Multimedia Tools and Applications
https://doi.org/10.1007/s11042-022-13244-w

Quantum based robust and swift hybrid security mechanism

Sangeeta Dhall[1] · Shailender Gupta[1]

Received: 22 January 2021 / Revised: 16 May 2021 / Accepted: 16 May 2022

Abstract
Intact communication of covert information is the key requirement of all the applications like medical, military, business transactions. For that matter need for a proficient security mechanism is apparent. This paper proposes a hybrid design containing Quantum based confusion and diffusion processes followed by Lifting Wavelet Transform (LWT) steganography mechanism. Moreover, a provisional compression mechanism is also employed. Secret data is initially checked for the frequency of characters, which is the decisive factor for the inclusion of compression operation. This data undergoes a bit-level confusion stage, with the help of a random key generated by Quantum based key scheduling algorithm. The subsequent process is diffusion, in which each perplexed bit undergoes XOR operation with random keys generated by a centralized key generation mechanism. Finally, this data is embedded into the Lifting Wavelet Transformed cover image. The mingled data bits are stored at random locations of carrier Image, ready to commune in an insecure site. The usage of simple and effective stages provides time efficiency, robustness, and power of confidentiality predominantly in a highly effective way compared to the available mechanism. Implementation using MATLAB shows that secret information is highly secure.

Keywords Compression · Confusion · Diffusion · Key scheduling algorithm · Lifting wavelet transform (LWT) · Quantum · Steganography

✉ Sangeeta Dhall
sangeeta_dhall@yahoo.co.in

Shailender Gupta
shailender81@gmail.com

[1] J.C.Bose University of Science and Technology, YMCA, Faridabad, India

Published online: 27 May 2022

1 Introduction

The need to communicate records, text, images, and other information is the mandatory action required in almost all the application areas. In the medical field, Electronic Patient Records are required to be stored and shared with health care workers, doctors, and patients [22]. In military and other defense fields' communication of secret messages amongst different units in a limited period and with high confidentiality and robustness are the primary concerns [30]. In business dealings, diverse digital transactions are the standard requirements. On similar lines, many others areas have similar needs. Consequently, it is crucial to protect all types of information to avoid exploitation or contravention.

Amongst existing solutions most admired are cryptography and steganography [9, 19]. Former converts secret information into the unreadable form for the intruders and later hides the private data in some carrier to not be perceived by an intermediary. However, a single layer of security is not sufficient for the protection of vital records; hence multiple stratums are employed to attain requisite enhanced safety [7]. Though copious hybrid mechanisms are available in the literature, with escalating security threats, the need for further enhanced multilevel protection algorithms for given objectives is always there in the practical scenario. Researchers in the literature have been proposed an assortment of hybrid schemes. [7] Concerning security, the requirements of the different fields and sectors include confidentiality, robustness, high speed of execution, imperceptibility, and complete reproducibility of data.

In this paper, to fulfill these protection issues in diverse applications, a hybrid secure, robust, and fast, authentic mechanism is proposed to secure secret records. This proposal has incorporated Quantum based key scheduling algorithm, which is used to generate keys for different stages of the given scheme like confusion, diffusion, and steganography. The key generation algorithm uses Quantum logistic maps for the generation of keys. This map has chosen because of its features of high randomness and sensitivity towards initial keys. Information to be secured is initially checked for its randomness or frequency of available characters, so that decision on the compression stage can be taken. If the frequency of character is higher than the threshold, then data is compressed using the Huffman algorithm; otherwise, without this process, move towards the next stage, which is bit-level confusion. This process is undergone using a random array generated with the help of seed taken from randomly generated keys by the centralized algorithm. This confused data is then diffused using simple XOR operation of each bit with a separate key generated centrally. This highly random resultant information is then embedded into the cover image. For embedding, the carrier image is processed by transforming into the frequency domain. Lifting wavelet frequency transformation is chosen because of its simplicity and lossless recovery. The resultant secret data is stored in random locations of one of the bands of LWT transformed Image. These random locations are also chosen from random keys generated centrally. This proposal is designed with the following objectives;

- High Robustness,
- High confidentiality,
- High perceptibility of stego Image,
- High Randomness,
- High speed of execution and reproducibility,
- Complete Recovery of Information.

These objectives are justified in subsequent sections. The complete paper is organized as follows: Section 2 gives Literature Survey. The proposed mechanism is described in detail under Section 3. Section 4 provides the setup parameters. The complete analysis of results is done in Section 5, followed by an overall comparison. Section 6 gives the conclusion, which is followed by references.

2 Literature survey

The severity of security needs motivates researchers to put in lots of effort to propose highly protected security mechanisms to save the fragile information used in diverse sectors. In [21], the hybrid approach consists of cascading cryptography and steganography using the DES encryption, and LSB substitution steganography mechanism is employed. As per results for better imperceptibility, the proposed method provides a high correspondence between the cover and stego images. The twofold layer of security was proposed by [5]. The first layer constitutes RC4 cryptography, followed by the second layer of LSB substitution steganography. This scheme features high embedding capacity, but the spatial domain steganography technique lowers reliability for signal processing attacks. [18], proposed a versatile technique to provide improved protection for confidential data. In this RC4cryptography and modified pseudorandom steganography are used, in which an adaptive method is employed, and this scheme is, in turn, depends on the size of secret data for random pixel selection in order to store data. In [14], dual-layer security is provided by using AES cryptography for changing the secret data into cipher followed by a new Steganography technique to hide large data in the cover image. This new method uses the idea of status checking for embedding and retrieval of information. In [17], three different types of encryption are proposed. Watermark is embedded in selective DWT co-efficient of medical image. This resultant image is encrypted before communication. In [26], medical image watermarking along with encryption is proposed. For encryption, the RSA scheme is employed, inserted into the DWT co-efficient of the cover image. Region of Interest (ROI) is recognized before embedding. [25] proposed a twofold watermarking technique. Duality is accomplished by inserting a secret record and image watermark in the cover medical image. In order to enhance the robustness of the watermark, four diverse error correction codes are employed. However, here, EPR and Medical Image are embedded in a single cover image, which results in reduced PSNR. [23], introduced a novel secure mechanism based on the Visual Cryptography (VC) scheme. In this proposal, a protected share creation mechanism is produced by XOR based VC scheme, in which after the formation of shares, these are encrypted separately using Advanced Encryption Standard (AES) cryptography. As the shares and AES algorithm attach collectively to give the resultant shares, thus these are termed as the encapsulated shares. In [29], a manifold security mechanism is employed in which, firstly, stego image is partitioned on the color plane basis, then Discrete Wavelet Transform (DWT) steganography is applied on each plane. This step is followed by embedding secret data using Improved Bit Plane Complexity Segmentation (IBPCS) steganography, and finally, Inverse DWT (IDWT) is performed to form a stego image. Thus, it consists of both frequency and spatial domain steganography mechanisms. [6] proposed a manifold security mechanism using visual cryptography (VC) followed by Status LSB substitution steganography. The secret data is initially compressed using Huffman lossless encoding scheme and then encrypted using VC, and finally, this altered information is inserted in the status bit evaluated LSB substitution steganography mechanism. This scheme

has a high time of execution with low Randomness. In [28], hierarchical Visual Cryptography and Improved Bit Plane slicing scheme (IBPCS) steganography mechanism is implemented. Here Huffman encoding is an additional layer of security. This proposal provides good picture quality due to the usage of Status bit LSB. Also, embedding capacity is improved. [4] introduced a dual-layer image encryption mechanism based on chaotic maps and Vigenère Scheme. This proposal has one round consisting of two steps: diffusion and confusion. The diffusion step consists of three stages: forward diffusion, a matching process using the Vigenère scheme, and backward diffusion. In the confusion stage, location permutation using a chaotic map is employed to swap pixel positions. In ([24] a) combination of DCT and DWT is proposed for embedding. RSA and MD5 are employed for enhancing the level of security. Besides, Hamming error correction code technique is used for declining BER. [3] has proposed a technique based on the matching of bit pairs. In this, pixel bits of the cover image and the information to be embedded, i.e., watermark image, are arranged in pairs, and then after comparison of pairs, replacement of bit pairs takes place with the respective matched pair. Here, before insertion watermark image undergoes symmetric key encryption for enhancing security. In [10], the projected model is formed through the amalgamation of either 2-D discrete wavelet transform 1 level (2D-DWT-1 L) or 2-D discrete wavelet transform 2 levels (2D-DWT-2 L) steganography technique. It is a multi-layered security mechanism that encrypts the secret data and then inserts it in a frequency transformed cover image to form the final stego image. For encryption, confidential data is partitioned into even and odd parts, and then two separate cryptography mechanisms are employed; these are RSA and AES, respectively. [15] introduced the combination of Visual Cryptography (VC) and frequency domain DCT mechanism to provide improved protection for secret information for communication. The first stage is encryption of confidential data, by dividing it into shares using VC and then storing them into Discrete Cosine Transformed cover image to form a stego image. [7] proposed multi-level security mechanism by cascading Huffman compression and Quantum-based encryption mechanism, finally the modified output of stages is embedded in selected regions of the cover image. [27] proposed a multilayer security mechanism formed by AES encryption followed by XOR operation of encrypted information. This modified information is embedding in DCT transformed cover image. LSB replacement of DCT transformed pixel values is used. [16] projected a mechanism consisted of Huffman compression and hierarchical visual encryption of records to be protected. This altered information is then embedded into the selected band of DWT transformed cover image. In [11], Pixel Value Difference (PVD) based high capacity steganography is employed. This embedding process utilizes both high and low contrast pixels to store information, thus focusing on PSNR and embedding capacity. Before embedding secret message is encrypted using dynamic pairing function methodology. Table 1 shows a concise description of the coverage of major objectives by the diverse security mechanisms available in the literature.

As observed from Table 1, the study of available mechanisms reveals that each proposal is designed to optimize some of the objectives and has its pros and cons for fulfilling defined objectives. As mentioned above, for security, the requests of the diverse fields and sectors include confidentiality, robustness, high speed of execution, imperceptibility, and complete reproducibility of data. Also, some applications require significant embedding capacity, if the information to be protected is of considerable size [1]. Due to the availability of enormous cryptography and steganography mechanisms, multiple combinations can be produced as outcomes. Each researcher had tried groupings to get desired results in terms of the best values of defined parameters. As seen from Table 1, all the goals are still not satisfied by any

Table 1 Literature Survey

References	Imperceptibility	Confidentiality & Robustness	Speed of Execution	Randomness	Reproducibility
[21]	√				√
[5]	√	√		√	√
[18]	√	√			√
[17]	√	√	√		√
([26]	√	√			√
[14]	√	√			√
[23]		√	√		√
[25]	√	√			√
[6]	√	√	√		√
[29]	√	√		√	√
[29]	√	√	√		√
[4]	√	√	√	√	
[24]	√	√			√
[10]	√	√			√
[15]		√	√		
[3]	√	√			√
[7]	√	√		√	√
[27]	√	√			√
[16]	√	√	√		√
[11]	√	√			√
[22]	√	√			√
[8]	√	√			√

single proposal. The motivation behind this work is to optimize all mentioned goals. For that rationale, the core contributions of the paper are:

- **Ensuring Imperceptibility:** This feature make certain that the hidden information shouldn't be visible to the third party. This is achieved by the selection of appropriate algorithms (LWT steganography) and frequency band for embedding sensitive information. Optimize results of PSNR and correlation coefficient confirms high imperceptibility.
- **Ensuring Confidentiality:** For inculcating this feature, multiple layers of security are used, to ensure that even if one layer is breached data should be protected by another one. These layers are formed by conditional compression, confusion, diffusion and finally steganography.
- **Ensuring Robustness:** For securing data in vulnerable channel exposed with probable attacks and noises information can be secured by hiding in such regions of cover image, which are not affected by revelation of unwanted alterations.
- **Ensuring High Speed:** Many applications are time restricted, that means need prompt data for further action. For reducing time of execution, very simple and effective processes are used and even one stage is conditional i.e. it will be used as per the want of data, to be secured.
- **Ensuring Randomness:** Encoding data in such a form which is unreadable for others can be performed by mingling it to great extent. This is introduced in proposal by using bit level confusion and diffusion processes by means of randomly generated keys using Quantum logistic maps.
- **Ensuring Reproducibility:** or data extraction is attained, by using all those algorithms at all the stages which are lossless, so that complete information is available for intended

user. In mechanism compression, confusion, diffusion and steganography, all are lossless and reversible to ensure desired data reception.

The next section gives the detail of the proposed hybrid model

3 The proposed model

A hybrid security model is proposed in this paper, which ensures the protection of the secret information used in varied applications in diverse apprehensive environments. The sender side process for the proposed model is described in Fig. 1, and hallmarks of the same are as under:

- Centralized Key Scheduling Algorithm.
- Conditional Compression
- Bit-Level Confusion
- Bit-Level Diffusion
- Frequency Domain Lifting Wavelet Transform

The subsequent section illustrates all the blocks of the proposed model, with the rationalization of the selection. Also, it is a reversible scheme; every stage can be reversed; thus, each stage is explained to demonstrate its both directions, sender side and receiver side function.

3.1 Key scheduling algorithm

For securing any information, it is required to protect it from varying facets. One of the aspects is the secret key used for the security algorithm. The proposed mechanism is a hybrid scheme consisting of different stages, and each step requires a unique key for implementation. For that matter, a centralized key scheduling algorithm is used for the generation of keys for all stages,

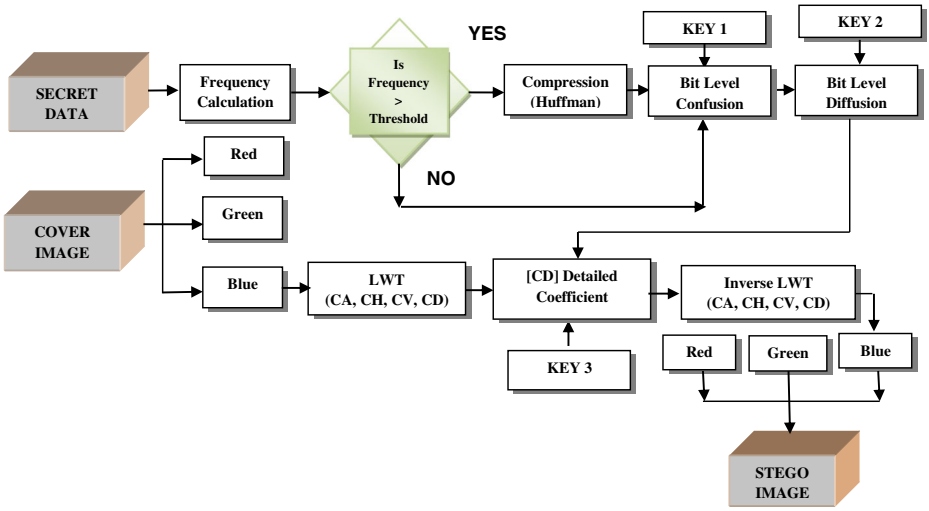


Fig. 1 The Proposed Model (Sender Side)

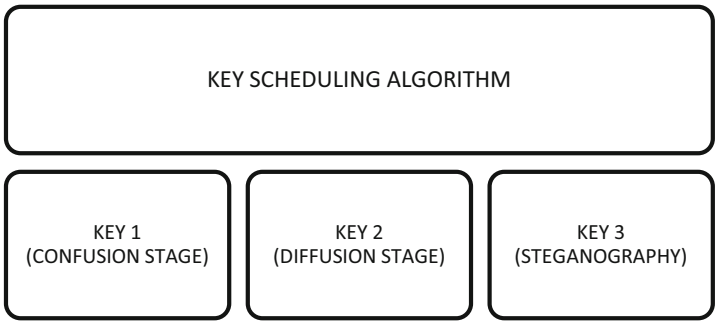


Fig. 2 Centralized Key Generation

as shown in Fig. 2. Secret keys are to be random and unique for every stage; that is why Quantum logistic Maps are employed.

Due to enormous advantages, as described in [19, 20], quantum logistic maps are chosen here. These desirable characteristics are listed below in Fig. 3:

Pseudo-code for key scheduling algorithm is described in Fig. 4, which generates keys for all the stages and have the characteristics of providing highly random keys.

All the keys generated in this section will be used in all the sections described below. Starting from the confusion stage. Before that, condition-based compression stage will appear.

3.2 Conditional compression

The initial action carried out in this work is the identification of the need for a compression algorithm. This is done by calculating the frequency of characters appearing in confidential data. If the available frequency is higher than a threshold value, which is taken as 2 in this implementation, then compression will be favourable for reducing the size of data for further processing; otherwise, it will proceed to the next stage without compression. This is because the Huffman compression algorithm works on the principle of encoding the characters as per their occurrences' in the data. If the frequency is high, then the small size of code will be assigned to the character, and inversely large size code will be given to low-frequency characters. This algorithm is chosen because of its significant advantage of being lossless, and the compression rate is very high [29]. Its compression rate varies from 30 to 50%, depending on the occurrence of the font in the information. The pseudo-code for the compression and decompression algorithms is described in Fig. 5.

Very High	• Sensitivity towards initial conditions
Very High	• key space
Very High	• Key sensitivity
Very High	• Entropy (Randomness)
Very Low	• Correlation coefficient
Very Low	• Execution Speed
High	• Resistance towards brute force search attacks

Fig. 3 Desirable Characteristics of Quantum Logistic Maps

ALGORITHM FOR KEY SCHEDULING ALGORITHM

INPUT: Initial Keys= a0, b0, c0, u, v, a_n and b_n; Secret Data Length =LENGTH(DATA);

OUTPUT: KEYS: key1, key2, key3.

STEP 1: INITIALIZE ALL INITIAL KEYS.

STEP 2: ITERATION OF FOLLOWING LOGISTIC MAP EQUATIONS 1000 TIMES, TO AVOID THE TRANSIENT EFFECT, USING THE INITIAL CONDITIONS AND CONTROL PARAMETERS INITIALIZED IN THE PREVIOUS STEP.

FOR n=1:1000

$$a(n+1) = u * \left(a(n) - |a(n)|^2 - u * b(n)\right)$$

$$b(n+1) = -b(n) * e^{-2v} + e^{-v} * u * [\left(2 - a(n) - a'(n)\right) * b(n) - a(n) * c'(n) - a'(n) * Z(n)]$$

$$c(n+1) = -c(n) * e^{-2v} + e^{-v} * u * [2 * \left(1 - a'(n)\right) * c'(n) - 2 * a(n) * b(n) - a(n)]$$

END

STEP 3: REPEAT THE MAP EQUATIONS ONCE USING NEW INITIAL CONDITIONS (CALCULATED IN STEP 2) TO GET NEW KEY VALUES (aNEW, bNEW AND cNEW).

$$a1new = mod((floor\left(anew(1,1) * (2^{32})\right), 2^{32});$$

$$b1new = mod((floor\left(bnew(1,1) * (2^{32})\right), 2^{32})$$

STEP 4: THE CONTROL PARAMETER (u) IS MODIFIED USING c WITH THE HELP OF ARITHMETIC OPERATIONS.

STEP 5: THIS MODIFIED VALUE OF RESULTANT KEYS IS REVERSED AND ALL THE STEPS FROM 2 TO 4 ARE REPEATED, FOR GENERATION OF LATEST KEY VALUES FROM NEW KEY VALUES.

STEP 6: FINALLY, THESE KEY VALUES ARE MANIPULATED AS FOLLOWS TO GET THE VALUES WHICH CAN BE USED AS KEYS FOR DIFFERNT STAGES:

```
H=KEYS;
H1=dec2hex(H);
H2=rem(numel(H1'),3);
HH3=padarray(H1,[0 H2],'replicate','post');
H3=reshape(HH3,[],3);
H4=(hex2dec(H3));
H5=(H4');
```

STEP 7: DIFFERENT KEYS ARE OBTAINED FROM THESE VALUES

```
Key1=H5(1);
Key2=H5(2:LENGTH(DATA)+1);
Key3=H5(LENGTH(DATA)+2:2* LENGTH(DATA)+2);
```

Fig. 4 Key Scheduling Algorithm

Depending on the value of frequency, the compression stage is included. Compressed information improves the embedding capacity as well as the imperceptibility of confidential data in the cover image. The next stage is the confusion of the data before storing it into the carrier image.

3.3 Bit level confusion

This stage is used to permute the information available in bits form from the previous stage. For making the permutation process more random, the key used for the generation of random numbers is taken from the key scheduling algorithm. Pseudo-code for confusion process is given in Fig. 6.

After getting the secret data in confused form i.e. in permuted structure, the next stage is diffusion.

ALGORITHM FOR HUFFMAN COMPRESSION (SENDER SIDE)

```
INPUT:  Secret Data = data
OUTPUT: Compressed Data = hcode
STEP 1: INITIALIZE ALL POSSIBLE SYMBOLS IN SECRET DATA.
         symbols =0:255;
STEP 2: PROBABILITY OF EACH SYMBOL IS CALCULATED
         probability=ones(1,length(symbols));
         frequency=0;
         FOR J=MIN(symbols):MAX(symbols)
           FOR I=1:LENGTH(data)
             if data(I)== J
             frequency = frequency +1;
            END
          END
         probability(j+1)= frequency /length(data);
         frequency =0;
         END
STEP 3: DICTIONARY IS FORMED USING SYMBOLS AND CORRESPONDING PROBABILITY
        dict = huffmandict(symbols,probability);
STEP 4: HUFFMAN CODE FOR EACH CHARACTER OF DATA IS ASSIGNED
        hcode= huffmanenco(data,dict);
STEP 5: RESULT IS THE HUFFMAN CODE hcode.
```

ALGORITHM FOR HUFFMAN DECOMPRESSION (RECEIVER SIDE)

```
INPUT:  Compressed Data = hcode
OUTPUT: Secret Data = secret_data

STEP 1: CREATION OF DICTIONARY OR OBTAIN DICTIONARY FROM SENDER SIDE.

STEP 2: VALUE OF EACH CHARACTER IS IDENTIFIED
        secret_data= huffmandeco(hcode,dict)
STEP 3: RESULT IS THE SECRET DATA secret_data.
```

Fig. 5 Compression and Decompression Algorithm

3.4 Bit level diffusion

The diffusion process affects numerous bits of the ciphertext with alteration in each plaintext bit or key bit. For diffusion operation also keys are taken from a centralized key generation algorithm. The key size is the same as the size of confused data bits, to be diffused. The pseudo-code for this process is described in Fig. 7.

After applying all the processes i.e. compression, permutation and key-wise XOR operation, next stage comprises of hiding these bits in frequency transformed cover image using steganography.

3.5 Steganography mechanism

After confusion and diffusion of secret information, it is store into secure locations of a carrier. Various steganography mechanisms are available in the literature with their respective advantages along with application requirements [12]. Steganography is the process of hiding a secret message, by embedding it in another safe cover in such a way that only the sender and intended recipient are responsive of existence of the secret information. This technique is becoming a widespread platform in protecting sensitive communications used by intelligence and law enforcing agencies to avoid crime and terrorism; in health care systems to preserve the solitude of crucial information such as Electronics Patient Records (EPR); and in financial

ALGORITHM FOR BIT LEVEL CONFUSION (SENDER SIDE)

```
INPUT:  Compressed Secret Data or Secret Data = hcode or data (bits)
OUTPUT: Confused Data = conf_data

STEP 1: TAKE SEED VALUE FROM KEY GENERATION ALGORITHM.
STEP 2: UNIQUE RANDOM ARRAY IS GENERATED USING THIS SEED
        SEED=KEY1;
        RAND_ARRAY=randperm(LENGTH(data), LENGTH(data),);
        A=RAND_ARRAY;
STEP 3: PERMUTE BITS OF COMPRESSED DATA OR DATA BITS USING THIS GENERATED
        RANDOM ARRAY
        FOR I=1:LENGTH(hcode or data)
            ind=A(I);
            conf_data(ind)=hcode(I);
        END
STEP 4: RESULT IS THE CONFUSED ARRAY OF DATA BITS conf_data.
```

ALGORITHM FOR REVERSE CONFUSION (RECEIVER SIDE)

```
INPUT:  Confused Data = conf_data1
OUTPUT: Compressed Secret Data or Secret Data = hcode1 or data1 (bits)
STEP 1: TAKE SEED VALUE FROM KEY GENERATION ALGORITHM.
STEP 2: UNIQUE RANDOM ARRAY IS GENERATED USING THIS SEED
        SEED=KEY1;
        RAND_ARRAY=randperm(LENGTH(data), LENGTH(data),);
        A1=RAND_ARRAY;
STEP 3: RETRIVE BACK BITS OF COMPRESSED DATA OR DATA BITS USING THIS
        GENERATED RANDOM ARRAY
        FOR J=1:LENGTH(conf_data1)
            Ind1=A(J);
            Hcode1(J) = conf_data1(ind1);
        END
STEP 4: RESULT IS THE RETRIVED ARRAY OF DATA BITS hcode1 or data1.
```

Fig. 6 Pseudo-code for Bit-Level Confusion

organizations such as banks to avert account information of clients from being accessed illegally [2]. In the proposed model, Lifting Wavelet Transform (LWT) is considered due to the enormous advantages listed in Fig. 8.

The wavelet transform is one of the accepted processes for multi-resolution image analysis. It separates an image using approximate and detailed analysis by sorting out the frequencies into low and high frequencies. This 2D Wavelet Transform, results in four sub-bands: CA, CH, CV, CD. LWT with lifting scheme 'Integer wavelet' uses a fixed-point arithmetic configuration which involves not as much memory requirement as needed by the wavelet characterized by floating-point arithmetic. In most of the application areas, the pixel values are integers which are input for the wavelet filters but, the consequential filtered output no longer consists of all integers, which at times instigate rounding error. Therefore, it is firmly required to use some wavelet transform function which returns integer value after conversion. With the same objective, the proposed model uses LWT [13, 31].

Pseudo-code for embedding information in Cover Image is described in Fig. 9.

After embedding modified version of secret data in the carrier image, this resultant image is required to move through the insecure channel. Thus, it is required to study response of resultant mechanism with respect to different known parameters and its comparison with existing renowned techniques to check its efficacy and validation.

ALGORITHM FOR DIFFUSION (SENDER SIDE)

```
INPUT:  Confused Data = conf_data
OUTPUT: Diffused Data = diff_data
 STEP 1: TAKE KEYS FROM KEY GENERATION ALGORITHM key2.
 STEP 2: BIT-WISE XOR OPERATION OF KEY WITH IT'S OWN BITS AND FINALLY
         WITH CONFUSED SECRET DATA BIT.
         FOR I=1:LENGTH(conf_data)
               number=key2(I);
               number_bi=de2bi(number,16);
                FOR J=1:15
                number_bi(J+1)=bitxor(number_bi(J), number_bi(J+1));
                END
                diff_data(I)=BITXOR(conf_data(I), number_bi(16));
          END
STEP 3: RESULT IS THE DIFFUSED ARRAY OF DATA BITS diff_data.
```

ALGORITHM FOR REVERSE DIFFUSION (RECEIVER SIDE)

```
INPUT:  Diffused Data = diff_data1
OUTPUT: Retrived_data = ret_data
 STEP 1: TAKE KEYS FROM KEY GENERATION ALGORITHM key2.
 STEP 2: BIT-WISE XOR OPERATION OF KEY WITH IT'S OWN BITS AND FINALLY
         WITH CONFUSED SECRET DATA BIT.
         FOR I=1:LENGTH(diff_data1)
              number=key2(I);
              number_bi=de2bi(number,16);
              FOR J=1:15
              number_bi(J+1)=bitxor(number_bi(J), number_bi(J+1));
              END
              ret_data(I)=BITXOR(conf_data(I), number_bi(16));
        END
 STEP 3: RESULT IS THE RETRIVED ARRAY OF DATA BITS ret_data.
```

Fig. 7 Pseudo-code for Bit-Level Diffusion

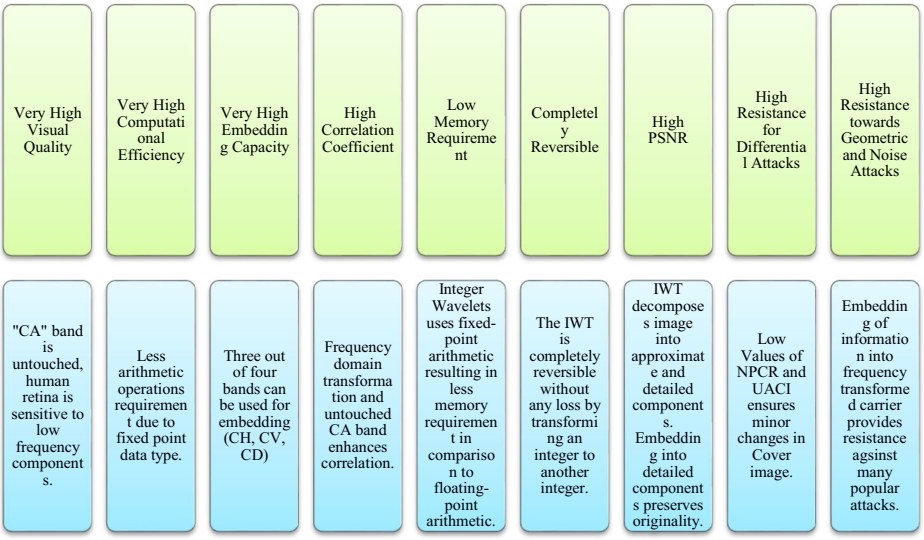


Fig. 8 Advantages of LWT

ALGORITHM FOR STEGANOGRAPHY (SENDER SIDE)

```
INPUT:  Cover Image = Im, Secret Information = diff_data, KEY=key3;
OUTPUT: Stego Image = Im_out

STEP 1: READ COLOURED COVER IMAGE Im.
STEP 2: SEPARATE ALL THE PLANES OF IMAGE.
        I_RED = Im(:,:,1);
        I_GREEN = Im(:,:,2);
        I_BLUE = Im(:,:,3);
STEP 3: APPLY 2D-LWT TRANSFORM ON BLUE PLANE WITH LIFTWAVE SCHEME OF
        INTEGER TO INTEGER (Int2Int).
         LS = liftwave('db4','Int2Int');
         [CA, CH, CV, CD]=lwt2(I_BLUE,LS);
STEP 4: EMBEDDING OF SECRET INFORMATION IN SELECTED BAND USING FOLLOWING
        METHOD. BAND CHOSEN IS 'CD'.
        [M,N]=size(CD);
        CD1=reshape(CD,1,[]);
        FLAG=1;
        diffd=diff_data;
        FOR I=1:LENGTH(diff_data)
                ind123=KEY(I);
                num=CD1(ind123);
                num1=de2bi(typecast(int32(num),'uint32'));
                num1(1)= diff_data(flag);
                num2=bi2de(num1);
                num3=typecast(num2,'int32');
                CD1(ind123)=num3;
                FLAG=FLAG+1;
        END
        CD12=reshape(CD,m,n);

STEP 5: APPLY INVERSE LIFTING WAVELET TRANSFORM ON BLUE PLANE AND
       COMBINE ALL PLANES TO FORM STEGO IMAGE.
        I_BLUE=ilwt2(CA, CH, CV, CD12, LS);
        Im(:,:,3)= I_BLUE;
        Stego_image=Im;

STEP 6: RESULT IS THE STEGO IMAGE stego_image.
```

ALGORITHM FOR REVERSE STEGANOGRAPHY (RECEIVER SIDE)

```
INPUT:  Stego Image = Im_out, KEY=key3;
OUTPUT: Retrieved Secret Data = ret_data;

STEP 1: READ STEGO IMAGE stego_image.
STEP 2: SEPARATE ALL THE PLANES OF IMAGE.
        S_RED = stego_image (:,:,1);
        S_GREEN = stego_image (:,:,2);
        S_BLUE = stego_image (:,:,3);
STEP 3: APPLY 2D-LWT TRANSFORM ON BLUE PLANE WITH LIFTWAVE SCHEME OF
        INTEGER TO INTEGER (Int2Int).
        LS = liftwave('db4','Int2Int');
        [CA1, CH1, CV1, CD1]=lwt2(S_BLUE,LS);
STEP 4: RETRIVEING SECRET INFORMATION BITS FROM SELECTED BAND USING
        FOLLOWING METHOD. BAND CHOSEN IS 'CD'.
        KEY=key3;
        [M,N]=size(CD);
        CD2=reshape(CD1,1,[]);
        FLAG1=1;
        FOR I=1:LENGTH(data)
                ind12=KEY(I);
                num=de2bi(typecast(int32(CD2(ind1234)),'uint32'));
                ret_data(FLAG1)= num(1);
                num1=bi2de(num);
                num2=typecast(num1,'int32');
                CD2(ind12)=num2;
                FLAG1=FLAG1+1;
        END

STEP 5: RESULT IS THE retrieved data ret_data at the receiver side.
```

Fig. 9 Pseudo-code for Embedding and Retrieval Algorithms

4 Simulation set up parameters

The Setup parameters used for recording results are shown in Table 2 and standard images taken for implementation and comparative analysis are revealed in Table 3. This table also endow with details regarding references taken for comparative analysis. All the Images are considered for varying sizes, as mentioned in Table 2.

As mentioned in Table 3, in order to validate the proposed method, it is compared with available renowned multilevel mechanisms. References considered for comparison are recent ones and chosen because of having similar construction, which results from a combination of diverse techniques. The data set used for experimental analysis consists of Images used as cover images and secret data to be hidden in that cover image. Images used as carrier consists of the set having some standard images like Baboon, Leena, Sunflower, Doll, and others taken from the Internet. All are shown in Table 3. Message to be embedded in these images are also taken of diverse sizes varying from 10 bytes to 500 bytes. These are combinations of alphabets, numbers, and blank spaces.

The following section demonstrates the experimental results of the proposed mechanism and its comparison with the latest references.

5 Results

This proposed model is assessed based on the variety of parameters that are represented in this section. All the results based on these performance matrices are illustrated here. Also these outcomes are compared with existing mechanisms to validate the results of given scheme.

Table 2 Set up Parameters

Parameters	Values	
Sizes of Cover Image	128x128x3, 192x192x3, 256x256x3, 512x512x3 (Set of six images for each size are taken for results)	
Image Category	Coloured Images (jpg Format)	
Secret Data (in bytes)	10, 25, 80, 150, 300, and 500 bytes	
Programming language version	MATLAB 2014	
Simulation Implement	64 bit MATLAB	
Processor	1.90Ghz, Intel (R) Core (TM i3-3227U)	
Memory	4GB	
Key value (Encryption Scheme)	**Original Key Values**	**Modified Key Values**
	a(1)=0.4523444336;	ad(1)=0.4523444335;
	b(1)=0.003453324562;	bd(1)=0.003453324562;
	c(1)=0.001324523564;	cd(1)=0.001324523564;
	u=3.99;	ud=3.99;
	v=6;	vd=6;
	a_n=0.002;	a_nd=0.002;
	b_n=0.004;	b_nd=0.004;
Keys for different stages	Key1: confusion, Key2: diffusion, Key3: steganography (all generated using key scheduling algorithm)	
Conditional Huffman	Threshold Frequency=2	

Table 3 Images and references taken for comparative analysis

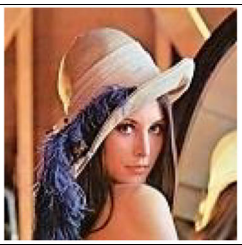


Image 1	Image 2	Image 3

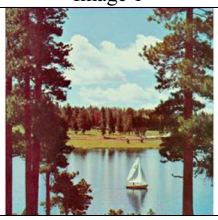



Image 4	Image 5	Image 6
		
Image 7		

REF 1	REF 2	REF 3	REF 4
(Ganguly et al., 2020)	(Bal et al., 2018)	(Jain et al., 2019)	(Tauhid et al., 2019)

5.1 Visual analysis for ensuring imperceptibility

5.1.1 Snapshots

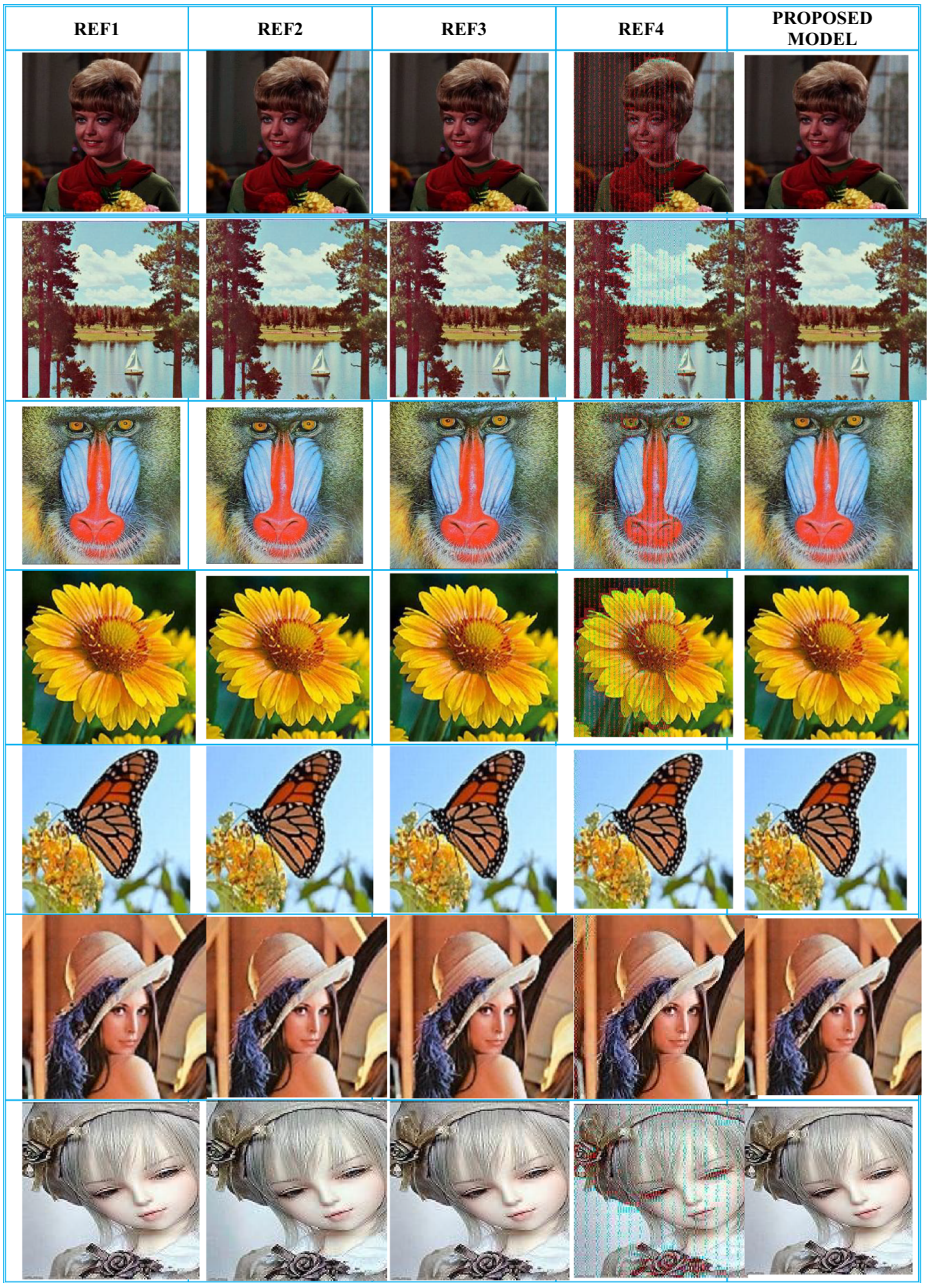
Table 4 portrays resultant stego-images, after implementing different algorithms. These results can be used for comparisons, so that visual quality and Imperceptibility of secret data in cover image can be verified.

As observed from the results, it is extremely hard to differentiate between all the images. That means all implemented mechanisms including proposed provides very fine visual quality. Several mechanisms like Ref 4 provide marks of presence of secret information in the cover image. Amount of information to be stored also marks impact on image's perceptibility.

5.2 Robustness and security analysis for ensuring confidentiality

Confidentiality of the mechanisms can be evaluated by investigation of image quality before and after embedding in both ways qualitatively and quantitatively. Former analysis is done by visual inspection of snapshots and later can be done using numerous matrices, which are described as under [9, 11, 29]:

Table 4 Stego-Images for Different Hybrid Mechanisms



5.2.1 Robustness analysis

PSNR stands for Peak signal to noise ratio. This factor is used to contrast each pixel of the image before and after inserting. High PSNR ensures the high confidentiality of stored

Table 5 Recorded PSNR and MSE Values

Images	Data size (bytes)	PSNR	MSE	Images	Data size (bytes)	PSNR	MSE
Image 1 to 7, 128*128	10	72.76	0.0034	**Image 1 to 7, 256*256**	10	79.85	0.0007
	25	69.65	0.0071		25	75.91	0.0017
	80	66.09	0.0160		80	72.98	0.0033
	150	63.57	0.0286		150	70.13	0.0065
	300	60.68	0.0557		300	67.29	0.0120
	500	59.23	0.0777		500	65.59	0.0181
Image 1 to 7, 192*192	10	75.85	0.0018	**Image 1 to 7, 512*512**	10	86.41	0.0002
	25	72.43	0.0040		25	82.84	0.0003
	80	70.39	0.0059		80	79.67	0.0007
	150	66.71	0.0152		150	77.09	0.0012
	300	63.68	0.0309		300	74.13	0.0025
	500	62.18	0.0434		500	72.49	0.0040

information. It can be calculated as under.

$$PSNR = 10*\log_{10}\left(\frac{\max^2}{\text{mse}}\right)$$

Where *max* represents the maximum value of the pixel of the image and *mse* is mean square error.

The MSE stands for mean squared error between the two images (cover and stego). Low values of MSE ensure lower error. It can be calculated as under.

$$MSE = \frac{1}{m*n}\sum_{k=1}^{m}\sum_{j=1}^{n}\left[\left(B(i,j)-A(i,j)\right]^2\right.$$

Where B and A represent cover and stego image respectively. m and n give row and column size of the image.

Seven Images of varying sizes are taken for calculations of results. Table 5 represents recorded PSNR and MSE values for proposed model.

The proposed mechanism is compared with other renowned techniques available in literature for validation of results. The comparison results are shown in Figs. 10 and 11 for PSNR and MSE respectively. As observed from the results, in comparison to the available methods, the proposed model gives the high PSNR and low MSE values. This is accomplished

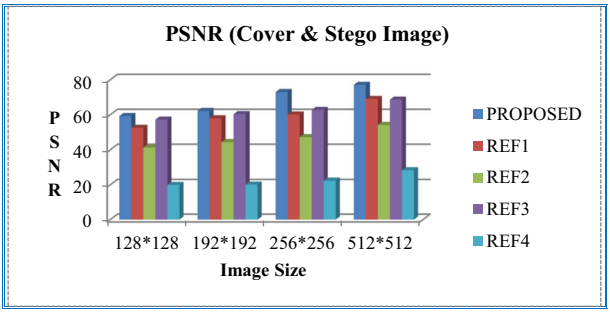


Fig. 10 PSNR Comparison

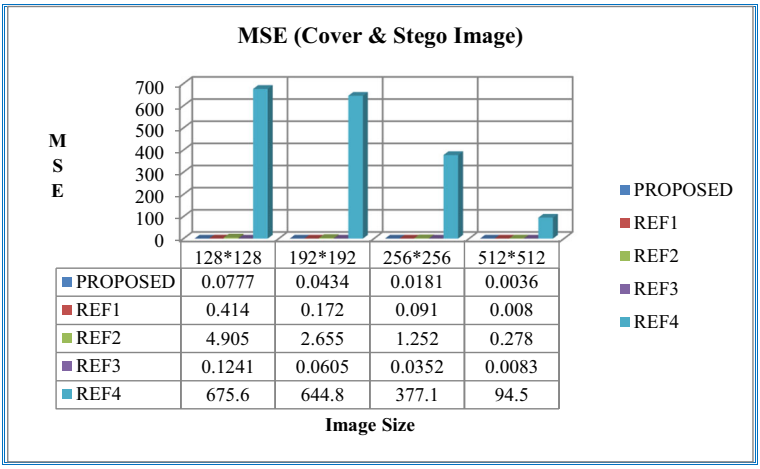


Fig. 11 MSE Comparison

by choosing the appropriate band for embedding and usage of compression process before insertion of records into cover image.

5.2.2 Security analysis

The security analysis compares the pixel values, probability distribution, and histograms between the cover and stego images. Assortment of parameters is used in this respect, to measure the similarity or dissimilarity between both images. These are the Jaccard Index (JI), Universal Image Quality Index (UIQI), Structural Similarity Index Metric (SSIM), Bhattacharya Coefficient (BC), Correlation Coefficient (CC) and Intersection Coefficient (IC). Tables 6, shows values for all the parameters for the proposed model.

Bhattacharya Coefficient (BC) gives an estimated measure of the count of overlapping between two images. It measures the relative closeness between the images. It can be computed as:

$$.BC(B,A) = \sum_{i=1}^{N} \sqrt{B1(i)*A1(i)}$$

Where *B1* and *A1* are probability distributions of the two images respectively.

Intersection Coefficient (IC) provides a count of the same value of pixels between two histograms. If the probability distribution of two images is taken as *B1* and *A1* respectively, then Intersection coefficient is given by

$$IC(B,A) = \sum_{i=1}^{N} \min[B1(i), A1(i)]$$

Where *B* and *A* represent images before and after embedding respectively. The range of value for this coefficient is between 0 to1. Where 0 represents complete mismatch and 1 represents exactly match.

Universal Image Quality Index (UIQI) is an index which computes any kind of deformation as a combination of three factors: Loss of correlation, contrast distortion and luminance distortion. Final value is calculated by multiplying these three factors.

Table 6 Recorded JI, BC, IC, UIQI, CC and SSIM Values

Images	Data size (bytes)	BC	IC	UIQI	CC	SSIM	JI
Image 1 to 7, 128*128	10	0.999989	0.996918	0.999999	0.999999	0.999992	1
	25	0.999978	0.995361	0.999999	0.999997	0.999982	0.999984
	80	0.999947	0.992696	0.999997	0.999994	0.999957	0.999931
	150	0.999908	0.990402	0.999994	0.999989	0.999929	0.999948
	300	0.999833	0.987137	0.999989	0.999978	0.999855	0.999855
	500	0.999769	0.985235	0.999984	0.999969	0.99979	0.999839
Image 1 to 7, 192*192	10	0.999997	0.998417	1	0.999999	0.999997	0.999998
	25	0.999992	0.997317	0.999999	0.999998	0.999991	0.999981
	80	0.999992	0.997233	0.999999	0.999998	0.999989	0.999972
	150	0.99997	0.99494	0.999997	0.999994	0.999969	0.999953
	300	0.999943	0.992806	0.999994	0.999988	0.999937	0.999876
	500	0.999924	0.991571	0.999991	0.999983	0.999913	0.99984
Image 1 to 7, 256*256	10	1	0.999415	1	1	0.999994	1
	25	0.999999	0.999017	1	0.999999	0.999988	0.999999
	80	0.999998	0.998636	0.999999	0.999999	0.999977	0.999986
	150	0.999996	0.998057	0.999999	0.999997	0.999953	0.999975
	300	0.999993	0.997459	0.999997	0.999995	0.999910	0.999969
	500	0.999988	0.996820	0.999996	0.999992	0.999862	0.999927
Image 1 to 7, 512*512	10	1	0.999869	1	1	0.999998	0.999999
	25	1	0.999782	1	1	0.999996	0.999994
	80	1	0.99971	1	1	0.999992	0.999993
	150	1	0.999537	1	0.999999	0.999986	0.99998
	300	1	0.999366	0.999999	0.999999	0.999973	0.999974
	500	0.999999	0.999247	0.999999	0.999998	0.999962	0.999953

$$\text{Loss of correlation}, LC(B,A) = \frac{2*SD_{AB}}{SD_A + SD_B}$$

$$\text{Contrast Distortion}, CD(B,A) = \frac{2*SD_A*SD_B}{{SD_A}^2 + {SD_B}^2}$$

$$\text{Luminance Distortion}, LD(B,A) = \frac{2*M_A*M_B}{{M_A}^2 + {M_B}^2}$$

$$UIQI(B,A) = LC(B,A)*CD(B,A)*LD(B,A)$$

Where B and A represent images before and after embedding respectively. M and SD are mean and standard deviation respectively of images (A and B). SD_{AB} is covariance between A and B.

Correlation Coefficient (CC) is an assessment of the linear association between two images. It varies from -1 to +1 both inclusive, where 1 indicates perfect match and −1 implies entirety mismatch. The correlation coefficient can be calculated as:

$$CC(B,A) = \frac{SD_{AB}}{SD_A*SD_B}$$

Where B and A represent images before and after embedding respectively. SD_{AB} is the covariance between A and B. SD is a standard deviation.

Structural Similarity Index Metric (SSIM) actually gauges the perceptual distinction between two similar images. It quantifies image quality degradation that may be caused by processes such as data embedding, compression or by losses in information communication. It is a full reference metric that involves two images; a cover or original image and a processed image.

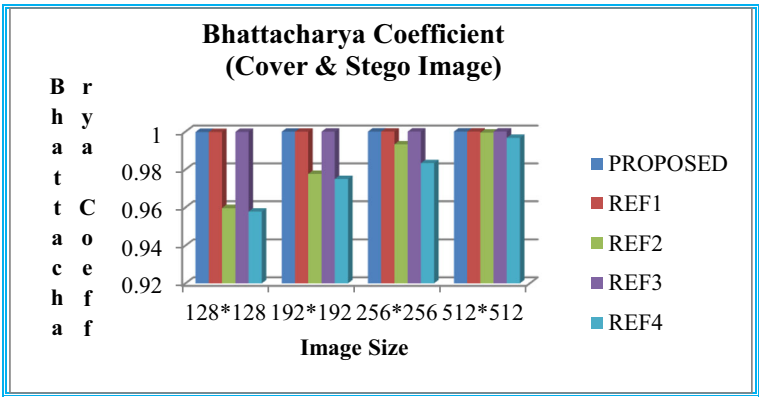


Fig. 12 Bhattacharya Coefficient Comparison

Jaccard Index (JI) is an evaluation of relationship for the two sets of data, with a range from zero to a hundred percent. High percentage indicates more similarity. It can be computed as:

$$JI(B,A) = \frac{|A \cap B|}{|A \cup B|} * 100$$

Where B and A represent images before and after embedding respectively, $|A \cap B|$ indicates the value in both images and $|A \cup B|$ tells the quantity in either image.

Figures 12, 13, 14, 15, 16, and 17 provide a comparative analysis of the projected mechanism with available methods; it can be observed from the results that the proposed approach obtains optimize results in terms of most of the metrics. Consequently, it has the competency to be more protected and offers more excellent safety towards secret information.

Results of all the parameters (JI, CC, BC, UIQI, SSIM, and IC) for security analysis are publicized in Tables 6, and Figs. 12, 13, 14, 15, 16 and 17 shows the comparison of the proposed model with other renowned mechanisms before and after embedding secret records of 500 bytes on a different basis, i.e., values (similar and dissimilar), probability distribution, intensity, standard deviation, etc. As observed from the figures, almost every outcome of comparison shows that all the parameters of the proposed mechanism have optimized values in contrast to formally accepted techniques available in the literature; this is due to the fact of employing Lifting Wavelet Transform steganography and also the choice of appropriate

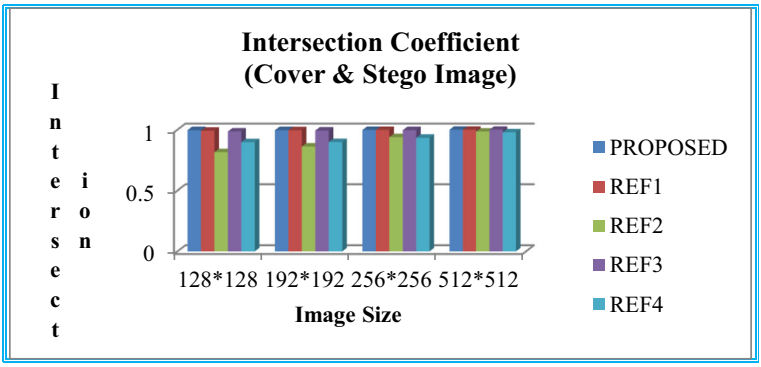


Fig. 13 Intersection Coefficient Comparison

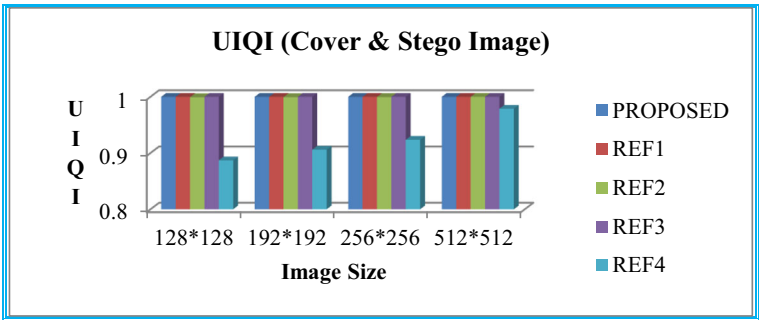


Fig. 14 UIQI Comparison

frequency bands for the embedding of information. Alteration of confidential data before embedding grants add-on protection; thus, it is conferred that the proposed technique is immensely secured.

5.2.3 Embedding efficiency

Embedding Efficiency is defined as the accepted number of embedded random secret message bits per one embedding modification. It means minimizing the alterations made to the cover

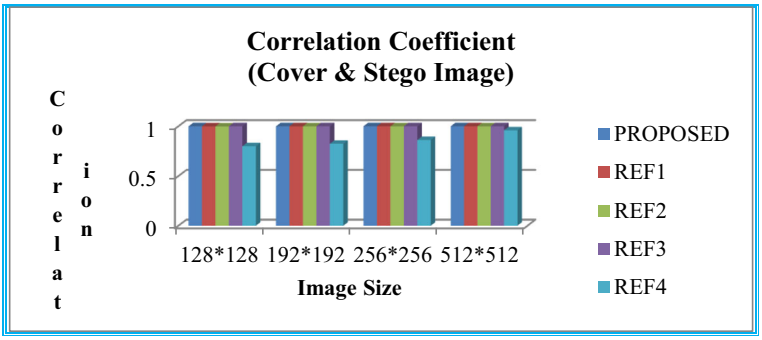


Fig. 15 Correlation Coefficient Comparison

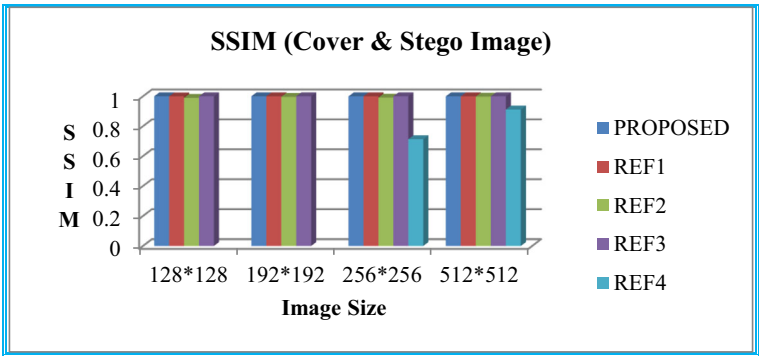


Fig. 16 SSIM Comparison

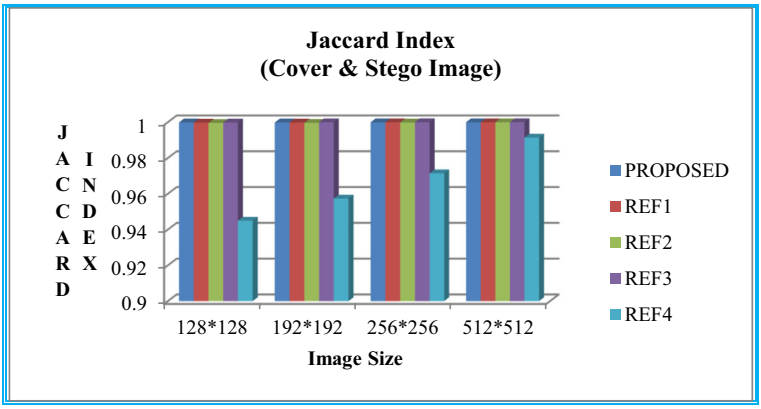
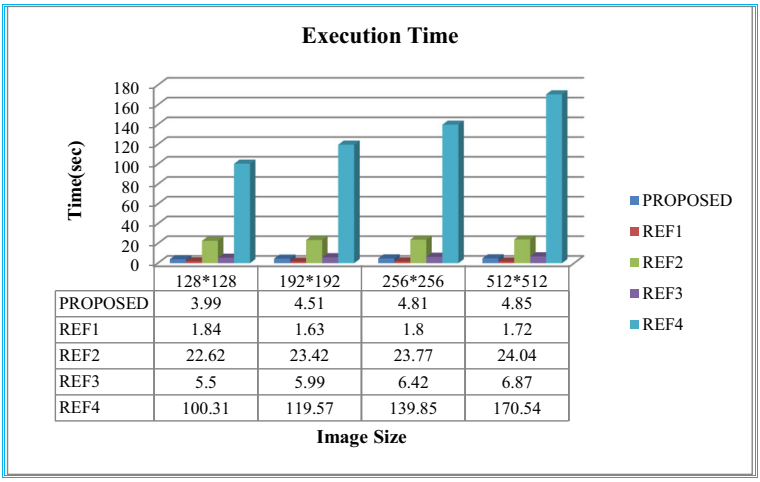


Fig. 17 Jaccard Index Comparisons

image pixels due to embedding the secret message bits while preserving capacity. Embedding capacity is of utmost importance when information to be protected is of significant amount.

1. The proposed mechanism uses LWT-based steganography, which transforms the cover image into detailed and approximate coefficients based on frequency filtering. This results in four bands; bands with Integer values similar to image pixel value ranges are selected and used for embedding. If secret message bits are large enough to complete into a single band, multiple bands can be embedding. This shows that the embedding capacity of the proposed mechanism is high enough to absorb a large amount of information.
2. Ref 1 employed Pixel Value Difference (PVD) for embedding information into the cover image. As per the algorithm, embedding is not limited only to high contrast pixel pairs; instead, low contrast pairs are also taken into account to enhance the capacity. However, the embedding process differs as per the contrast of the detected pixel pair. Thus, this algorithm provides enhanced embedding capacity for a large amount of information storage.
3. In Ref 2, a steganography technique based on the matching of bit pairs is proposed. Pixel bits of the original image and secret information, to be embedded, are arranged in pairs. The pixel bit pairs of secret messages are compared with all bit pairs of the original image, and accordingly, the substitution of bit pairs takes place with the respective harmonized pair. If no match is found, then the 0th pair is substituted, i.e., the two LSB are replaced with the value of pair number 0. This mechanism also provides good payload capacity.
4. Ref 3 employs DWT as a steganography technique, a transform domain mechanism that proves to be robust than other spatial domain steganography techniques. It employs decomposition of the cover image using ‘haar’ transform to obtain four sub-bands. Secret bits embedding are done in the selected sub-band using the Encoded Stream (ES) and Random Matrix (RM). If bit status in ES is ‘0’, RM is added to the corresponding sub-band value; otherwise, no change in value will occur. Inverse DWT is applied on the modified selected sub-band and the other three sub-bands to achieve the stego image. This mechanism can also employ multiple bands in case of a large amount of data to be embedded.
5. In Ref 4, the transform domain steganography mechanism is employed. Discrete Cosine Transformation (DCT) of the cover image is obtained, and then LSB replacements in the



	128*128	192*192	256*256	512*512
PROPOSED	3.99	4.51	4.81	4.85
REF1	1.84	1.63	1.8	1.72
REF2	22.62	23.42	23.77	24.04
REF3	5.5	5.99	6.42	6.87
REF4	100.31	119.57	139.85	170.54

Fig. 18 Speed Comparisons

Discrete Cosine Transformed (DCT) coefficients occur. In this mechanism, embedding capacity is limited as secret data bits can be stored only in the DC coefficient of the transformed image for better perceptibility. Hiding a large amount of data will result in a distorted stego image.

5.3 Time analysis for ensuring high speed of execution

In many data communication and security applications, time restriction is very prominent, requiring prompt data for further action. For reducing the time of execution, straightforward and effective processes are used, and even one stage is conditional, i.e., it will be used as per the want of data to be secured. Figure 19 shows the time required for embedding secret data in different images using various algorithms.

As observed from Fig. 18, the execution time for the proposed model is comparable with other renowned mechanisms. These values are recorded for the sender side process, used for inserting 300 bytes of secret data. Usage of simple processes for confusion and diffusion of confidential data results in a reduced amount of time complexity.

5.4 Reproducibility analysis for ensuring comprehensive data recovery

Another significant consideration to judge a protection mechanism is its capability for data extraction, i.e., the encrypted secret information hidden in the cover image should be reproduced in original form for its subsequent usage. For analyzing this factor bit error rate is measured for recovered secret data.

Table 7 shows the data recovery for different sizes of secret information and cover images. As seen from the results, the given mechanism provides perfect reproducibility of retrieved data. However, if the stego image is altered due to potential attacks or noises, then the information will not be retrieved as Huffman decompression will not allow distorted retrieved data to be converted into original form. In those cases, where the value of frequency of

Table 7 BER for Recovered Data

Images	Data size (bytes)	BER	Images	Data size (bytes)	BER
Image 1 to 7, 128*128	10	0	**Image 1 to 7, 256*256**	10	0
	25	0		25	0
	80	0		80	0
	150	0		150	0
	300	0		300	0
	500	0		500	0
Image 1 to 7, 192*192	10	0	**Image 1 to 7, 512*512**	10	0
	25	0		25	0
	80	0		80	0
	150	0		150	0
	300	0		300	0
	500	0		500	0

characters is less than threshold and compression is not employed, their bit error rate is more than 50%, and hence original secret data cannot be taken out.

5.5 Analysis of cryptography mechanism for ensuring randomness

As the proposed model is a hybrid mechanism having manifold stages, secret data undergo conditional compression and encryption before embedding. The cryptography mechanism used in the proposal consists of the confusion stage followed by the diffusion process. This dual process encryption has many factors worth analyzing. These are bit error rate, key sensitivity analysis, key-space analysis, and plain text sensitivity.

Table 8 shows the percentage of bits change when original secret data undergoes confusion and diffusion processes. More than 50% of bits are modified after the dual-stage encryption process, as seen from the results.

Figure 19 shows comparative results of encryption mechanism with existing techniques used in different hybrid models. These results are taken for encryption of 300 bytes records. As inferred from the results, randomness is highest in the proposed model compared to other algorithms as more than 50% of bits are modified after applying the proposed mechanism.

One of the main attractions of the projected mechanism is the centralized key scheduling algorithm, which is used for generating keys for different stages of hybrid model confusion stage, diffusion stage, and finally for steganography stage. This algorithm is implemented using Quantum Logistic Maps, which is selected for its desirable feature of creating randomness in generated keys. The following results show the key sensitivity towards change in initial conditions. Figure 20(a) demonstrates a change in key values used in different stages with a

Table 8 BER for Encrypted Data

Images	Data size (bytes)	BER (%)
For All Sizes of Images 1 to 7	10	49
	25	54
	80	53
	150	49
	300	52
	500	49

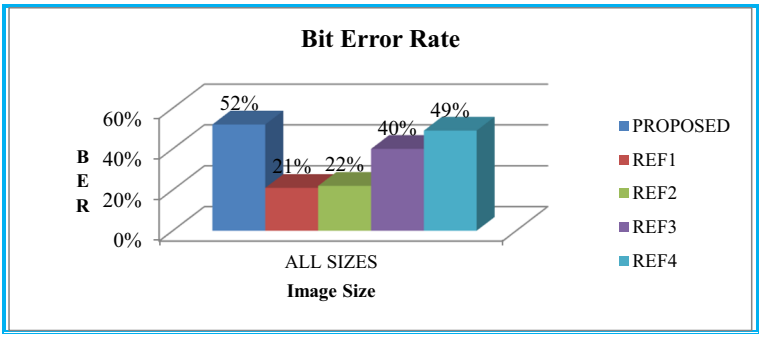


Fig. 19 BER comparison for Encryption

Keys	BER
Key1	48.85%
Key2	50.06%
Key3	49.77%

(a)

Key= {a(1), b(1), c(1), a_n, b_n, u, v}	
Specifications	**Quantum Logistic Maps Keys**
Key size	448 bits
Key space	2^{448}

(b)

Fig. 20 **a** Bit Error Rate For minor change in Initial Conditions, **b** Key Size and Space for Key scheduling Algorithm

slight change in initial conditions or keys of logistic maps. Both values are declared in set up parameters, original and modified. This resultant change in the entire key set will further modify the encryption stage values and alter the storage location in the steganography stage.

Figure 20(b) details the size of the initial keys used in the encryption mechanism along with the keyspace provided by these keys. The encryption mechanism of the proposal uses keys generated from a centralized key generation process which uses these Initial Key= {a (1), b(1), c(1), an, bn, u, v}, hence acquires key-space of 2448, which is reasonably high indicating that brute force search time for hackers is very high. This scheme provides a sizeable key spacing, hence can resist the brute force attacks, and provided a significantly less computational time for image encryption/decryption due to the usage of straightforward but effective processes.

6 Conclusion

With the increased information transversal over insecure networks and other interconnected networks, demand for crucial data protection has also elevated. The paper exemplifies a hybrid security model used to protect the confidential data used for diverse applications. The proposed scheme offers a highly secured mechanism by inculcating manifold security for data. These are conditional compression followed by dual-stage encryption and finally embedding the

modified version of records in Lifting Wave Transformed cover image. This whole mechanism provides the following desirable security characteristics:

- Ensuring confidentiality by modifying the secret data and finally hiding it into random locations of frequency transformed Image.
- Ensuring perceptibility of stego-image by choosing suitable frequency bands in lifting wavelet transformed cover image and conditional compression of the data.
- Ensuring reproducibility of retrieving records with zero bit error if an intruder does not attack it. In case of attack, reversal of records is not possible.
- Ensuring randomness by adopting Quantum logistic maps for key generation of all the stages and then applying bit-level confusion and diffusion processes.
- Ensuring high speed of execution with simple yet effective processes at each stage along with conditional compression phase.

The proposed method provides high visibility by getting the optimized values of diverse security and other parameters like SSIM, PSNR, JI, CC, IC, BC, and Speed of Execution.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography, thesis, 2015
2. Abdulla AA, Sellahewa H, Jassim SA (2014) Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping. In: Chen L, Mitchell C (eds) Security standardisation research. Lecture Notes in Computer Science. Springer International Publishing, Cham, pp 151–166. https://doi.org/10.1007/978-3-319-14054-4_10
3. Bal SN, Nayak MR, Sarkar SK (2018) On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching J King Saud Univ - Comput Inf Sci:S1319157817305153. https://doi.org/10.1016/j.jksuci.2018.04.006
4. Bansal R, Gupta S, Sharma G (2017) An innovative image encryption scheme based on chaotic map and Vigenère scheme. Multimed Tools Appl 76:16529–16562. https://doi.org/10.1007/s11042-016-3926-9
5. Bouslimi D, Coatrieux G, Roux C (2012) A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. Comput Methods Prog Biomed 106:47–54. https://doi.org/10.1016/j.cmpb.2011.09.015
6. Chaudhary D, Gupta S, Kumari M (2016) A novel hybrid security mechanism for data communication networks. International Journal of Information Privacy, Security and Integrity 2(3):216–231
7. Dhall S, Sharma R, Gupta S (2019) A multi-level steganography mechanism using quantum chaos encryption. Multimed Tools Appl 79(3–4):1987–2012
8. Dhall S, Gupta S (2021) Multilayered highly secure authentic watermarking mechanism for medical applications. Multimed Tools Appl 80:18069–18105. https://doi.org/10.1007/s11042-021-10531-w
9. Dhall S, Bhushan B, Gupta S (2016) An improved hybrid mechanism for secure data communication. Int J Comput Netw Inf Secur 8:67–79. https://doi.org/10.5815/ijcnis.2016.06.08
10. Elhoseny M, Ramirez-Gonzalez G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608. https://doi.org/10.1109/ACCESS.2018.2817615
11. Ganguly NM, Paul G, Saha SK, Burman D (2020) A PVD based high capacity steganography algorithm with embedding in non-sequential position. Multimed Tools Appl 79:13449–13479. https://doi.org/10.1007/s11042-019-08178-9

12. Gao T, Chen Z (2008) Image encryption based on a new total shuffling algorithm. Chaos Solitons Fractals 38:213–220. https://doi.org/10.1016/j.chaos.2006.11.009
13. Gholipour M (2011) Design and implementation of lifting based integer wavelet transform for image compression applications. In: Cherifi H, Zain JM, El-Qawasmeh E (eds) Digital information and communication technology and its applications. Communications in Computer and Information Science. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp 161–172. https://doi.org/10.1007/978-3-642-21984-9_14
14. Islam MR, Siddiqa A, Uddin MP, Mandal AK, Hossain MD (2014) An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. 2014 International Conference on Informatics, Electronics & Vision (ICIEV). https://doi.org/10.1109/ICIEV.2014.6850714
15. Jain Y, Sharma G, Anand G, Dhall S (2018) A hybrid security mechanism based on DCT and visual cryptography for data communication networks. In: Bokhari MU, Agrawal N, Saini D (eds) Cyber security. Advances in Intelligent Systems and Computing. Springer Singapore, Singapore, pp 131–142. https://doi.org/10.1007/978-981-10-8536-9_14
16. Jain Y, Dhall S, Gupta S, (2019) A robust multilevel security mechanism against geometric attacks. Power Eng 7
17. Kannammal A, Subha Rani S (2014) Two level security for medical images using watermarking/encryption algorithms. Int J Imaging Syst Technol 24:111–120. https://doi.org/10.1002/ima.22086
18. Kumar Nain A, Gupta S, Bhushan B, Chawla R (2013) An adaptive pseudorandom STEGO-CRYPTO technique for data communication. Int J Comput Netw Commun 5:173–188. https://doi.org/10.5121/ijcnc.2013.5414
19. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8:37. https://doi.org/10.1007/s13319-017-0148-5
20. Moizuddin M, Winston J, Qayyum M (2017) A comprehensive survey: quantum cryptography, in: 2017 2nd international conference on anti-cyber crimes (ICACC). In: Presented at the 2017 2nd international conference on anti-cyber crimes (ICACC), IEEE, Abha, Saudi Arabia, pp 98–102. https://doi.org/10.1109/Anti-Cybercrime.2017.7905271
21. Nivedhitha R, Meyyappan DT, Phil M, (2012) Image security using steganography and cryptographic techniques. Int J Eng Trends Technol 6
22. Panwar P, Dhall S, Gupta S (2021) A multilevel secure information communication model for healthcare systems. Multimed Tools Appl 80:8039–8062. https://doi.org/10.1007/s11042-020-10083-5
23. Shankar K, Eswaran P (2015) Sharing a secret image with encapsulated shares in visual cryptography. Procedia Comput Sci 70:462–468. https://doi.org/10.1016/j.procs.2015.10.080
24. Sharma A, Singh AK, Ghrera SP (2017) Robust and secure multiple watermarking for medical images. Wirel Pers Commun 92:1611–1624. https://doi.org/10.1007/s11277-016-3625-x
25. Singh AK, Dave M, Mohan A (2016) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 75:8381–8401. https://doi.org/10.1007/s11042-015-2754-7
26. Solanki N, Malik KS (2014) ROI based medical image watermarking with zero distortion and enhanced security. Int J Mod Educ Comput Sci 6(10):40–48. https://doi.org/10.5815/ijmecs.2014.10.06
27. Tauhid A, Tasnim M, Noor SA, Faruqui N, Yousuf MA (2019) A secure image steganography using advanced encryption standard and discrete cosine transform. J Inf Secur 10:117–129. https://doi.org/10.4236/jis.2019.103007
28. Tayal N, (2016) A novel hybrid security mechanism for data communication networks Multimed Tools Appl 28, A novel hybrid security mechanism for data communication networks, 76, 24090
29. Tayal N, Dhall S, Gupta S (2016) A robust hybrid steganography mechanism for security in data communication networks. Int J Comput Netw Appl 3:13
30. Wrona K, de Castro A, Vasilache B (2016) Data-centric security in military applications of commercial IoT technology. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, pp 239–244. https://doi.org/10.1109/WFIoT.2016.7845511
31. Yan Y, Dong Z (2000) An approach to integer wavelet transform for medical image compression in PACS. An approach to integer wavelet transform for medical image compression in PACS 5:3–206