



# A superlative image encryption technique based on bit plane using key-based electronic code book

Manju Kumari<sup>1</sup> · Shailender Gupta<sup>1</sup> · Anjali Malik<sup>1</sup>

Received: 26 January 2020 / Revised: 30 July 2020 / Accepted: 13 August 2020 /

Published online: 31 August 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2020

## Abstract

To contend with the growing concern of information security, firms are espousing cryptography for protection. To comprehend this need, the paper proposes a block cipher that ensures confidentiality and secrecy for secure data communication network. A high-quality cryptographic process ensures high entropy, high key sensitivity, ability to resist known plaintext and chosen-plaintext attack, high speed of execution, high key space, high randomness and resistance towards differential attack. In projected work, encryption mechanism is comprises of multiple processes and each process is devised key dependent utilizing diverse keys to ensure high key sensitivity and vast resistance power towards differential attack. The keys are generated using contemporary encryption process- the quantum chaotic map due to its high randomness and non periodicity, which includes confusion and diffusion processes. For the confusion process, Electronic Code Book (ECB), Initial Permutation (IP), Bit plane scrambling, and Inter bit plane scrambling are employed. The ECB and IP, being matching processes are chosen for high speed of execution. Bit level permutation unlike byte level is applied to reinforce randomness, in conjunction with variable number of rounds as per the security key. For diffusion process, the folding technique is used along eight directions, exploiting different keys. To reveal the efficacy of the proposed methodology, it is compared with the existing renowned methods on the basis of Cryptanalysis, Perceptibility analysis, Statistical analysis, etc. It is asserted that results such as differential attack, cryptanalysis, and key space analysis are reasonably enhanced than others while entropy and speed of execution are at equivalence with other techniques.

**Keywords** Bit plane scrambling · Block cipher · Confusion · Cryptanalysis · Cryptography · Diffusion · Electronic code book · Encryption · Initial permutation block · Quantum chaotic map

---

✉ Anjali Malik  
anjalmalik0611@gmail.com

Extended author information available on the last page of the article

# 1 Introduction

The world is interconnected by the distinct spectra of technology. Advancement in technology budge into the future of automation which raises reliance on cyber connectivity, resulting in exposure of secret messages, images to the attackers that are always trying to uncover and exploit vulnerabilities. Henceforth necessitates protection of usability for smooth transfusion of data from one port to another [15]. Securing a network is the process of targeting a variety of threats and stopping them from rampaging through the system, as just a few minutes of exposure can cause widespread disruption and massive damage to public and private organization's bottom line and reputation; thus protective measures must always be in place. Confidentiality is the core ingredient that accounts for the plausibility of security services for a message. Mainly providing privacy between the sender and the user is advocated by the phenomena of confidentiality. The authorization over data is held confidential only to the permitted users, attaining garbage values for an unauthorized user. As described, Images perform very crucial role in communication of information on insecure channels. So, this paper works upon the principle of preserving confidentiality particularly for images.

Cryptography [12] is regarded as the art of euphemism of messages to codes or ciphers to prevent it from being deciphered by adversaries. Extensive researches are going on in this direction for securing images that are transferred in data communication network.

Previously designed encryption techniques [2, 7, 8, 12, 16, 18, 19, 21, 22, 25] were complicated and were compatible mainly with texts. The techniques possessed low randomness, limited key size and consumed large processing time to encrypt images, while small key space leads to an easy intruder attack. Chaos-based techniques [6, 9, 10, 13, 23, 24, 27] were evolved and considered for securing confidentiality for the communication of images over the network. In this modification secret keys were used at multilevel processing of encryption of images before transmission. In chaos based mechanisms the pixel positions and values are both modified using confusion and diffusion respectively. The randomness of encrypted images is much larger due to the nonlinear characteristics of chaotic maps used. Furthermore, Quantum chaos [1, 3, 14] based logistic maps were put to use to encrypt images, which results in improvement of all the parameters like randomness, entropy, key sensitivity, image perceptual quality and time complexity. Recently proposed Quantum Qubit based techniques [15, 28] lead to further increase in the extent of randomness and entropy due to the usage of bit instead of byte plane encryption.

This paper attempts to develop a fine quality cryptography technique. The projected work is a block cipher based system that consists of both confusion and diffusion processes. The hallmarks of the proposed scheme are:

- To ensure high key sensitivity, the confusion and diffusion processes of encryption changes utterly on altering one bit of key. Thus results in a completely different encrypted image and making the process more secure.
- The number of iterations for the confusion process is dynamic; it depends on the key which makes the encryption process more secure. As the key changes, the number of iterations also changes resulting in increased randomness.
- In confusion process ECB (Electronic Code Book) and IP block are used to secure the data by altering the pixels of an image. As ECB and IP are matching processes, so it will augment speed of execution.
- The folding procedure used for the diffusion process uses different keys for diverse directions of folding applicable on three channels of colored image independently. This not only increases the key space but also enhance randomness in the mechanism.

- To ensure high entropy value of encrypted image and low correlation among adjacent pixels, bit plane manipulation of pixels is executed. Both intra and inter bit plane scrambling operations are performed on all the channels collectively instead of scrambling the bit planes of R, G, B channels individually.
- To ensure vast resistance power towards differential attack, all the processes utilize different keys, resulting in dissimilar operation for separate set of keys. This will ensure success in differential analysis.

Hence the proposed technique consists of complex processes, passes UACI & NPCR test, consumes less time to execute and fulfill all the major requirements. Rest of the paper is organized as follows: Section 2 gives the literature survey along with some preliminary concepts. The proposed mechanism is described in detail under section 3. Section 4 provides the setup parameters. The complete investigation of results is performed in section 5 followed by overall comparison and references.

## 2 Literature survey

Various techniques are available in literature which has done confusion and diffusion process utilizing different algorithms.

After the usage of traditional encryption mechanisms [2, 7, 8, 12, 16, 18, 19, 21, 22, 25], Chaos-based techniques [6, 9, 10, 13, 23, 24, 27] were evolved and considered for securing confidentiality for the communication of images over the network. In these, the pixel positions and values are both modified using confusion and diffusion respectively. The randomness of encrypted images is much larger due to the nonlinear characteristics of chaotic maps used. Few chaos based techniques available in the literature are described below:

M. Francois et al. [9] utilised chaotic function based on linear congruence is used to generate large chaotic keys. Coupling of chaotic function with a XOR operation on binary treatment during encryption process is done to enhance the randomness. I.Shatheesh Sam et al. [23] used bit permutation as the confusion process for scrambling of pixels and non linear followed by zig zag diffusion for alteration of pixel values. Mixed transformed logistic map is used to generate chaotic keys. It also uses mixing of color pixels making it highly secure mechanism. I.Shatheesh Sam et al. [24] utilized intertwining chaotic map to enhance key length. Nonlinear and sub diagonal diffusion of adjacent pixels is done to alter the pixel values. It also uses process such as permutation and byte substitution to improve the randomness. Guodong Ye et al. [27] performed permutation, modulation, diffusion (PMD) operations to alter pixel values and positions. Information entropy is employed to make the permutation's key stream dependent on plain image. Modulation operation is introduced between the permutation and diffusion process to avoid the failing of unchangeable gray distribution before diffusion. Gururaj Hanchinamani et al. [10] used Peter De Jong chaotic map to determine initial keys for RC4 generator and also for permutation process. RC4 stream generator provides pseudorandom numbers for diffusion process. Processing time is improved due to simple algorithm but the complexity and randomness is high because of the Peter De Jong chaotic map.

Furthermore, Quantum chaos [1, 3, 14] based logistic maps were put to use to encrypt images, which results in improvement of all the parameters like randomness, entropy, key sensitivity, image perceptual quality and time complexity. Some of the Quantum chaos based techniques are explained below.

Ahmed A. Abd El-Latif et al. [3] used toral automorphism integer wavelet transform for scrambling only the Y (Luminance) component of low frequency sub band. Quantum logistic map is used to generate chaotic keys at both horizontal and vertical diffusion stage. Substitution/ confusion is done using chaotic key stream generated with the help of adapted quantum chaotic system. A. Akhshani et al. [1] used Dissipative quantum logistic map in 3-dimensional form. Hui Liu et al. [14] proposed a general Arnold scrambling algorithm in which keys are exploited to permute the pixels of color components. In order to get the high randomness and complexity, the two-dimensional logistic map and quantum chaotic map are coupled with nearest-neighboring coupled-map lattices. An improved Arnold transform map enlarges the key space to resist against any key sensitivity. The folding of plain image during diffusion process is done to achieve sensitivity, robustness, resistance against common attacks, large key space.

Recently proposed Quantum Qubit based techniques [15, 28] lead to further increase in the extent of randomness and entropy due to the usage of bit instead of byte plane encryption. Some of the techniques are explained below.

Nanrun Zhou et al. [28] proposed a new cross-exchange operation under quantum color image, which is applied to scramble the original image. The initial parameters of the 5D hyper-chaotic system are employed to increase the number of keys and key space. Channel swapping operation is used to diffuse the gray values of corresponding pixels. The parallel computation and the bit-level quantum color image encryption reduce the computational complexity. Xingbin Liu et al. [15] utilized both intra and inter bit level permutation on bit planes to scramble pixel positions. The intra bit permutation is achieved by sorting chaotic sequence key generated by applying quantum logistic map. The inter bit permutation is done by applying qubit XOR operations between the two selected bit planes.

Table 1 defines the abbreviations used in the paper. The surveyed encryption techniques are described concisely in the Table 2 given below:

As seen in Table 2, most of the techniques possesses admirable image perceptual quality but doesn't provide optimum values for the other desired parameters i.e. methods does not live up to expectations from many prospective. Some chaotic techniques have large time complexity which is not a preferred property of cryptography techniques for real-time long-distance communication whereas qubit quantum techniques come up to overcome many shortcomings of previously designed mechanisms but fail in NPCR and UACI tests.

The objectives for the proposed work are to achieve high randomness, high entropy, high speed of execution, resistance towards differential attacks, high key space, low correlation in all the three directions, high image perceptual quality and resistant toward known plaintext attack and chosen plain text attack.

### 3 Preliminary knowledge

- **Quantum Chaotic Map**

To protect information various image encryption schemes are proposed which are designed on the basis of various maps. Chaotic systems have various features such as sensitivity to initial conditions and parameters, high efficiency, ergodicity which makes it appropriate for secure image encryption schemes.



**Table 1** Abbreviations used in the paper

ABBREVIATIONS USED IN THE PAPER	
ECB	Electronic Code Book
IP	Initial Permutation
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
KS	Key Space
IPQ	Image Perceptual Quality
NPCR	Number of Pixel Change Ratio
UACI	Unified Average Change in Intensity
SOE	Speed of Execution
KSA	Key Sensitivity Analysis
RA	Randomness Analysis
KPA	Known Plaintext Attack
CPA	Chosen Plaintext Attack

Nowadays, image encryption schemes use quantum chaotic systems to generate pseudo random sequence due to their excellent properties such as randomness, sensitive to initial conditions and deterministic nature [20]. The randomness and non-periodicity of quantum chaotic map are successfully verified by statistical complexity and the normalized Shannon entropy [4, 11].

To study the effects of quantum corrections,  $a = \langle a \rangle + \Delta a$  is considered, where  $\Delta a$  is quantum fluctuations about  $\langle a \rangle$  [4]. The quantum chaotic map with lowest order quantum corrections is followed by the following equations:

$$\begin{cases}
 x(i + 1) = r(x(i) - (\text{abs}(x(i)))^2) - r * y(i) \\
 y(i + 1) = (-y(i) * \exp(-2\beta)) + \left( \exp(-\beta) * r \left[ (2 - x(i) - \overline{x(i)})y(i) - x(i)\overline{z(i)} - \overline{x(i)}z(i) \right] \right) \\
 z(i + 1) = (-z(i) * \exp(-2\beta)) + \left( \exp(-\beta) * r \left[ 2(1 - \overline{x(i)})z(i) - 2x(i)y(i) - x(i) \right] \right)
 \end{cases}
 \tag{1}$$

where  $x = \langle a \rangle$ ,  $y = \langle \Delta a + \Delta a \rangle$ ,  $z = \langle \Delta a, \Delta a \rangle$  and  $\beta$  are dissipation parameter and in general  $x(i)$ ,  $y(i)$  and  $z(i)$  are complex numbers with  $\overline{x(i)}$ ,  $\overline{z(i)}$  be the complex conjugate of  $x(i)$  and  $z(i)$

**Table 2** Literature survey

Paper Reference	Image Perceptual Quality	UACI/NPCR	Key Space	Key Sensitivity Analysis	Randomness	Speed of Execution
[9]	Low	Pass	High	High	High	Slow
[23]	High	Pass	High	High	High	Slow
[24]	High	Pass	High	High	High	Slow
[27]	High	Pass	High	High	High	Moderate
[10]	High	Pass	High	High	High	High
[3]	High	Pass	Moderate	High	High	High
[1]	High	Pass	High	High	High	High
[14]	Low	Pass	High	High	High	Moderate
[28]	High	Fail(NPCR)	Moderate	High	Moderate	Slow
[15]	High	Fail	High	High	High	Slow

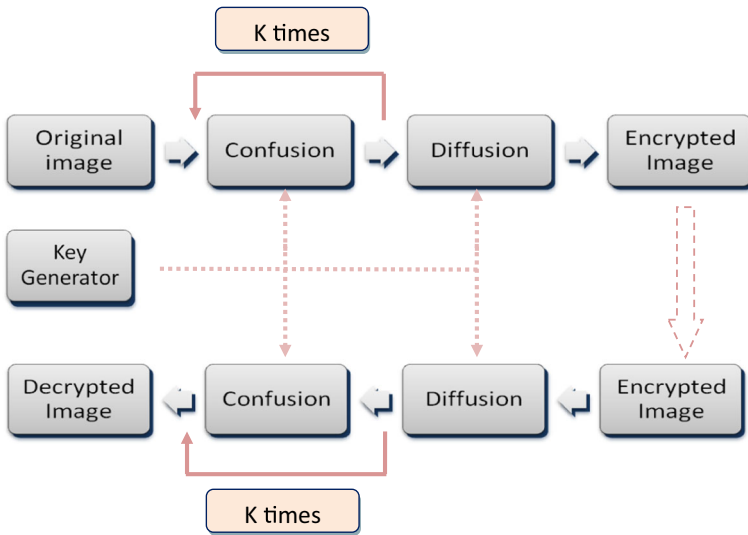


Fig. 1 Basic block diagram of encryption and decryption process of proposed technique

respectively. If initial conditions being real values then all successive values will also be real. The random sequences used in subsequent sections are generated with a quantum chaotic map because it is a special case in limiting the strong dissipation.

### 4 Proposed encryption scheme

Figure 1 shows the basic block diagram of the encryption and decryption process of the proposed model.

The proposed encryption scheme is elaborated in this section. The whole image encryption process includes two stages, i.e. confusion and diffusion along with requirement of keys to be used in these two processes. These are created using key generation algorithm.

#### 4.1 Key generation

The keys are generated using the quantum chaotic maps so that initial conditions and control parameters are highly sensitive to the changes in even a single bit change in the secret key.

Table 3 m values corresponding to different key values

Key	m values
k1, k2, k28-k54	256
k3-k27	24
k55	4

The algorithm for the key generation and creating random sequence of diverse sizes using the key is given below.

---

**ALGORITHM FOR KEY GENERATION AND GENERATING RANDOM SEQUENCE OF DIFFERENT SIZES USING KEY**

---

```

STEP 1: INPUT x(1)=0.4523444336; y(1)=0.003453324562; z(1)=0.001324523564;
r=3.9;b=4.5; xn=0.002; zn=0.004;keys=[k1,k2,k3,...,k55]; [m n p]=size of
image
STEP 2: ITERATE QUANTUM CHAOTIC MAP 1000 TIMES TO ELIMINATE TRANSIENT
EFFECTS
FOR (i=1:1:1000)
    x(i+1)=r*(x(i)-(abs(x(i)))^2)-r*y(i);
    y(i+1)=(-y(i)*exp(-2*b))+(exp(-b)*r*((2-x(i)-xn)*y(i)-x(i)*zn-
    xn*z(i)));
    z(i+1)=(-z(i)*exp(-2*b))+(exp(-b)*r*(2*(1-xn)*zn-2*x(i)*y(i)-
    xn));
END
STEP 3: INPUT x1(1)=x(1001); y1(1)=y(1001); z1(1)=z(1001); %This becomes
the initial condition for generating the required keys in the steps given
below after elimination of transient effects.
STEP 4: ITERATING THE MAP TO GET x1, y1 AND z1 VALUES NEEDED FOR KEYS (k1-
k55)
FOR (j=1:1:55)
    x1(j+1)=r*(x1(j)-(abs(x1(j)))^2)-r*y1(j);
    y1(j+1)=(-y1(j)*exp(-2*b))+(exp(-b)*r*((2-x1(j)-xn)*y1(j)-
    x1(j)*zn-xn*z1(j)));
    z1(j+1)=(-z1(j)*exp(-2*b))+(exp(-b)*r*(2*(1-xn)*zn-2*x1(j)*y1(j)-
    xn));
END
STEP 5: APPLYING ROUND AND MOD FUNCTION AND MULTIPLICATION OPERATION TO GET
NECESSARY KEY VALUES IN INTEGER FOR GENERATING RANDOM VALUES OF DIFFERENT
SIZE.
    COMPUTE k55=round(mod(((z1(55)*2^32)),4)); %mod 4 is done to get
the key k55 value in range 0 to 4.
    COMPUTE k1=round(mod(((y1(1)*2^32)),256)); %mod 256 is done to
get the key k1 value in range 0 to 256.
STEP 6: Random sequence sk1 using key k1:
    rng(k1)
    sk1=randperm(256); % randperm (256) is used to generate scrambled
sequence containing values from 1 to 256. It is used in matching
process.
STEP 7: COMPUTE k2=round(mod(((y1(2)*2^32)),256));
STEP 8: Random sequence sk2 using key k2:
    rng(k2)
    sk2=randperm(m*n);
STEP 9: COMPUTE k3=round(mod(((y1(3)*2^32)),24));
STEP 10: Random sequence sk3 using key k3:
    rng(k3)
    sk3=randperm(24);
STEP 11: FOR (i=1:1:24)
    ki+3=round(mod(((x1(i+3)*2^32)),24));
    Random sequences ski+3 using keys ki+3:
    rng(ki+3)
    ski+3(:,i)=randperm(m*n);
END
STEP 12: FOR (i=1:1:27)
    ki+27=round(mod(((x1(i+27)*2^32)),256));
    Random sequence sk(:,i) using keys ki+27:
    rng(ki+27)
    sk(:,i)=randi([0,255],m); % To generate random matrix of
size m*m with values 0 to 255 randi([0,255],m) is used.
END

```

---

**Table 4** Different keys used for generation of random sequence of varying sizes and values, corresponding to the encryption block

Sequence Using Keys/ Key	Used in the encryption block	Random sequence size for $m*n*3$ image using Key
sk1	ECB block in confusion process	$1*256$
sk2	IP block in confusion process	$1*(m*n)$
sk3	Bit plane scrambling in confusion process	$1*24$
sk4-sk27	Inter bit plane scrambling in confusion process	$1*(m*n)$
sk28-sk54	Diffusion process	$1*256$
k55	The number of times confusion process is through	$1*1$

The quantum chaotic map given in Eq. 1 is iterated 1000 times using  $x = 0.4523444336$ ,  $y = 0.003453324562$ ,  $z = 0.001324523564$ ,  $\bar{x} = 0.002$ ,  $\bar{z} = 0.004$ ,  $r = 3.9$  and  $\beta = 4.5$  as initial condition and control parameters in order to remove the transient effect. Then, the map is iterated to get  $x_1$ ,  $y_1$  and  $z_1$  values needed for generating keys (k1-k55).

Further, round and mod function along with multiplication operations are applied as given in Eq. 2 to get necessary key values in integer format for generating random values of different sizes.

$$k(i) = (x(i) * 2^{32}) \bmod m \quad (2)$$

Finally random sequences are generated, (sk<sub>1</sub> to sk<sub>55</sub>) which are used in different encryption process.

Table 3 shows the values ‘m’ (in Eq. 2) for corresponding keys by which mod is taken.

Table 4 shows the different keys used for the generation of a random sequence of varying sizes and values, corresponding to the encryption block. Different processes of proposed scheme use a diverse set of keys for the generation of random sequence which is further used in the process for encryption and decryption of an image.

## 4.2 Confusion process

The process applies a random key sequence generated using keys K each in different confusion processes as described in Table 4. This progression helps in securing the data by making a complicated relationship between the encrypted data and the keys. Usage of this procedure makes it hard for the unauthorized source to find the key even if large combinations of original data and encrypted data are found. The confusion process includes ECB (Electronic Code Book), IP block (Initial Permutation), Bit plane scrambling, and Inter bit plane scrambling. Figure 2 shows the basic block diagram of the confusion process with the corresponding keys used in each process. These courses of action are iterated for k times and this k value is at variance for different secret keys. K value is found using k55 key whose range is from 1 to 4 and different values of k makes it more difficult for the unauthorized source to find the number of iteration for decrypting the data.

### 4.2.1 ECB (electronic code book)

In cryptography, block cipher mode of operation is an algorithm which utilizes a block cipher for providing security. Electronic code book is one of such algorithm and is the straight forward way of changing the data. In this process, a codebook is generated by using a random sequence with all the values from 0 to 255, corresponding to each pixel value of an image

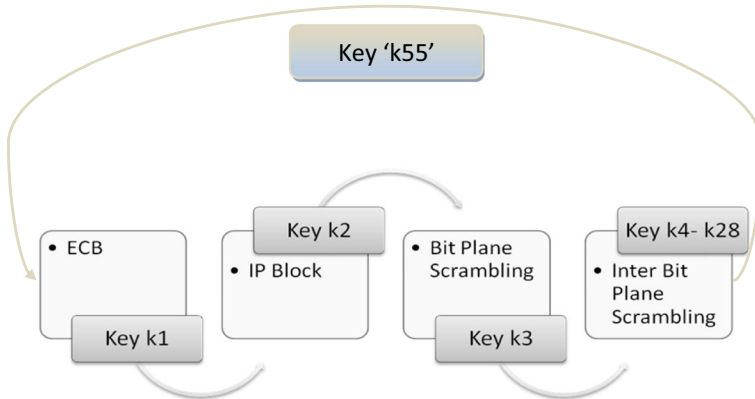


Fig. 2 Block diagram of confusion process

using random sequence  $sk_1$  generated using key  $k_1$ . This generated codebook replaces the pixel values of all the 3 planes R, G, B of the color image with the assigned value in it. Entire procedure is deterministic as if original data are replaced twice using the same random sequence or key, then the encrypted data is the same as original data. The algorithm for the first stage of confusion process i.e. Electronic Code Book is given below.

---

**ALGORITHM FOR ELECTRONIC CODE BOOK (ECB) CONFUSION PROCESS**

---

**Input:** I= RGB Image;  $sk_1(i)$ : value at  $i$ th position of random sequence generated using key  $k_1$ ; [R G B]: R, G, B planes of image I; [m n p]: size (I); (i, j):  $i$ th row and  $j$ th column pixel of image; I'ecb= output confused image of ECB process

```

STEP 1: FUNCTION I'ecb= ECB (I,sk1)
    STEP 1a:  $sk_1=sk_1(1:256)-1$ ;
    STEP 1b: FOR  $i=1:l:m$ 
                FOR  $j=1:l:n$ 
                     $R'(i, j)=sk_1(R(i, j)+1)$ ;
                     $G'(i, j)=sk_1(G(i, j)+1)$ ;
                     $B'(i, j)=sk_1(B(i, j)+1)$ ;
                END
            END

```

```

STEP 2: COMPUTE  $I'ecb=[R' G' B']$ 

```

---

**4.2.2 IP block**

This process is similar to the s-box used in AES [21]. In this process, a random 1-dimensional sequence is generated with the values from 1 to each plane size of an image (i.e.  $m*n$  for the color image of size  $m*n*3$ ) using random sequence  $sk_2$  generated using key  $k_2$ . The values of the sequence correspond to the position where the pixel value needs to be placed and the inverse process also uses the same key and changes the position of the pixel value back to the original position. This process scrambles the pixel values but does not change the value of an image pixel. This progression is followed by method for altering bits within pixels. The algorithm for the second stage of confusion process i.e. Initial Permutation (IP) Block is given below.

---



---

**ALGORITHM FOR INITIAL PERMUTATION (IP) BLOCK OF CONFUSION PROCESS**


---



---

**Input:** I= RGB Image; sk2(i): value at ith position of random sequence generated using key k2; [R G B]: R, G, B planes of image I in 1D array of size (1,m\*n); [m n p]: size (I); (i,j): ith row and jth column pixel of image; I'IP= output confused image of IP process

```

STEP 1: FUNCTION I'IP= ip_block(I'ecb,sk2);
        STEP 1a: FOR (i=1:m*n)
                    R'(sk2(i))=R(i);
                    G'(sk2(i))=G(i);
                    B'(sk2(i))=B(i);
        END
STEP 2: Convert R', G' and B' into matrix of size m*n
STEP 3: COMPUTE I'IP=[R' G' B']

```

---



---

### 4.2.3 Bit plane scrambling

Subsequent to byte level permutation in IP stage, bit level alteration is executed in bit plane and inter bit plane scrambling steps. A color image is a combination of RGB channels. The pixel values of the color image are changed by bit plane scrambling process. In this process,

- All the three channels (R, G, B) of a colored image are divided into the 8-bit planes each to get 24-bit planes.
- Using key k3 a random sequence sk<sub>3</sub> of values 1 to 24 is created only once.
- Now all the 24-bit planes are scrambled according to the random sequence. For e.g., if in random sequence first value is 15, that means now the first-bit plane will be the 15th bit plane of the image. So, all the 24-bit planes are scrambled using this process.
- Reverse bit plane process is exactly the reversal of this procedure.

The algorithm for the third stage of confusion process i.e. Bit plane scrambling process is given below.

---



---

**ALGORITHM FOR BIT PLANE SCRAMBLING CONFUSION PROCESS**


---



---

**Input:** bp= bit planes of RGB Image (m\*n\*24); sk3(i): value at ith position of random sequence generated using key k3; I'bps= output confused image of IP process

```

STEP 1: FUNCTION I'bps= bit_plane_scramb(bp,sk3)
        STEP 1a: FOR (i=1:1:24)
                    I'bps(:, :, i)=bp(:, :, sk3(i));
        END

```

---



---

### 4.2.4 Inter bit plane scrambling

In this stage of bit level scrambling, a random sequence of size 1\*(m\*n) is generated, having values from 1 to m\*n only once.

- The  $i^{\text{th}}$  bit plane is converted into a 1D array ( $1*(m*n)$ ). The values of the sequence correspond to the position where the bit value needs to be placed and the inverse process also uses the same key and amends the position of the bit value back to the original position.
- Now all the bit planes are combined back to get the image of size  $m*n*3$ .

The algorithm for the last stage of confusion process i.e. Inter bit plane scrambling is given below.

---



---

#### ALGORITHM FOR INTER BIT PLANE SCRAMBLING CONFUSION PROCESS

---



---

**Input:** I= RGB Image; ski+3(:, :, i): value at ith position of random sequence generated using key k2; [R G B]: R, G, B planes of image I in 1D array of size (1,m\*n); [m n p]: size (I); (i,j): ith row and jth column pixel of image; I'IP= output confused image of IP process

```

STEP 1: Function A= inter_bit_scramb (I'bps,ski+3)
STEP 1a: a=reshape(I'bps,1,m*n);
STEP 1b: For (i=1:m*n)
            A(ski+3(i))=a(i);
            End
STEP 1c: COMPUTE I'ibp=reshape(A,m,n);
  
```

#### ALGORITHM

```

STEP 1: For (i=1:1:24)
            I'ibp(:, :, i)=inter_bit_scramb (I'bps(:, :, i),ski+3(:, :, i));
            End
  
```

---



---

The number of iterations to be performed for the complete encryption process is based on the key k55. The value of k55 is in the range from 1 to 4. This elevates the security of the encryption process for making it extremely protected.

### 4.3 Diffusion process

Confusion stage is trailed with diffusion process, which applies a random key sequence generated using keys  $K_{R, G, B}$  each in different processes for all the 3 channels (R, G, B). This process aids in escalating redundancy. Even a single bit change in the secret key makes non uniform changes in the image, which makes it harder for the unauthorized user to detect the data correctly. In this procedure, the folding technique is used along 8 directions and for each path diverse key is utilized. The block diagram of the diffusion process with folding is shown in Fig. 3. The process is described as follows:

- Using key k28-k54, a random matrix  $sk_{28}$ - $sk_{54}$  of size  $m*n$  is generated having values from 0 to 255. From this, we get 27 matrices to say X28, X29... X54.
- For the R channel, the key matrix used is X28 to X36, whereas, for G channel, the key matrix used is X37 to X45 and for B channel, the key matrix used is X46 to X54.
- To explain the process, just the R channel is taken into consideration. The R channel matrix is folded from 8 directions for encryption. Eight directions include eight rounds.



The algorithm of the Diffusion process for the proposed technique is given below.

---



---

**ALGORITHM FOR DIFFUSION PROCESS**

---



---

**STEP 1 (Fig 4a, 4b):**

THE MATRIX  $R'$ , IS DIVIDED INTO TWO EQUAL HORIZONTAL PARTS:  $H_u$  and  $H_l$ .

$$\text{STEP 1a: } H_u'(i,j) = H_u(i,j) \oplus X28(i,j) \quad (3)$$

$$\text{STEP 1b: } H_l'(m-i+1,j) = H_u(m-i+1,j) \oplus H_u'(i,j) \quad (4)$$

Where  $i=1, 2, \dots, m/2$  and  $j=1, 2, \dots, n$  AND  $\oplus$  DENOTES XOR OPERATION.

**STEP 2 (Fig 5a, 5b):**

THE MATRIX  $R_1$  OBTAINED AFTER STEP 1 IS DIVIDED INTO TWO EQUAL DIAGONAL PARTS:  $T_u$  and  $T_l$ .

$$\text{STEP 2a: } T_u'(i,j) = T_u(i,j) \oplus X29(i,j) \quad (5)$$

$$\text{STEP 2b: } T_l'(j,i) = T_l(j,i) \oplus T_u'(i,j) \quad (6)$$

Where  $i=1, 2, \dots, m$  AND  $j=i, i+1, \dots, n$ .

**STEP 3 (Fig 6a, 6b):**

THE MATRIX  $R_2$  OBTAINED AFTER STEP 2 IS DIVIDED INTO TWO EQUAL VERTICAL PARTS:  $V_r$  and  $V_l$ .

$$\text{STEP 3a: } V_r'(i,j) = V_r(i,j) \oplus X30(i,j) \quad (7)$$

$$\text{STEP 3b: } V_l'(i, n-j+1) = V_l(i,j) \oplus V_r'(i, n-j+1) \quad (8)$$

WHERE  $i=1, 2, \dots, m$  AND  $j=n/2+1, n/2+2, \dots, n$

**STEP 4 (Fig 7a, 7b):**

THE MATRIX  $R_3$  OBTAINED AFTER STEP 3 IS DIVIDED INTO TWO EQUAL DIAGONAL PARTS:  $T_u$  and  $T_l$ .

$$\text{STEP 4a: } T_l'(i,j) = T_l(i,j) \oplus X31(i,j) \quad (9)$$

$$\text{STEP 4b: } T_u'(i,j) = T_u(i,j) \oplus T_l'(i,j) \quad (10)$$

WHERE  $i=1, 2, \dots, m$  AND  $j=n-i+1, n-i+2, \dots, n$ .

**STEP 5 (Fig 8a, 8b):**

THE MATRIX  $R_4$  OBTAINED AFTER STEP 4 IS DIVIDED INTO TWO EQUAL HORIZONTAL PARTS:  $H_u$  and  $H_l$ .

$$\text{STEP 5a: } H_l'(i,j) = H_l(i,j) \oplus X32(i,j) \quad (11)$$

$$\text{STEP 5b: } H_u'(n-i+1,j) = H_u(n-i+1,j) \oplus H_l'(i,j) \quad (12)$$

WHERE  $i=m/2+1, m/2+2, \dots, m$  AND  $j=1, 2, \dots, n$ .

**STEP 6 (Fig 9a, 9b):**

THE MATRIX  $R_5$  OBTAINED AFTER STEP 5 IS DIVIDED INTO TWO EQUAL DIAGONAL PARTS:  $T_u$  and  $T_l$ .

$$\text{STEP 6a: } T_l'(i,j) = T_l(i,j) \oplus X33(i,j) \quad (13)$$

$$\text{STEP 6b: } T_u'(j,i) = T_u(j,i) \oplus T_l'(i,j) \quad (14)$$

WHERE  $i=1, 2, \dots, m$  AND  $j=1, 2, \dots, i-1$ .

**STEP 7 (Fig 10a, 10b):**

THE MATRIX  $R_6$  OBTAINED AFTER STEP 6 IS DIVIDED INTO TWO EQUAL DIAGONAL PARTS:  $V_l$  and  $V_r$ .

$$\text{STEP 7a: } V_l'(i,j) = V_l(i,j) \oplus X34(i,j) \quad (15)$$

$$\text{STEP 7b: } V_r'(i, n-j+1) = V_r(i,j) \oplus V_l'(i, n-j+1) \quad (16)$$

WHERE  $i=1, 2, \dots, m$  AND  $j=1, 2, \dots, n/2$ .

**STEP 8 (Fig 11a, 11b):**

THE MATRIX  $R_7$  OBTAINED AFTER STEP 7 IS DIVIDED INTO TWO EQUAL DIAGONAL PARTS:  $T_u$  and  $T_l$ .

$$\text{STEP 8a: } T_u'(i,j) = T_u(i,j) \oplus X35(i,j) \quad (17)$$

$$\text{STEP 8b: } T_l'(i,j) = T_l(i,j) \oplus T_u'(i,j) \quad (18)$$

WHERE  $i=1, 2, \dots, m$  AND  $j=1, 2, \dots, n-i$ .

**STEP 9:** AFTER ROUND 8, MATRIX  $R_8$  IS XORED WITH  $X36$ , AND FINALLY RESULTED IN AN ENCRYPTED IMAGE  $ER$ . STEPS 1 To 9 ARE CARRIED OUT FOR  $G'$  AND  $B'$  CHANNEL

---



---

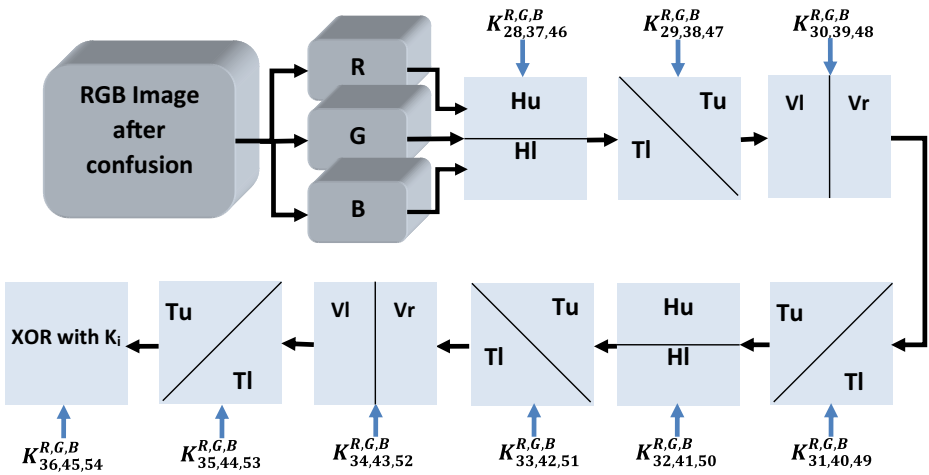


Fig. 3 Block diagram of diffusion process

This was the complete process to encrypt the R channel. Similarly, G and B channels are encrypted using keys and key matrix corresponding to them, to get EG and EB 0028 (Figs. 4-11).

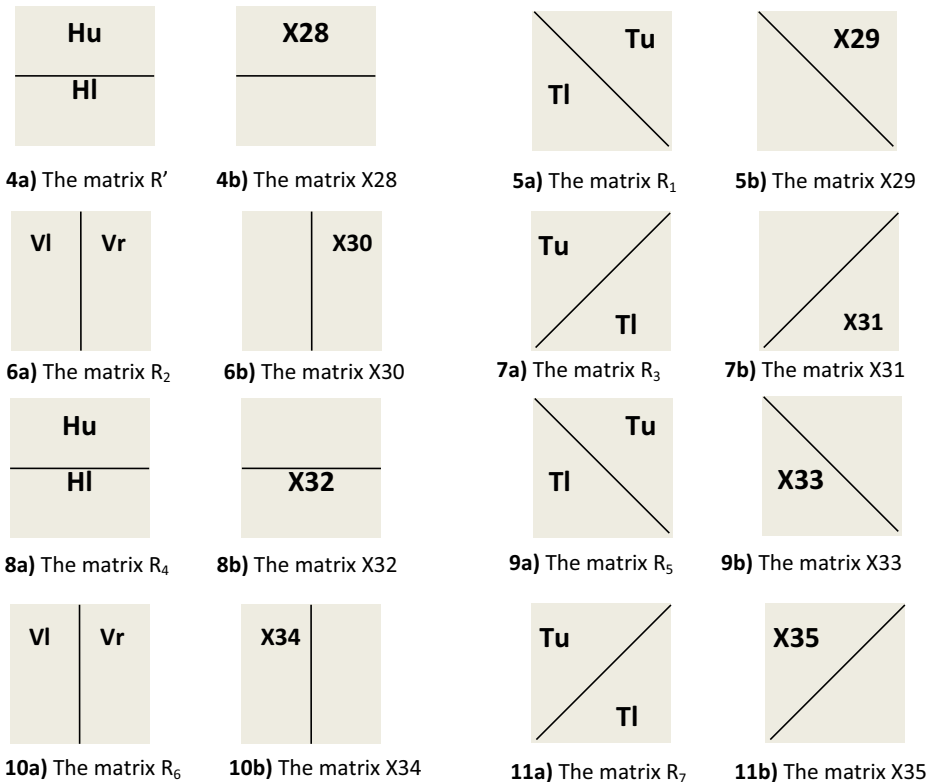


Fig. 4-11 Diffusion Process of the proposed encryption

The reverse of the diffusion process is performed using the same key and the key matrix generated using the key. Firstly, all three channels ER, EG and EB of the encrypted image are XORed with the key matrix X36, X45, and X54 respectively. Then, the process of opening the folded matrix is performed on all the channels. For e.g. the opening process for round 1 is as follows:

$$DHI(m-i+1, j) = DHI'(m-i+1, j) \oplus DHu'(i, j) \quad (12)$$

$$DHu(i, j) = DHu'(i, j) \oplus X28(i, j) \quad (13)$$

where  $i = 1, 2, \dots, m/2$  and  $j = 1, 2, \dots, n$ .

Similarly, opening process is performed for all the 8 rounds and for all the 3 channels. The decryption process is performed just in the reverse manner of encryption process. Next section provides set up parameters used in this work.

## 5 Simulation setup parameters

Table 5 provides simulation setup parameters used, while performing different experiments using proposed mechanism.

## 6 Simulation results and security analysis

The results are simulated in the MATLAB version R2014a. The simulation results of the proposed mechanism are demonstrated as follows. These shown results are an average for 10 images of two different sizes for the below mentioned performance matrices:

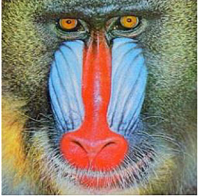

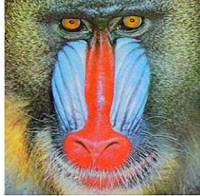
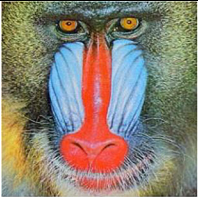

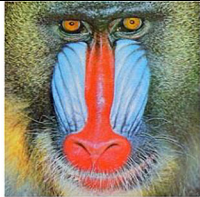
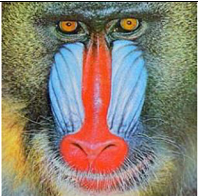

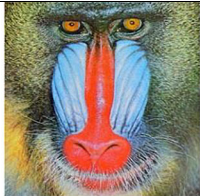
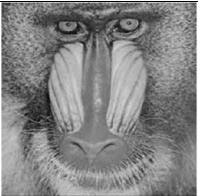
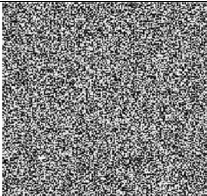
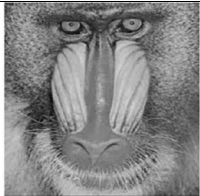
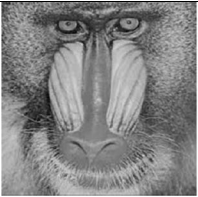
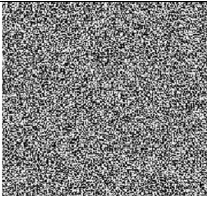
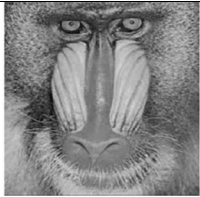
- **Visual Analysis**

A good image encryption scheme shows no visual information similarity to the original image. Table 6 shows the Visual analysis of images of sizes 256\*256 and 512\*512 of the proposed technique and different techniques available in the literature. It can be seen that the encrypted image does not show any visual resemblance with the original image due to multilevel encryption process.

**Table 5** Setup parameters

Processor	1.50GHz Intel Core i3
Operating system	Windows 8
Image type	.jpg, .jpeg
Simulation tool	MATLAB version: R2014a serial update 2
Color type	RGB
Key used in Quantum Chaotic Encryption	$x = 0.4523444336$ , $y = 0.003453324562$ , $z = 0.001324523564$ , $\bar{x} = 0.002$ , $\bar{z} = 0.004$ , $r = 3.9$ and $\beta = 4.5$

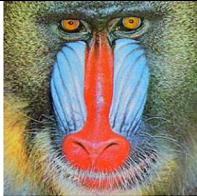

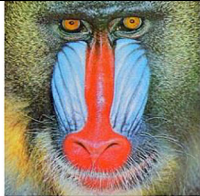
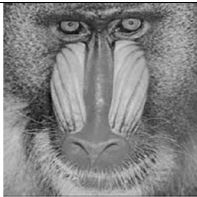
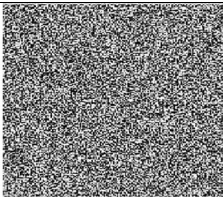
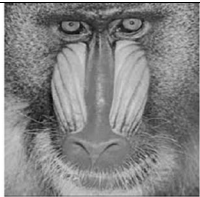
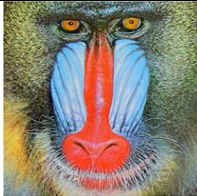

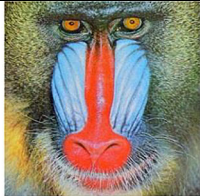
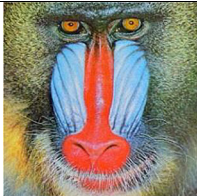

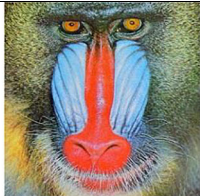
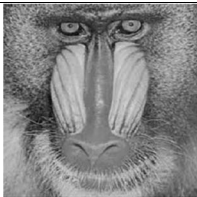
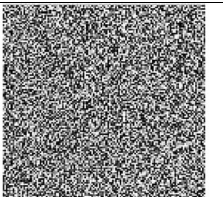
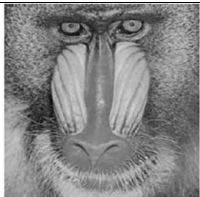
**Table 6** Visual analysis of different size of images

IMAGE SIZE (256*256)			
TECHNIQUE	ORIGINAL IMAGE	ENCRYPTED IMAGE	DECRYPTED IMAGE
Chaos 1 [9]			
Chaos 2 [23]			
Chaos 3 [24]			
Chaos 4 [27]			
Chaos 5 [10]			

- **Histogram Analysis**

Histogram of an image [15] is a graphical portrayal of the frequency distribution of the pixel intensity values present in a computerized image. Table 7 shows the histogram analysis of

Table 6 (continued)

<b>Quantum Chaos 1 [3]</b>			
<b>Quantum Chaos 2 [1]</b>			
<b>Quantum Chaos 3 [14]</b>			
<b>Quantum Chaos 4 [28]</b>			
<b>Quantum Chaos 5 [15]</b>			

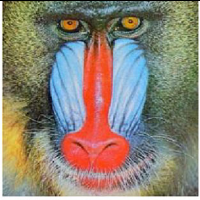
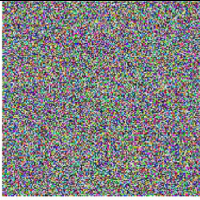
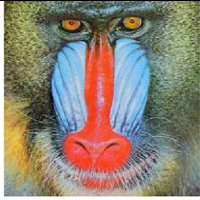



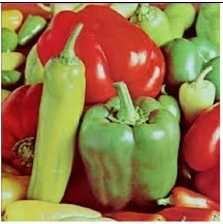


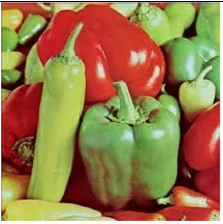


original, encrypted and decrypted images for the proposed scheme of image size  $256 \times 256$  and  $512 \times 512$ . The histograms of the original and encrypted images are not similar. The histogram of the encrypted image is moderately uniform which shows that the attack based on the histogram is difficult.

- **Correlation Analysis**

In addition to statistical analysis [5], correlation analysis is also performed on images. An image, when encoded, ought to have no connection between the nearby pixels. The




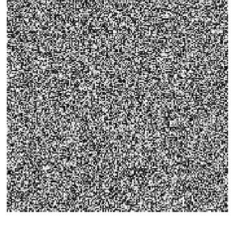
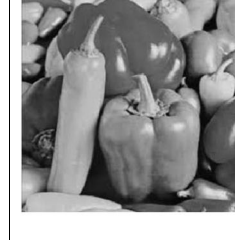

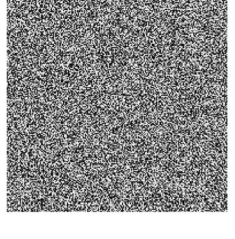
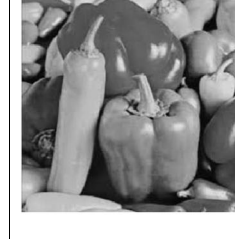

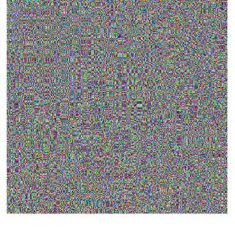
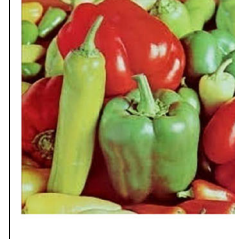

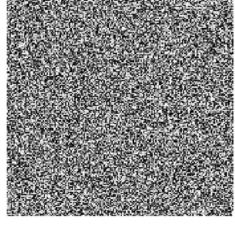
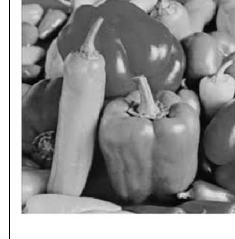
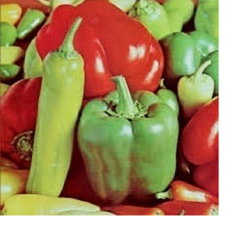
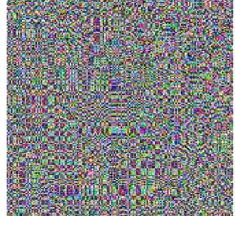

**Table 6** (continued)

<b>Proposed</b>			
<b>IMAGE SIZE (512*512)</b>			
<b>TECHNIQUE</b>	<b>ORIGINAL IMAGE</b>	<b>ENCRYPTED IMAGE</b>	<b>DECRYPTED IMAGE</b>
<b>Chaos 1 [9]</b>			
<b>Chaos 2 [23]</b>			
<b>Chaos 3 [24]</b>			

relationship coefficients go between - 1 and 1, where the boundaries demonstrate an ideal negative or positive direct connection separately.

For good encryption, the encrypted image must have very little correlation among adjacent pixels in all three directions. Table 8 and Figs. 12, 13 and 14 shows the tabular and graphical comparison of correlation in all three directions for image size 256\*256 and 512\*512 for different techniques available in the literature. The proposed technique depicts very less correlation among the adjacent pixels. This is achieved due to the bit plane scrambling confusion process at inter and intra bit plane levels.





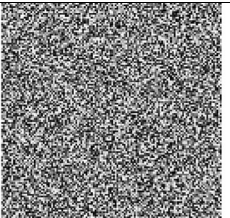


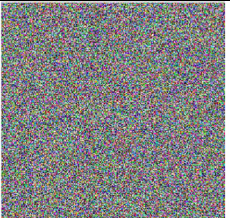

Table 6 (continued)

<b>Chaos 4 [27]</b>			
<b>Chaos 5 [10]</b>			
<b>Quantum Chaos 1 [3]</b>			
<b>Quantum Chaos 2 [1]</b>			
<b>Quantum Chaos 3 [14]</b>			

The proposed technique depicts very less correlation among the adjacent pixels in all the three directions as depicted in Figs. 12, 13 and 14 and Table 8. This is achieved due to the bit plane scrambling confusion process at inter and intra bit plane levels.



**Table 6** (continued)

<p><b>Quantum Chaos 4 [28]</b></p>			
<p><b>Quantum Chaos 5 [15]</b></p>			
<p><b>Proposed</b></p>			

- **Differential Analysis**

**NPCR:**

**Number of pixel change ratio [26]** implies the rate of change in the number of pixels when the original and a pixel altered plain-image are encoded first and then compared. A slight change in key and original image should result in a completely different encrypted image. The impact of one-pixel change is analyzed by NPCR and UACI [26].

Table 9 shows the theoretical results of NPCR related to image size of 256\*256 and proposed NPCR values. The techniques, quantum 4 and quantum 5 does not pass even single-level NPCR test which are based on the qubit, whereas the proposed technique passes the entire NPCR level tests. This shows that the proposed technique is sensitive to small changes and has great resistance power towards differential attack. This is due to the fact that our proposed technique is key dependent at each level of encryption process.

The pass or fail status in test depends on the reported values of the techniques. If the reported value is greater than the theoretical value or the critical value at each level, then that technique passes the NPCR test.

- **UACI (Unified Average Change in Intensity):**

**Unified Average Change in Intensity [26]** is the difference in average intensity between the plain and encrypted images. Table 10 shows the theoretical results of UACI related to 256\*256

**Table 7** Histogram analysis of Original and Encrypted Image

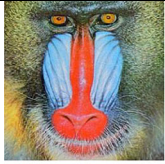
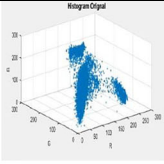

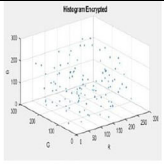
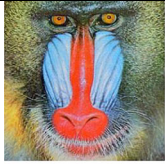
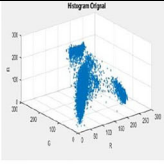

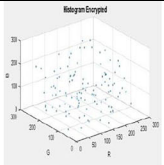
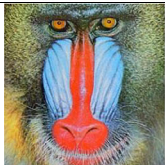
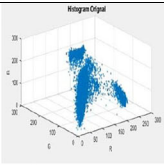

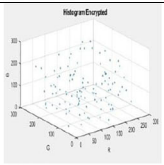
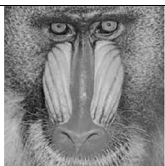
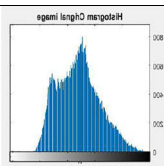
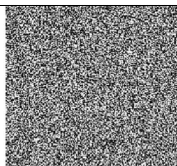
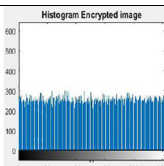
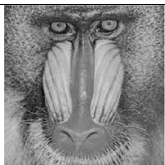
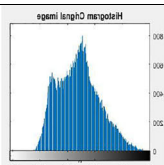
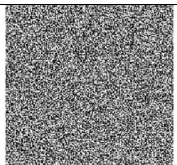
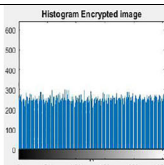
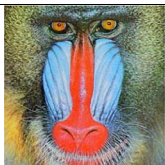
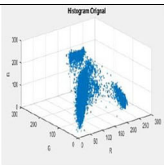
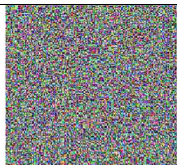
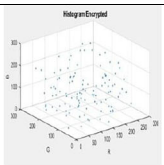
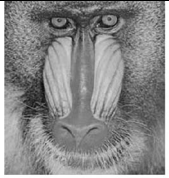
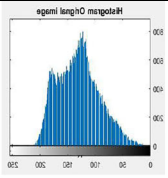
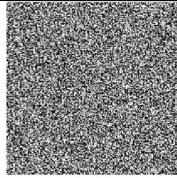
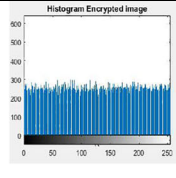
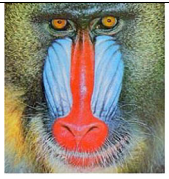
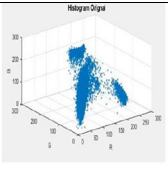

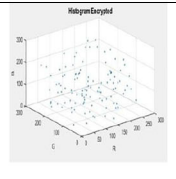
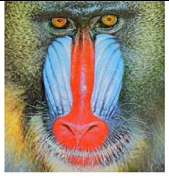
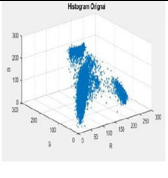

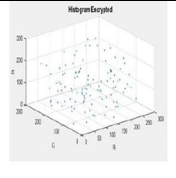
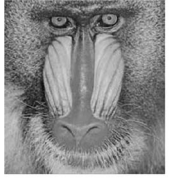
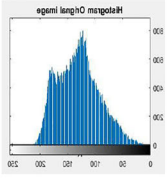
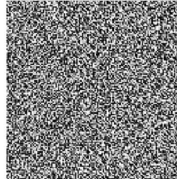
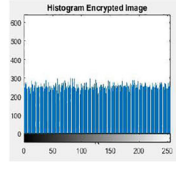
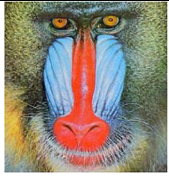
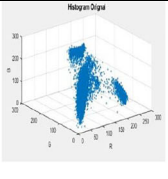

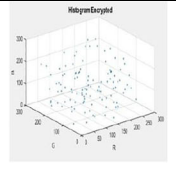
IMAGE SIZE (256*256)				
TECHNIQUE	ORIGINAL IMAGE	HISTOGRAM ORIGINAL IMAGE	ENCRYPTED IMAGE	HISTOGRAM ENCRYPTED IMAGE
<b>Chaos 1 [6]</b>				
<b>Chaos 2 [3]</b>				
<b>Chaos 3 [1]</b>				
<b>Chaos 4 [14]</b>				
<b>Chaos 5 [28]</b>				
<b>Quantum Chaos 1 [20]</b>				


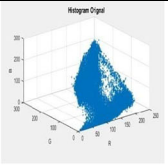
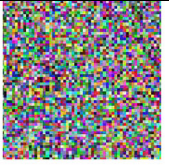
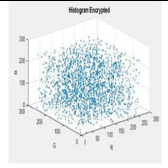

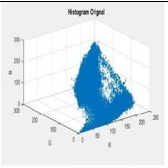
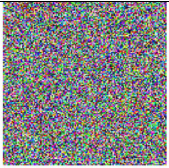
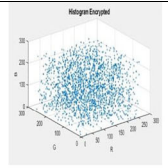

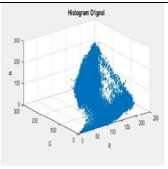
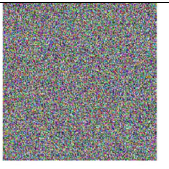
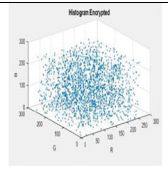

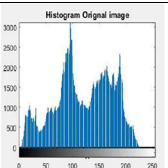
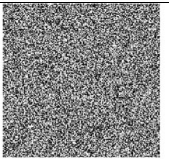
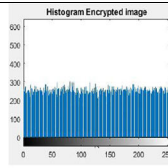

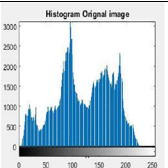
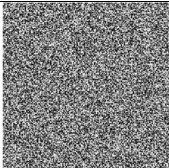
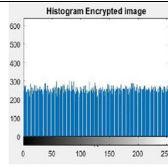

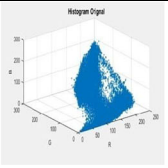
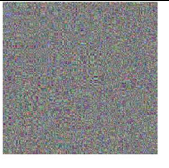
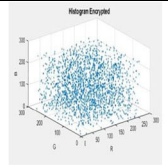
Table 7 (continued)

<p><b>Quantum Chaos 2 [26]</b></p>		<p>egeni langhC meqoleH</p> 		<p>Histogram Encrypted Image</p> 
<p><b>Quantum Chaos 3 [11]</b></p>		<p>Hologen Digma</p> 		<p>Hologen Digma</p> 
<p><b>Quantum Chaos 4 [4]</b></p>		<p>Hologen Digma</p> 		<p>Hologen Digma</p> 
<p><b>Quantum Chaos 5 [25]</b></p>		<p>egeni langhC meqoleH</p> 		<p>Histogram Encrypted Image</p> 
<p><b>Proposed</b></p>		<p>Hologen Digma</p> 		<p>Hologen Digma</p> 
<p><b>IMAGE SIZE (512*512)</b></p>				
<p><b>TECHNIQUE</b></p>	<p><b>ORIGINAL IMAGE</b></p>	<p><b>HISTOGRAM ORIGINAL IMAGE</b></p>	<p><b>ENCRYPTED IMAGE</b></p>	<p><b>DECRYPTED IMAGE</b></p>

size of image and proposed UACI values. The results illustrate that the proposed scheme provides the readings of UACI lie in the range of theoretical values [26]. This shows that the proposed technique is sensitive to small changes and has great resistance power towards differential attack. This is due to the fact that proposed technique is key dependent at each level of encryption process.



**Table 7** (continued)

<b>Chaos 1 [6]</b>				
<b>Chaos 2 [3]</b>				
<b>Chaos 3 [1]</b>				
<b>Chaos 4 [14]</b>				
<b>Chaos 5 [28]</b>				
<b>Quantum Chaos 1 [20]</b>				


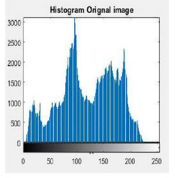
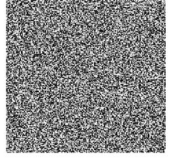
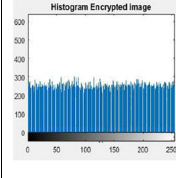
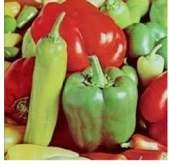
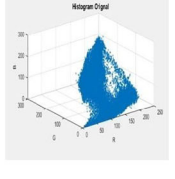

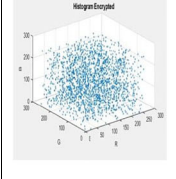

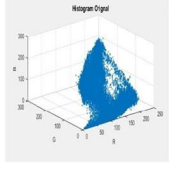
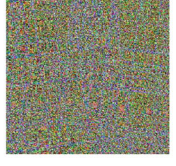
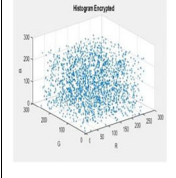

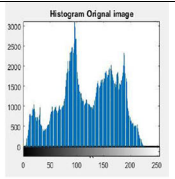
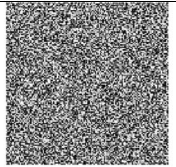
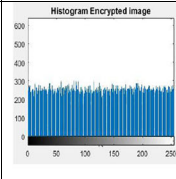
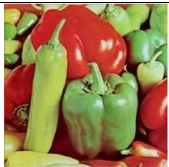
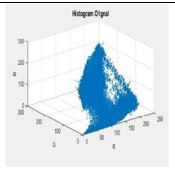
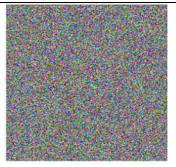
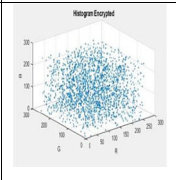
The pass or fail status of test depends on the reported values of the techniques. If the reported value is in between the upper and lower theoretical ranges or the critical value for each level, then that technique passes the UACI test.

- **Quantitative Analysis:**

**PSNR (Peak Signal to Noise Ratio):**

**Peak Signal to Noise Ratio** is the proportion between the most extreme power part of the signal and the noise present in it. By and large, a logarithmic decibel scale is utilized to portray

Table 7 (continued)

<p><b>Quantum Chaos 2 [26]</b></p>		<p>Histogram Original image</p> 		<p>Histogram Encrypted image</p> 
<p><b>Quantum Chaos 3 [11]</b></p>		<p>Histogram Original</p> 		<p>Histogram Encrypted</p> 
<p><b>Quantum Chaos 4 [4]</b></p>		<p>Histogram Original</p> 		<p>Histogram Encrypted</p> 
<p><b>Quantum Chaos 5 [25]</b></p>		<p>Histogram Original image</p> 		<p>Histogram Encrypted image</p> 
<p><b>Proposed</b></p>		<p>Histogram Original</p> 		<p>Histogram Encrypted</p> 

PSNR, as this sort of scaling can be utilized for a compact representation of a wide range of signal.

The Figs. 15 and 16 shows the MSE and PSNR for two different sizes of images for diverse renowned mechanisms. MSE is inversely proportional to PSNR. The proposed scheme shows the competent results in comparison to available techniques in literature.

- **Entropy:**

Figure 17 and Table 11 shows the graphical and numerical representation of entropy between encrypted and original image of different sizes. Entropy defines the randomness in the encrypted image. If image is completely randomized then the maximum value of entropy is revealed, which is 8. The proposed scheme shows entropy very close to ideal value i.e. 8 and hence can resist entropy attacks. This is due to the fact that the proposed technique uses inter

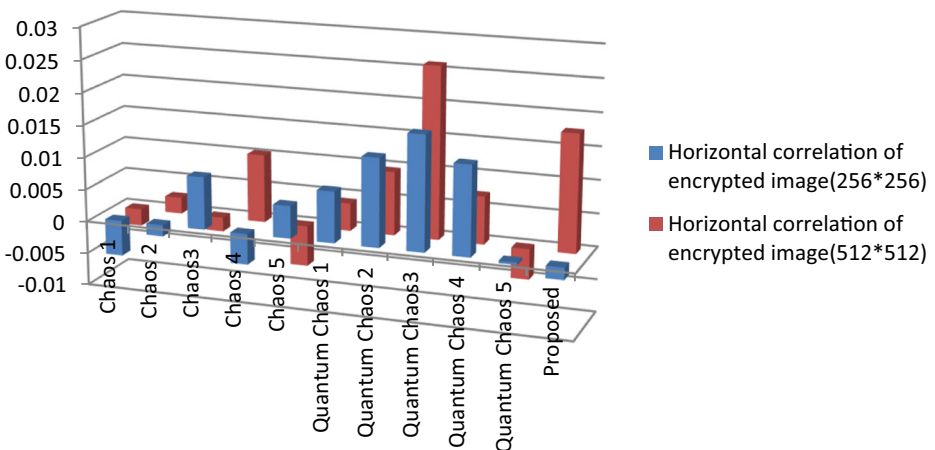
**Table 8** Comparison of correlation in all three directions for image size 256\*256 and 512\*512 for different techniques available in the literature

Size/ Techniques	256*256			512*512		
	Horizontal correlation	Vertical correlation	Diagonal correlation	Horizontal correlation	Vertical correlation	Diagonal correlation
Original Image	0.972303	0.971089	0.948257	0.990105	0.990105	0.977029
Chaos 1	-0.0055	-0.00137	-0.00181	-0.00262	0.001488	-0.00027
Chaos 2	-0.00175	-0.00681	0.000871	0.002496	-0.00163	-0.00315
Chaos3	0.00807	0.002598	0.002347	-0.00217	0.00275	-0.00078
Chaos 4	-0.00473	0.010352	-0.00747	0.010378	-0.00751	-0.00821
Chaos 5	0.005009	0.002751	0.002599	-0.00622	0.005434	-0.00227
Quantum Chaos 1	0.007849	-0.01281	-0.0035	0.004218	0.021133	0.002904
Quantum Chaos 2	0.013478	0.017343	0.009672	0.009622	0.015738	0.010788
Quantum Chaos3	0.017503	0.014874	0.001998	0.026076	0.026385	0.017633
Quantum Chaos 4	0.013705	0.049741	0.04845	0.007254	0.006084	0.022441
Quantum Chaos 5	-3.42E-04	-0.00895	0.005192	-0.00463	5.09E-04	0.015891
Proposed	-0.00656	0.000935	-0.00718	0.000685	-0.00417	-0.00241

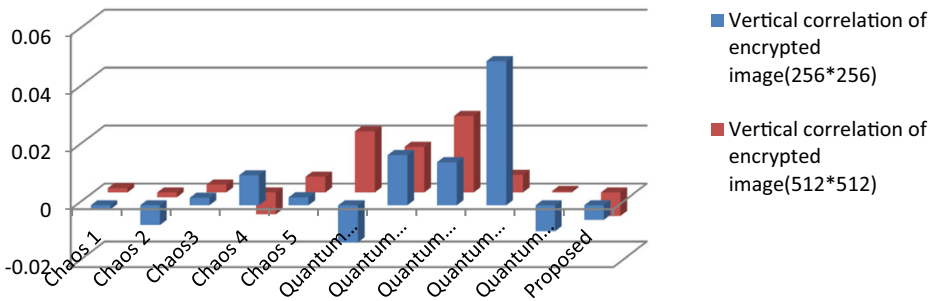
and intra bit plane confusion process and dynamic number of iterations. Entropy is at par with other techniques given in literature.

• **Speed of Execution:**

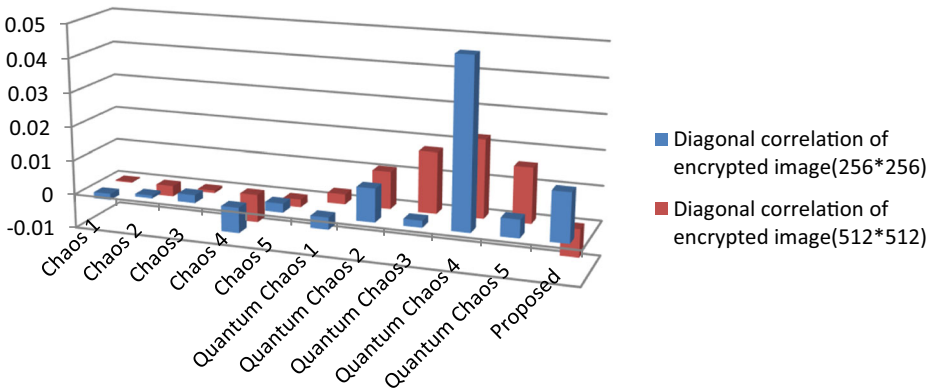
Table 12 shows the speed of execution of encryption mechanisms for two different image sizes. The speed of encryption/ decryption is also an important factor that depends on memory



**Fig. 12** Graph depicting Horizontal correlation graphs respectively compared with the chaos and quantum chaos techniques for 256\*256 and 512\*512 images



**Fig. 13** Graph depicting Vertical correlation graphs respectively compared with the chaos and quantum chaos techniques for 256\*256 and 512\*512 images



**Fig. 14** Graph depicting Diagonal correlation graphs respectively compared with the chaos and quantum chaos techniques for 256\*256 and 512\*512 images

**Table 9** NPCR Test Table

IMAGE	REPORTED VALUES	THEORETICAL NPCR CRITICAL VALUE		
		0.05 level	0.01 level	0.001 level
256*256		$N^*_{0.05} = 99.5693\%$	$N^*_{0.01} = 99.5527\%$	$N^*_{0.001} = 99.5341\%$
TECHNIQUES	REPORTED VALUES	0.05 level	0.01 level	0.001 level
Chaos 1 [9]	99.628194%	Pass	Pass	Pass
Chaos 2 [23]	99.568176%	Pass	Pass	Pass
Chaos 3 [24]	99.61344%	Pass	Pass	Pass
Chaos 4 [27]	99.594416%	Pass	Pass	Pass
Chaos 5 [10]	99.624633%	Pass	Pass	Pass
Quantum Chaos 1 [3]	99.5513%	Pass	Pass	Pass
Quantum Chaos 2 [1]	99.612426%	Pass	Pass	Pass
Quantum Chaos 3 [14]	99.59971%	Pass	Pass	Pass
Quantum Chaos 4 [28]	51.2329%	Fail	Fail	Fail
Quantum Chaos 5 [15]	50.2025%	Fail	Fail	Fail
Proposed	99.611218%	Pass	Pass	Pass



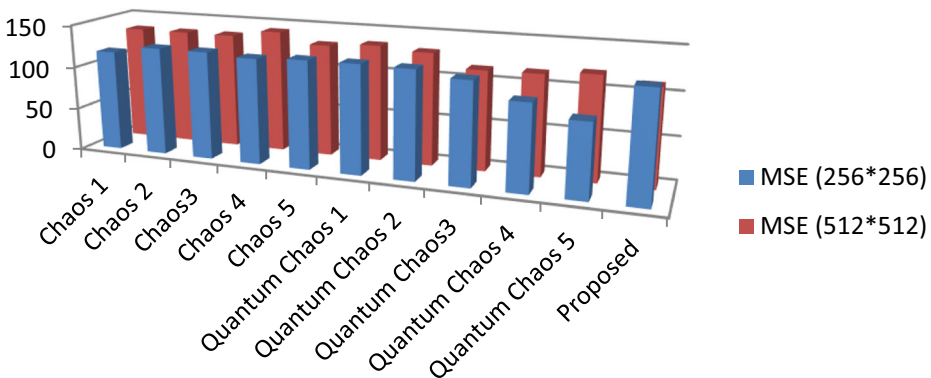
**Table 10** UACI Test Table

IMAGE		THEORETICAL UACI CRITICAL VALUE		
256*256		$U^*_{-0.05} = 33.284\%$	$U^*_{-0.01} = 33.2255\%$	$U^*_{-0.001} = 33.1594\%$
		$U^{*+}_{0.05} = 33.6447\%$	$U^{*+}_{0.01} = 33.7016\%$	$U^{*+}_{0.001} = 3.7677\%$
TECHNIQUES	REPORTED VALUES	0.05 level	0.01 level	0.001 level
Chaos 1 [9]	33.4688%	Pass	Pass	Pass
Chaos 2 [23]	33.4713%	Pass	Pass	Pass
Chaos 3 [24]	33.4598%	Pass	Pass	Pass
Chaos 4 [27]	33.4783%	Pass	Pass	Pass
Chaos 5 [10]	33.5468%	Pass	Pass	Pass
Quantum Chaos 1 [3]	33.4612%	Pass	Pass	Pass
Quantum Chaos 2 [1]	33.5012%	Pass	Pass	Pass
Quantum Chaos 3 [14]	33.5638%	Pass	Pass	Pass
Quantum Chaos 4 [28]	33.4674%	Pass	Pass	Pass
Quantum Chaos 5 [15]	25.0907%	Fail	Fail	Fail
Proposed	33.4942%	Pass	Pass	Pass

size, CPU structure, Operating system and many more. Hence, it is not comparable until the time execution is done using the same environment. From results, it is seen that the proposed scheme shows very less speed of execution in comparison to the most of techniques available in literature. This is achieved due to the implementation of matching process in the encryption process of the proposed technique. Still, further improvements can be done to decrease this factor.

• **Key Space Analysis:**

Key-space investigation is a significant parameter characterizing the possibility of an encryption plan to withstand a brute force attack [10, 24, 27]. To do this, the key size used for encryption must be a large combination of key spacing. This is important for resisting the brute force attack. Ideally, key space must be greater than 2100 for resisting brute force attacks with



**Fig. 15** Graph comparing MSE values of proposed technique with the chaos and quantum chaos techniques for 256\*256 and 512\*512 images

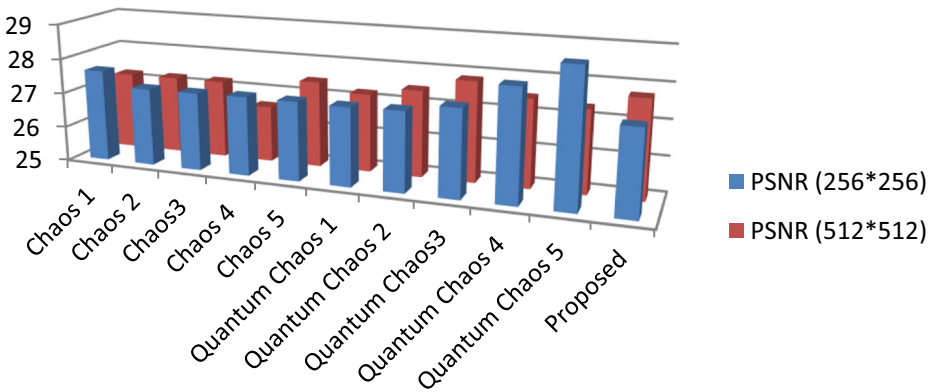


Fig. 16 Graph comparing PSNR values of proposed technique with the chaos and quantum chaos techniques for 256\*256 and 512\*512 images

the current computational ability of computers. As described in Simulation setup parameters the key space is  $2^{432}$ , which is greater than the ideal key space. Hence, the proposed scheme has a large enough key space for the secured transmission of images. Key space of different encryption techniques is shown in Table 13.

- **Cryptanalysis:**

The cryptanalysis attack [17] is the most important attack to validate encryption technique in terms of security. The most well known cryptanalysis attack are chosen plaintext attack and known plaintext attack. The chosen plaintext attack is the most intimidating attack. It is known that encryption scheme can resist all other attacks if it can resist the chosen plain text attack. Similar to other renowned techniques available in literature, proposed technique has the ability to resist chosen plain text as well as known plaintext attack. This resistance is developed due to its dependency on the original image and key generation using quantum chaotic map.

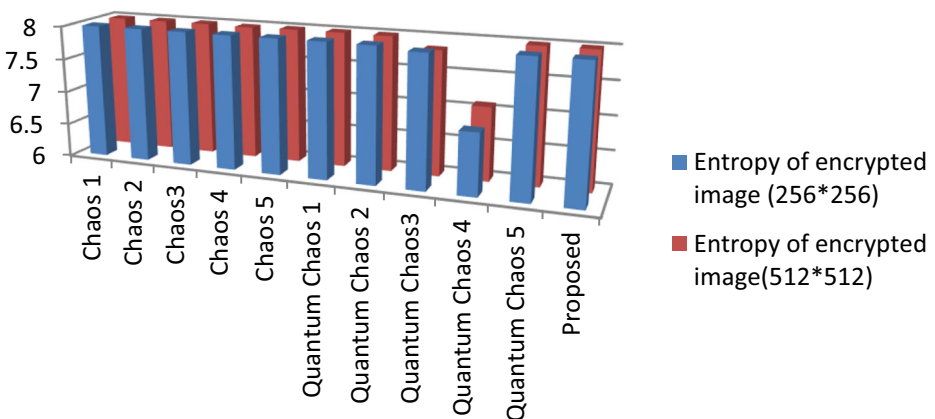


Fig. 17 Graph depicting Entropy values of proposed and different techniques of different size

**Table 11** Entropy of encrypted image for the proposed technique in comparison to other techniques available in literature

IMAGE (SIZE)	256*256	512*512
Chaos 1 [9]	7.998921	7.999762
Chaos 2 [23]	7.998924	7.999738
Chaos 3 [24]	7.999067	7.999759
Chaos 4 [27]	7.996967	7.989875
Chaos 5 [10]	7.997338	7.999302
Quantum Chaos 1 [3]	7.999021	7.999747
Quantum Chaos 2 [1]	7.993819	7.997016
Quantum Chaos 3 [14]	7.946061	7.843878
Quantum Chaos 4 [28]	6.917573	7.090036988161511
Quantum Chaos 5 [15]	7.997679	7.999341
Proposed	7.999009	7.9997583

## 7 Overall comparison

The proposed technique has enhanced results as requisite for a good encryption mechanism, as illustrated in the Table 14. The overall comparison of the diverse renowned mechanisms with the proposed technique is prepared in terms of various parameters such as image perceptual quality, UACI, NPCR, Key space, Key space analysis, Randomness, Speed of Execution, Known plaintext attack and Chosen plaintext attack.

## 8 Overall conclusions

The proposed mechanism utilizes quantum chaotic map for key generation to be used in different processes like generation of ECB, eight direction Folding and number of iterations used in overall methodologies. All the encryption stages and also the number of iterations are key dependent. The image to be encrypted is firstly confused using ECB, IP and Inter-intra bit scrambling. The confused image is diffused in next stage which includes folding process in eight directions and the number of folds for each direction depends on key values. After analyzing the results following conclusions are inferred:

**Table 12** Speed of execution of encryption for two different image sizes

Techniques	Speed of execution (256*256)	Speed of execution (512*512)
Chaos 1 [9]	119.2545	398.1214
Chaos 2 [23]	296.8307	1177.595
Chaos 3 [24]	721.2118	2243.863
Chaos 4 [27]	43.99586	64.3276
Chaos 5 [10]	1.557594	2.9874
Quantum Chaos 1 [3]	4.140006	7.4325
Quantum Chaos 2 [1]	5.552956	7.3254
Quantum Chaos 3 [14]	13.40669	17.5632
Quantum Chaos 4 [28]	206.47029	1767.316
Quantum Chaos 5 [15]	570.4578	2232.421
Proposed	3.654171	6.839909

**Table 13** Key space analysis of various techniques available in literature

Techniques	Key Space
Chaos 1 [9]	$2^{462}$
Chaos 2 [23]	$2^{192}$
Chaos 3 [24]	$2^{192} \text{--} 2^{216}$
Chaos 4 [27]	$10^{42}$
Chaos 5 [10]	$2^{384}$
Quantum Chaos 1 [3]	$2^{72}$
Quantum Chaos 2 [1]	$2^{256}$
Quantum Chaos 3 [14]	$2^{128}$
Quantum Chaos 4 [28]	$10^{72}$
Quantum Chaos 5 [15]	$>2^{100}$
Proposed	$2^{432}$

- This technique works on bit planes rather than working on bytes, which increases the entropy and randomness in the encrypted image.
- The entropy of the proposed techniques is close to 7.999 but still can be improved further.
- Due to the dependency on the original image and key generation using quantum chaotic map, proposed technique can efficiently resist chosen plaintext attack and known plaintext attack.
- Usage of the multilevel matching process in the confusion process requires less time for execution. This decreases the speed of execution and hence can be used in wide applications.
- The speed of execution of the proposed technique is less than almost all the techniques available in the literature. But it is greater than Chaos 5 technique. As this parameter is dependent on the number of iterations of the process. In proposed technique it is variable, as it is dependent on the key value. This feature makes projected mechanism more protected in comparison to others.
- In proposed technique the key size can be increased up to  $2^{432}$  which can achieve a vast range of key space. Hence, it can resist brute force attack resulting in extremely secure transmission of data.
- The proposed technique passes all the test levels of NPCR and UACI and hence turns out to be resistant towards differential attacks.

**Table 14** Overall Comparison of techniques available in literature with the proposed technique

Paper Reference	IPQ	UACI/NPCR	KS	KSA	RA	SOE	KPA	CPA
[9]	Low	Pass	High	High	High	Slow	Can resist	Can resist
[23]	High	Pass	High	High	High	Slow	Can resist	Can resist
[24]	High	Pass	High	High	High	Slow	Can resist	Can resist
[27]	High	Pass	High	High	High	Moderate	Can resist	Can resist
[10]	High	Pass	High	High	High	High	Can resist	Can resist
[3]	High	Pass	Moderate	High	High	High	Can resist	Can resist
[1]	High	Pass	High	High	High	High	Can resist	Can resist
[14]	Low	Pass	High	High	High	Moderate	Can resist	Can resist
[28]	High	Fail(NPCR)	Moderate	High	Moderate	Slow	Can resist	Can resist
[15]	High	Fail	High	High	High	Slow	Can resist	Can resist
Proposed	High	Pass	Very High	Very High	High	High	Can resist	Can resist

- Our results such as: differential attack, cryptanalysis, key space analysis, image perceptual quality, key sensitivity analysis are reasonably improved than others while entropy, correlation and speed of execution are at par with other techniques given in literature.

The proposed mechanism has enhanced outcomes as required for a superlative encryption mechanism.

## Compliance with ethical standards

**Conflict of interest** Author Manju Kumari declares that she has no conflict of interest. Author Shailender Gupta declares that he has no conflict of interest. Author Anjali Malik declares that she has no conflict of interest.

## References

1. Abd El-Latif AA, Li L, Wang N, Han Q, Niu X (2013) A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process* 93(11):2986–3000
2. Ahmed HEDH, Kalash HM, Allah OF (2007) Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images. In *2007 International Conference on Electrical Engineering*. IEEE, p 1–7
3. Akhshani A, Akhavan A, Lim SC, Hassan Z (2012) An image encryption scheme based on quantum logistic map. *Commun Nonlinear Sci Numer Simul* 17(12):4653–4661
4. Akhshani A, Akhavan A, Mobaraki A, Lim SC, Hassan Z (2014) Pseudo random number generator based on quantum chaotic map. *Commun Nonlinear Sci Numer Simul* 19(1):101–111
5. Anderson TW (1958) *An introduction to multivariate statistical analysis*. Wiley, New York
6. Bansal R, Gupta S, Sharma G (2017) An innovative image encryption scheme based on chaotic map and Vigenère scheme. *Multimed Tools Appl* 76(15):16529–16562
7. Barker E, Mouha N (2017) Recommendation for the triple data encryption algorithm (TDEA) block cipher (no. NIST special publication (SP) 800-67 rev. 2 (draft)). National Institute of Standards and Technology
8. Basu S (2011) International data encryption algorithm (idea)—a typical illustration. *J Global Res Com Sci* 2(7):116–118
9. François M, Grosjes T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. *Signal Process Image Commun* 27(3):249–259
10. Hanchinamani G, Kulkarni L (2015) An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher. *3D Res* 6(3):30
11. Jin C, Liu H (2017) A color image encryption scheme based on Arnold scrambling and quantum chaotic. *IJ Network Security* 19(3):347–357
12. Kester QA (2013) A hybrid cryptosystem based on Vigenere cipher and columnar transposition cipher. *arXiv preprint arXiv:1307.7786*
13. Kumari M, Gupta S (2018) A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. *3D Res* 9(1):10
14. Liu H, Jin C (2017) A novel color image encryption algorithm based on quantum chaos sequence. *3D Res* 8(1):4
15. Liu X, Xiao D, Xiang Y (2018) Quantum image encryption using intra and inter bit permutation based on logistic map. *IEEE Access* 7:6937–6946
16. Mandal S, Das S, Nath A (2014) Data hiding and retrieval using visual cryptography. *Int J Innov Res Adv Eng* 1:102–110
17. Matsui M (1994). The first experimental cryptanalysis of the data encryption standard. In *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg p 1–11
18. Matthews R (1989) On the derivation of a “chaotic” encryption algorithm. *Cryptologia* 13(1):29–42
19. Mousa A, Hamad A (2006) Evaluation of the RC4 algorithm for data encryption. *IJCSA* 3(2):44–56
20. Ran Q, Yuan L, Zhao T (2015) Image encryption based on nonseparable fractional Fourier transform and chaotic map. *Opt Commun* 348:43–49
21. Rayarikar R, Upadhyay S, Pimpale P (2012) SMS encryption using AES algorithm on android. *Int J Comput Appl* 50(19):12–17

22. Rivest RL (1994) The RC5 encryption algorithm. In International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, p 86–96
23. Sam IS, Devaraj P, Bhuvaneshwaran RS (2012) A novel image cipher based on mixed transformed logistic maps. *Multimed Tools Appl* 56(2):315–330
24. Sam IS, Devaraj P, Bhuvaneshwaran RS (2012) An intertwining chaotic maps based image encryption scheme. *Nonlinear Dynamics* 69(4):1995–2007
25. Schneier B (1994) The blowfish encryption algorithm. *Dr Dobb's Journal-Software Tools for the Professional Programmer* 19(4):38–43
26. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* 1(2):31–38
27. Ye G, Pan C, Huang X, Zhao Z, He J (2018) A chaotic image encryption algorithm based on information entropy. *Int J Bifurcation Chaos* 28(01):1850010
28. Zhou N, Chen W, Yan X, Wang Y (2018) Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quantum Inf Process* 17(6):137

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## Affiliations

Manju Kumari<sup>1</sup> · Shailender Gupta<sup>1</sup> · Anjali Malik<sup>1</sup>

Manju Kumari  
manjunimesh88@gmail.com

Shailender Gupta  
shailender81@gmail.com

<sup>1</sup> J C Bose University of Science and Technology, YMCA, Faridabad, Haryana, India