which is quite less than the complexity of schemes like [7, 12, 23].

6.10 Speed analysis

Apart from the security requirements, the speed of the algorithm also plays a significant role in a good cryptosystem. The speed analysis of the proposed HAIE algorithm is carried out by measuring the encryption/decryption time for various grayscale images. The scheme has been implemented using MATLAB 2019a on Windows 10 operating system with processor Intel® core™ i7-8565U CPU @ 1.8GHZ and 8GB RAM. The speed analysis of the proposed scheme is shown in Table 15 for different test images.

From Table 15, the average encryption time and decryption time of the proposed scheme for 256 × 256 size images is 1.4626 s and 0.8938 s, respectively, and that for 512 × 512 size images is 4.8987 s and 3.3741 s, respectively.

Table 16 shows the comparison of proposed scheme time with that of the other schemes. It is evident that the speed of the proposed scheme is faster than the speed of other schemes.

Table 14 Computational complexity

Operations	Number of times repeated
Permutation_1	(MxN)/2
Permutation_2	(MxN)/2
DNA encoding_1	4x(MxN)/2
DNA encoding_2	4x(MxN)/2
DNA encoding_3	4xMxN
DNA addition	4xMxN
DNA decoding	4xMxN
XOR	MxN

Table 15 Speed analysis

Image	Average encryption time (s)	Average decryption time (s)
Lena (256×256)	1.4273	0.8760
Baboon (256×256)	1.4707	0.8985
Airplane (256×256)	1.4232	0.8966
Cameraman (256×256)	1.4361	0.8998
Peppers (256×256)	1.5181	0.8941
Boat (256×256)	1.5002	0.8983
Lena (512×512)	4.8852	3.3788
Baboon (512×512)	4.8894	3.3709
Airplane (512×512)	4.9210	3.3760
Peppers (512×512)	4.8993	3.3710

Table 16 Comparison of speed with other algorithms

Image	Average encryption time (s)			Average decryption time (s)		
	Proposed	[13]	[31]	Proposed	[13]	[31]
Lena (256×256)	1.4273	1.914	7.14	0.8760	2.002	25.84
Lena (512×512)	4.8852	7.336	–	3.3788	7.394	–

7 Conclusion

This paper proposed a Hybrid Adaptive Image Encryption (HAIE) scheme based on chaotic maps and DNA computing. The proposed scheme uses two 1D chaotic maps; logistic map and tent map for the generation of random sequences or key streams in the key generation phase. The control parameters and the initial conditions of both the maps are controlled dynamically using statistical characteristics of the plain image. This makes the algorithm resilient to chosen and known plaintext attacks. The algorithm comprises of various other phases. In the permutation phase, half of the plain image is permuted using the logistic map and the other half using tent map, making the final permuted image a hybrid of two half-permuted images. After DNA encoding, the DNA addition operation is used to perform diffusion followed by XOR operation. To validate the effectiveness of the proposed algorithm, various security and performance analysis were carried out. It was observed that the scheme is extremely sensitive to the secret keys and also the key space is significantly large, approximately 2^{215}, making it robust against brute force attacks. The average entropy value of the encrypted images is nearly equal to 8 and the correlation coefficients are very small, close to 0. The average values of NPCR and UACI are 99.61% and 33%, respectively. PSNR and SSIM values also lie in the expected range. Robustness analysis also indicates that the scheme is resilient to noise and cropping attacks. Moreover, the computational complexity of this scheme is lower than some recently presented encryption schemes. A comparison of the proposed scheme with the state-of-the-art schemes shows that it performs better than those under comparison. In the future, we plan to extend this work to color (RGB) images.

Acknowledgements The authors would like to acknowledge the support of JK Science Technology and Innovation Council for funding this work under fund number (JKST&IC/SRE/874-77).

Declarations

- The authors have no relevant financial or non-financial interests to disclose.
- The authors have no competing interests to declare that are relevant to the content of this article.
- All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
- The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Adleman LM (1994) Molecular computation of solutions to combinatorial problems. Science 266(5187): 1021–1024
2. Alghafis A, Firdousia F, Khan M, Batoola SI, Amin M (2020) An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing. Math Comput Simul 177:441–466. https://doi.org/10.1016/j.matcom.2020.05.016
3. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcation Chaos 16(08):2129–2151
4. Arpaci B, Kurt E, Celik K (2020) Colored image encryption and decryption with a new algorithm and a hyperchaotic electrical circuit. J Electr Eng Technol 15:1413–1429
5. Assad SEI, Farajallah M (2016) A new chaos-based image encryption system. Signal Process: Image 41: 144–157
6. Babaei, A, Motameni, H, Enayatifar, R (2019) A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence, Optik. https://doi.org/10.1016/j.ijleo.2019.164000
7. Belazi A, Talha M, Kharbech S, Xiang W (2019) Novel medical image encryption scheme based on chaos and DNA encoding. IEEE Access 7:36667–36681
8. Chai X, Gan Z, Lu Y, Chen Y, Han D (2017) A novel image encryption algorithm based on the chaotic system and DNA computing. Int J Modern Phys C 28(05):1750069
9. Chai X, Gan Z, Yuan K, Chen Y, Liu X (2019) A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput & Applic 31:219–237
10. El-Samie FEA, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie ESM, Alshebeili SA (2013) Image encryption: a communication perspective. CRC Press. https://doi.org/10.1201/b1630
11. Farah MAB, Guesmi R, Kachouri A, Samet M (2020) A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt Laser Technol 121:105777
12. Hua Z, Yi S, Zhou Y (2018) Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process 144:134_144
13. Huang H (2019) Novel scheme for image encryption combining 2D logistic-sine-cosine map and double random-phase encoding. IEEE Access 7:177988–177996
14. Kumar M, Iqbal A, Kumar P (2016) A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process 125:187–202
15. Li C, Luo G, Qin K, Li C (2017) An image encryption scheme based on chaotic tent map. Nonlinear Dyn 87:127–133
16. Luo Y, Yu J, Lai W, Liu L (2019) A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimed Tools Appl 78:22023–22043
17. Luo Y, Tang S, Liu J, Cao L, Qiu S (2020) Image encryption scheme by combining the hyperchaotic system with quantum coding. Opt Lasers Eng 124:105836
18. Mondal B, Mandal T (2017) A lightweight secure image encryption scheme based on chaos and DNA computing. J King Saud Univ Comput Inf Sci 29(4):499–504. https://doi.org/10.1016/j.jksuci.2016.02.003
19. Niu Y, Zhou Z, Zhang X (2020) An image encryption approach based on chaotic maps and genetic operations. Multimed Tools Appl 79:25613–25633. https://doi.org/10.1007/s11042-020-09237-2
20. Patro KAK, Acharya B (2019) An efficient colour image encryption scheme based on 1-D chaotic maps. J Inf Secur Appl 46:23–41
21. Ping P, Fan J, Mao Y, Xu F, Gao J (2018) A chaos based image encryption scheme using digit-level permutation and block diffusion. IEEE Access 6:67581–67593
22. Sravanthi D, Patro KAK, Acharya B, Majumder S (2019) A secure chaotic image encryption based on bit-plane operation. Soft Computing in Data Analytics. Springer, Singapore, pp 717–726
23. Sun S (2018) A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. IEEE Photon J 10(2):1_14
24. Sun S, Guo Y, Wu R (2019) A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping. IEEE Access 7:28539–28547

25. Toughi S, Fathi MH, Sekhavat YA (2017) An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. Signal Process 141:217–227
26. Wang X, Guan N (2020) A novel chaotic image encryption algorithm based on extended zigzag confusion and RNA operation. Opt Laser Technol 131:106366
27. Wu XJ, Wang DW, Kurths J, Kan HB (2016) A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Inf Sci 349-350:137–153
28. Wu, J, Liao, X, Yang, B (2018) Image encryption using 2D Henon-sine map and DNA approach, Signal Process, https://doi.org/10.1016/j.sigpro.2018.06.008
29. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
30. Xuejing K, Zihui G (2020) A new color image encryption scheme based on DNA encoding and spatio-temporal chaotic system. Signal Process Image Commun 80:115670
31. Yasser I, Khalifa F, Mohamed MA, Samrah AS (2020) A new image encryption scheme based on hybrid chaotic maps. Complexity 2020:23
32. Ye GD, Huang XL (2016) A secure image encryption algorithm based on chaotic maps and SHA-3. Secur Commun Netw 9:2015–2023
33. Yu SS, Zhou NR, Gong LH, Nie Z (2020) Optical image encryption algorithm based on phase- truncated short-time fractional Fourier transform and hyper-chaotic system. Opt Lasers Eng 124:105816
34. Zarebnia M, Pakmanesh H, Parvaz R (2019) A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik 179:761–773
35. Zefreh, EZ (2020) An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. Multimed Tools Appl https://doi.org/10.1007/s11042-020-09111-1
36. Zhan K, Wei D, Shi J, Yu J (2017) Cross-utilizing hyperchaotic and DNA sequences for image encryption, Electron. Imaging 26(1):013021
37. Zhang J, Huo D (2019) Image encryption algorithm based on quantum chaotic map and DNA coding. Multimed Tools Appl 78:15605–15621