Multimedia Tools and Applications (2023) 82:14527–14555
https://doi.org/10.1007/s11042-022-13798-9

An efficient steganography technique based on S^{2}OA & DESAE model

Sachin Dhawan[1] · Rashmi Gupta[2] · Hemanta Kumar Bhuyan[3] · Ravi Vinayakumar[4] · Subhendu Kumar Pani[5] · Arun Kumar Rana[1]

Received: 10 September 2021 / Revised: 23 June 2022 / Accepted: 5 September 2022 /
Published online: 26 September 2022

Abstract
This paper gives a novel and efficient steganography technique based on hybrid algorithms that improves the various important parameters like PSNR, MSE, IF, capacity, security. It increases the security of the confidential data by using the encryption method and give improved quality of stego images with less error rate. This paper utilizes a grouping of wavelet domain & Salp Swarm based Optimization Algorithm (SSOA) and proposed embedding process for increasing the payload capacity. Initially, the integer discrete wavelet transform is utilized to process the cover image and DWT to extract the hidden image accurately. Furthermore, an edge localization process is proposed to localize the edge region of detail bands efficiently, which can be done by SSO Algorithm. To enhance the quality of the stego pictures, a deep enhanced stacked auto encoder (DESAE) has been proposed. The evaluation result of this technique achieves good image quality and high security. Also, it increases the payload capacity of the existing methods, which confirms the superiority of the proposed method compared to previous related techniques.

Keywords Deep enhanced stacked autoencoder · Salp swarm optimization · Steganography · Binary bit-plane decomposition · Integer discrete wavelet

1 Introduction

The images can be hidden using either steganography or watermarking approach. In the watermarking system, the data is embedded into a carrier file to protect the proprietorship or copyright of audio, video or image files. The security of the information hidden through the watermarking system is purely related to the carrier image. Here, the cover image is considered a medium for secure communication [17]. In recent days, cyber security specialists or investigators do not provide more attention to watermarking due to its lower capacity for

✉ Ravi Vinayakumar
vravi@pmu.edu.sa

Extended author information available on the last page of the article

retaining data. Also, one can easily remove the watermark with recent advancements in digital image software technologies. Ongoing improvements in PC security have introduced steganography as a superior technique for acquired information [32]. Steganography is the way toward concealing a message, sound, picture or video into another image, sound, message or video utilizing installing measures [8, 12]. Information protection is a severe concern while sending information over the web. Cryptography and steganography are being used together to provide further protection to the information [4]. The two techniques assume a considerable part in data security.

Most people in today's world transfer the data in video, text, image and audio over the medium. The data is termed to be personal and sensitive. The encryption process is needed to be performed when the sensitive data is transferred from one device to another. This encryption technology helps to protect the data from hackers.

With the assistance of cryptography, confidential information can be effortlessly encoded. A portion of the fundamental objectives of cryptography is honesty, validation and classification [2, 3]. Then, at that point, the steganography interaction shrouds the encoded information, so it's impossible for anyone to presume that secret information exists. The steganography framework regularly incorporates three segments: cover-object, privileged information, and stego-object. If the data is implanted in the picture record (cover picture), a result is a stego-picture object [5]. The Steganography approach is decent if it considers three boundaries for the preparation, which implies limit, security, and picture quality [9, 35].

There have been different wavelet domain steganography approaches developed for embedding the secret image into the cover image [25, 29, 33]. Even though they achieved better payload capacity, they provided poor private pictures after extraction. The main reason behind this is that they used DWT, which causes truncation error due to its floating-point representation at the time of reconstruction [27]. Furthermore, the wavelet domain steganography approaches require increasing the embedding capacity by developing new embedding procedures. The sensitivity of the human visual system is not enough for edge portions. Hence, one can embed a lot of secret information in the edge portion to enhance the payload capacity and maintain better visual quality.

In Optimisation, the technique is utilized to optimize steganography [11]. Dhawan et al. proposed the novel steganography method by using the Salp swarm optimization technique and hybrid fuzzy neural technique for the best results of steganography that is measured based on PSNR, MSE, Image fidelity, and payload capacity. One more approach given by dhawan et al. has utilized the combination of a hybrid edge detector and vernam algorithm for the optimised result of steganography [10]. The nodes infuzzification layer fuzzify the input variables. Fuzzification process is performed using the membership function. One major problem in fuzzy based neural system is the difficulty of constructing the membership functions. Also, the defuzzification layer will give the output of HFNN. It computes the reconstruction error after getting the output from defuzzification layer. But the neural network used here is a shallow network, Hence it will not represent the input features efficiently. Also, it produces data loss while propagating the data from lower layer to higher one.

To avoid the disadvantages of HFNN, in our proposed technique, deep architectures are modelled that consist of multiple levels of nonlinearities. In DESAE, different auto encoders have been stacked together to get a deep architecture. Every auto encoder learns the features obtained from its lower one by minimizing the reconstruction error. To avoid data loss while propagating from lower to higher, it reconstructs the feature vector using the feature vector obtained from the lower layer and the original input data. One can achieve a good representation of input data at the output by doing this.

The proposed algorithm tries to solve all the problems related to the existing algorithms by developing an efficient secret image encryption algorithm and an efficient wavelet domain based on the encryption embedding process. It improves the security level of the encryption algorithm by combining the use of binary biplane decomposition, chaotic system and bit-level permutations. It introduced a bit level permutation between the arrangements of decomposed biplanes for permuting the bits from one plane to another using a chaotic system. As a result, the encryption algorithm will resist differential attacks. Accordingly, it takes less time and increases the security of the data compared to the methods that used RSA. RSA takes a long time to encrypt the image when the critical length is very high. When it used a shorter Key to decrease the processing time, it reduced the security of the cryptosystem. To enhance the strength of the data security, the proposed steganography method used an image encryption algorithm that combines chaotic synchronization with bit-level permutation. In addition, the proposed steganography method used a wavelet domain adaptive steganography embedding function with a new Edge/smooth block localization process for embedding the hidden image by considering the frequency domain of the cover image, which increases the payload capacity without affecting the visual quality of the picture.

This paper proposed a new steganography approach for achieving the enhanced overall presentation of the steganography scheme.

The primary role of this research is given as follows:

- A wavelet domain steganography embedding function has been proposed for embedding the confidential data by considering the frequency domain of the cover image for increasing the payload capacity. Also, it used IDWT rather than DWT to reduce the reconstruction error. Hence, this approach can be applied for any secret image.
- At first, the secret image is embedded into three approximate parts. These are HH HL and LH bands. If the size of the private image is more than LL band is also utilized to accommodate hidden image. In this way, payload capacity can be increased.
- Also, a new Edge/smooth block localization process is proposed using the Salp Swarm Optimization Algorithm to determine the edge and smooth block of the LL band. It further increases the embedding capacity of the IDWT-based algorithm.
- For best performance and high security, binary bit-plane decomposition is used for image encryption.
- Finally, a DESAE model is proposed to enhance the visual quality of the stego image as same as the input cover image.

The remaining paper is organized as follows: Section 2 gives a literature survey on image steganography. Novel steganography is proposed in Section 3. Result discussion and assessment with previous works presented in Section 4. In the end, Section 5 concludes the paper.

2 Related work

In one of the double precision technique [19] the author suggested a new high-capacity steganography methodology in double precision pictures based on 64-bit double-precision IEEE754 floating-point number notation. This number system is extremely exact, necessitating the use of 64 bits to represent pixel values in a picture. Any change caused by data hiding in double precision picture pixels is fairly little, increasing the proposed technique's capacity and PSNR. In another technique, Visual inspection and automated detection techniques were used to evaluate image-based steganography systems [1]. In another paper it makes use of a DCT coefficients and it employ a statistical model of covers to develop the analytical formulation of the most powerful detector in the context of hypothesis testing theory. The steganographer's goal is to reduce the "omniscient detector's" statistical performance, which reflects the "worst-case" situation for security [6]. In one more technique [38], first step is to develop a resilience model based on the spatial domain computed from DCT coefficients. The security cost is then calculated by comparing the spatial pixels generated from new DCT coefficients to the spatial pixels modified by the robustness model. The proposed approach, which combines the distortion function with the robustness cost function, provides great robustness while maintaining good security.

The most common and decades old method of secret image hiding in the spatial domain is LSB substitution. It conceals secret bits in every pixels of cover image equally. Therefore, the effect of embedding distortion is equally distributed in the cover image. Also, it is susceptible to attacks because of its simplicity. Hence, Kini et al [37] introduced an alternative secured algorithm. Here, a password has been deliberated as a stego key and it has been added as the additional data in the cover image. Initially, the ASCII codes have been obtained from the password and then the pixels have been selected from the cover image using stego keys. In addition, a modified technique was introduced for inserting a stego key within it. For making the changes of the cover image invisible to the human eye, the secret image and stego key have been encrypted within the first and second LSBs of the cover image. Nolkha et al [1, 26, 37] proposed channel-based image steganography. They were considered three channels, among that, one channel is considered as an indicator. Here, the stego picture was formed for various color models using LSB substitution method. The presence of confidential data in the color channels was indicated by the LSB of the indicator channel.

The replacement and information planning techniques for picture steganography developed by utilizing MLSB i.e. modified LSB [7]. As a general rule, the vast majority of the LSB strategies were not relying upon pixel connection and the substance of the pictures. Along these lines, it very well may be distinguished through RS examination.

In general, cryptographic methods are used to encrypt the image data for making secure transmission and keeping the transferred data more secure in a scientific way. Generally, the cryptographic systems use block encryption methods and other systems. Instead, the RSA algorithm increases the crypto stability and hence it has been used in different encryption applications. Also, the cryptosystem that performs bit level operations instead of bytes give higher security. Because of the advantages of RSA and bit-level operations in encryption algorithm, Kovalchuk et al. [22] gives a novel encryption algorithm by combining the elements of the RSA algorithm and bitwise binary operations. But the RSA algorithm kept object's outlines in the encrypted image.

To tackle this issue, Kovalchuk et al. [23] used the concept of topological image coverage and RSA algorithm. This method split the original image into segments to make the image coating topologically finite, which avoided the partial saving of contours at some point in encryption based on RSA. These authors also considered a theoretical observation for the combined usage of quaternary fractional-linear transformations and RSA algorithm [22]. This mathematical scheme used to avoid the outlines of image object in the encrypted image. Later, the crypt stability of the encryption approach has been improved by combining the projective transformations along with the

RSA algorithm [24]. The speed of the RSA algorithm is very low when it is applied for encrypting large data using the same computer. Also, it didn't provide authentication, confidentiality and integrity using a single phase. Instead, the chaotic systems provided a greater data security in encryption as compared to RSA algorithms. The chaos holds close relationships with cryptology due to its exact dependency on initial conditions and control parameters [13, 39]. Hence, the chaotic system has been combined with RSA algorithms [18] to strengthen the security of the cryptosystems.

Thus, Hameed et al. [14] proposed Histogram of oriented gradient (HOG) algorithm based steganography method that considered the dominant edge direction of every 2 × 2 blocks presented. Subsequently, the gradient magnitude and angles were used to identify the interested blocks of the cover image adaptively. Finally, the PVD approach has been utilized for hiding secret data along the dominant edge direction. At the same time, the remaining pixels were hidden with the LSB substitution approach. However, the payload capacity of this approach has been reduced due to the consideration of the spatial domain. Kadhim et al. [20] modified the edge-based steganography method for increasing the payload capacity with the help of a machine learning approach. This approach embedded the data adaptively by considering the Dual-Tree Complex Wavelet Transform (DT-CWT) sub-band coefficients. Also, it used a K-nearest neighbour (KNN) for the identification of smooth and texture region before the start of embedding. This approach increased the retrieval error due to the consideration of Complex Wavelet Transform.

3 Proposed methodology

Figure 1 shows the complete description of proposed technique. At first, reasonable cover and secret pictures are chosen. Here, the size of the secret picture ought not surpass the size of the cover picture. Then, at that point, the secret picture is changed over into a code picture utilizing encryption [15].

In embedding phase, the frequency domain of the cover image is considered for data embedding that can increase the pay load capacity. Initially, the cover image is converted into four frequency bands using Integer Discrete Wavelet Transform (IDWT). Here, integer DWT will be considered to avoid the error introduced due to the floating-point representation of DWT during data extraction process. At first, the secret image is embedded into three approximate bands (i.e., LH, HL and HH). If they are not enough to accommodate the entire secret image then the detail band (LL band) will embed the secret image. This edge based embedding process embeds more data into the edge region than smooth region.

Consequently, the programmed thresholding capacity is utilized to distinguish the edge parts in the LL-band of cover picture. Here, the secret picture is installed into the cover picture dependent on steganographic inserting capacity. This interaction will utilize diverse boundary esteems for edge and smooth regions. At long last, we will acquire the stego-picture. Yet, the nature of this stego picture isn't adequate. Hence, DESAE with back proliferation learning calculation is utilized to upgrade the nature of the stego pictures.

The conventional stacked auto-encoder (SAE) learns the original input data features through an unsupervised layer-wise pre-training approach. Every layer learns the features obtained from its lower one by minimizing the reconstruction error. Hence, it produces data loss while propagating from the lower layer to a higher one. Thus, it does not signify the learned features' original data patterns. In an enhanced stacked auto encoder (ESAE), every layer adds an extra constraint to reconstruct the original input data. One can achieve a good representation of input data at the output by doing this.

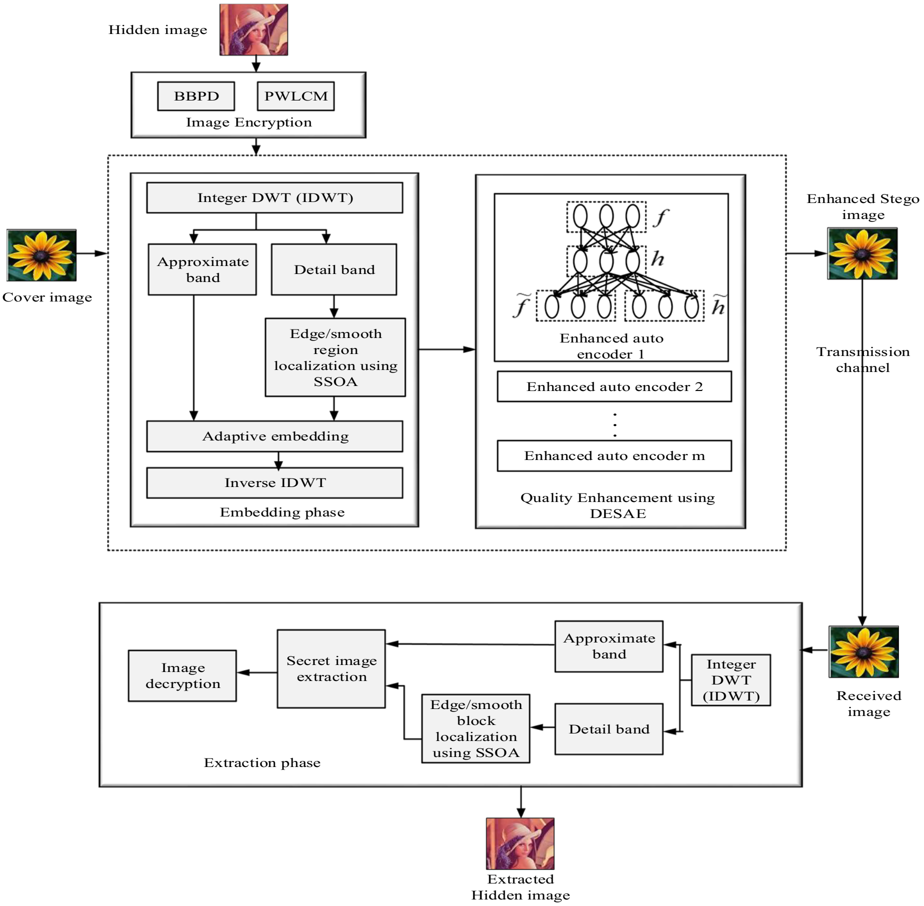


Fig. 1 Flowchart of the Proposed technique of steganography

3.1 Image encryption

This process is for encrypting the confidential image, which is initially divided into an 8-binary bit plane [18]. The binary representation is given below in the form of a decimal number represented by D:

$$D = \sum_{j=0}^{m-1} b_j \cdot 2^j = b_0 \cdot 2^0 + b_1 \cdot 2^1 + \ldots . + b_{m-1} \cdot 2^{m-1} \tag{1}$$

In this encryption, diffusion and confusion stage are utilized to generate secret key $K_1(y_0, \delta_1)$. The PWLCM [15] is given as below:

$$y_{j+1} = F\left(y_j, \delta\right) = \begin{cases} y_j/\delta & y_j \in [0, \delta) \\ \left(y_j - \delta\right)/(0.5 - \delta) & y_j \in [\delta, 0.5) \\ F\left(1 - y_j, \delta\right) & y_j \in (0.5, 1) \end{cases} \tag{2}$$

Further Y_1(j) will be generated with the help of Eq. 2. Y_1(j) can be expressed as given in Eq. 3.

$$Y_1 = mod\left(\boldsymbol{floor}\left(Y \times 10^{14}\right), 256\right) \tag{3}$$

Diffusion stage:

1. Combine all P_2 as shown below:

$$S_1 = \sum_{j=1}^{4MN} P_2(i) \tag{4}$$

2. Obtain the P_{11} element from the P_1 matrix.
3. Scramble the first component of P_{11} with the past element of P_{11} and the first component of P_2 with the principal component of K_1 as given underneath:

$$Q_1(i) = P_{11}(i) \oplus P_{11}(i{-}1) \oplus P_2(i) \oplus k_1(i) \tag{5}$$

4. Add every one of the components in Q_1 as given beneath:

$$S_2 = \sum_{j=1}^{4MN} Q_1(i) \tag{6}$$

5. Perform cyclic shift activity in the P_2 grid to acquire P_{22}. Here, the components in the P_2 framework are correctly moved by S_2 bits.
6. Encrypt the first component of P_{22} with the past element of P_{22} and the first component of Q_1 with the main component of K_2 as given underneath:

$$Q_2(i) = p_{22}(i) \oplus p_{22}(i{-}1) \oplus Q_1(i) \oplus k_2(i) \tag{7}$$

Next is the confusion stage:

1. Combine every one of the components in Q_1 and Q_2 as given beneath:

$$S_3 = \sum_{j=1}^{4MN} Q_1(i) + Q_2(i) \tag{8}$$

2. Produce keystream Z_1 and Z_2 using the mysterious key $K_2(z_0, \delta_2)$. The accompanying articulation is utilized to produce the underlying va

$$a_0 = mod(z_0 + S_3/4MN, 1) \tag{9}$$

3. Produce a sequence A={a_1, a_2, ... a_{2MN}} with the help of PWLCM.

   Sequence $Z_1$and Z_2 are generated from the sequence of A:

$$Z_1 = mod\left(floor\left(A_1 \times 10^{14}\right), 4MN\right) + 1 \tag{10}$$

$$Z_2 = mod\left(floor\left(A_2 \times 10^{14}\right), 4MN\right) + 1 \tag{11}$$

4. Get the encoded column vector R_1 by trading the components in Q_1 and Q_2 as given underneath

$$temp = Q_1(i) \tag{12}$$

$$Q_1(i) = Q_2(Z_1(i)) \tag{13}$$

$$Q_2(Z_1(i)) = temp \tag{14}$$

5. Acquire the scrambled line vector R_2 by trading the components in Q_1 and Q_2 as given beneath:

$$temp = Q_2(i) \tag{15}$$

$$Q_2(i) = Q_1(Z_2(i)) \tag{16}$$

$$Q_1(Z_2(i)) = temp \tag{17}$$

6. Convert the row vectors R_1 and R_2 into M x N picture to acquire the code picture

After image encryption, the images can be decomposed into low and high-frequency components using DWT. Here, the maximum signal energy of the image will be accumulated in the low-frequency component. Instead, the detailed information will be represented by the high-frequency component. Here, Haar-IDWT is applied to decompose the image into approximate (HL, LH and HH) and detail (LL) bands. The conventional DWT provides floating-point representation for wavelet coefficients. If the confidential data is embedded into this floating-point representation, it causes some truncation error while extracting the data. Hence, it will give a poor quality secret image. But, integer to integer mapping will be carried out by IDWT for decomposing and reconstructing the images perfectly with no truncation error. Here, Haar-IDWT is used for decomposing the cover image, which ensures that the secret bits can be separated from the stego image accurately without introducing any truncation error.

3.2 Embedding process using Salp swarm optimization algorithm (SSOA)

Both smooth and edge areas are utilized to insert the mysterious picture information by setting distinctive boundary esteem in the steganography. Here, the approximate bands considered the same parameter value since it does not contain any edge regions. While embedding the data into a detail band (i.e., LL-subband), the SSOA algorithm is utilized by setting a target [28] based on Manhattan Distance administrator (l_1 – standard) [36]. The most extreme worth of the target work addresses the presence of edges. Then, at that point, the mysterious bit esteems are inserted into the cover picture dependent on the adjusted implanting steganography installing capacity for recurrence area cover picture. This cycle will utilize distinctive boundary values for edge and smooth regions. In the end, a stego-picture will be obtained.

3.2.1 Localization of edge/smooth block

In the proposed work, SSOA calculation is presented to confine the edge/smooth pixels in the LL-band of the cover picture by recognizing ideal edge esteem dependent on the boost of target work (Manhattan Distance administrator (l_1 – standard). The SSOA is a populace-based improvement calculation that copies the multitude of salps in nature. In salp swarm, it consists of two people: a leader and followers.

$$S_i = \begin{bmatrix} s_1^1 & s_2^1 & \cdots & s_n^1 \\ s_1^2 & s_2^2 & \cdots & s_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^m & s_2^m & \cdots & s_n^m \end{bmatrix} \tag{18}$$

After instating the populace as in (20), the wellness of each search specialist ought not be set in stone to get the ideal edge an incentive for edge identification. The (l1 – standard) is Fig.d by every salp in the SSOA. When any salp finds itself in the coefficient situated at the LL-band of cover picture, the Manhattan Distance of each of the 8-adjoining coefficients from the center coefficient is determined utilizing (21). This targeted work decides the discrete subsidiaries of the neighbouring coefficients to prove the presence of edges. The most significant worth of the target work addresses the higher possibility of advantages.

$$\begin{aligned} f = |C_{((i-1),(j-1))}-r| + |C_{(i-1,j)}-r| + |C_{(i-1,j+1)}-r| + |C_{(i,j-1)}-r| + |C_{(i,j+1)}-r| \\ +|C_{(i+1,j-1)}-r| + |C_{(i+1,j)}-r| + |C_{i+1,j+1}-r| \end{aligned} \tag{19}$$

Where |·| shows the operator for getting total qualities and r addresses the center coefficient at a position (i, j)inside the cover picture C, wherein the most recent high mountain is positioned. After acquiring wellness, everything being equal, the best inquiry specialist is considered the pioneer salp. In SSOA, the area of the pioneer molecule is processed as:

$$s_j^1 = \begin{cases} T_j + \varepsilon_1\left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j\right) \varepsilon_3 \geq 0.5 \\ T_j - \varepsilon_1\left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j\right) \varepsilon_3 < 0.5 \end{cases} \tag{20}$$

Where S_j^1 represents the situation of pioneer, and T_j addresses the position vector of food source, B_U^j and B_L^j Addresses the upper and lower limits individually. ϵ_2 & ϵ_3 are irregular qualities in the scope of 0 and 1. The significant boundary ϵ_1 not really settled utilizing the accompanying articulation

$$\varepsilon_1 = 2e^{-\left(\frac{4n}{N_{\max}}\right)2} \tag{21}$$

$$s_j^i = 0.5 \times \left(s_j^i + s_j^{i-1}\right) \tag{22}$$

Where s_j^i addresses the situation of ith follower in jth measurement. In SSOA, every one of the salps is started arbitrarily. Then, at that point, the fittest salp is chosen by assessing the target capacity, everything being equal. Conditions (20) and (22) are utilized to refresh the position vectors of pioneer and devotees separately. Meanwhile, the boundary ϵ_1 is refreshed utilizing (21). Algorithm 1 shows the calculation for getting the ideal edge using SSOA calculation.

Algorithm 1 Edge and smooth area detection using SSOA algorithm

```
1.  Set the most extreme number of emphases $N_{max}$, populace size m, boundaries of SSOA and characterize the target work
2.  Set the places of salps on LL-sub band cover picture C in an arbitrary way
3.  Set n:=1
4.  Repeat
5.  Ascertain the fitness function of each search specialist situated at an organizing of cover picture C utilizing (21)
6.  Choose T as the hunt specialist
7.  Change the fundamental boundary of SSOA $\epsilon_1$ utilizing (21)
8.  for ( i=1: i≤ m) do
9.  if i==1, then
        Update pioneer's position utilizing (20)
    else
10. Update devotee's positions utilizing (22)
    end for
11. Verify if any hunt specialist doesn't have a place with the upper and lower limits and correct it.
12. Decide the strength task of the search specialist.
13. Update T in case of a superior arrangement
14. Set n= n+1
15. until n< $N_{max}$
16. Return optimal T
```

After getting the edge/smooth upsides of the cover pictures utilizing the ideal limit esteem, the LL-sub band of the cover picture is partitioned into non-covering k-coefficient blocks. Their relating coefficient esteems are g = (g1, g2, ...gk). Given the presence of edge esteems, the squares are distinguished as edge squares and smooth squares, as shown (25)

$$class = \begin{cases} edge\ block & if\ N_e > N_s \\ smooth\ block & if\ N_e < N_s \end{cases} \tag{23}$$

Where N_e and N_s represent several edge values and smooth values, respectively.

3.2.2 Embedding process wavelet domain adaptive

The secret image is embedded into three approximate bands (i.e., LH, HL and HH). If they are not enough to accommodate the entire hidden image, then the detail band (LL sub-band) will be used to embed the secret image. The main aim of the proposed embedding process is to create less change in the raw coefficient of the cover image to increase the visual quality. ρ_l and $b_s = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_l}{j} x\ 2^j$ They are used by the three approximate bands and smooth blocks of the LL-sub band. Edge block uses ρ_h and $b_e = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_h}{j} x\ 2^j$ Embedding process are shown below:

1. Find the wavelet domain F(g) = Ag^Tmod b_1, in which b_1 = b_s and ρ_1= ρ_l for approximate bands and b_1 = b_s and ρ_1= ρ_l and b_1 = b_e and ρ_1= $\rho_h$for smooth and edge block of detail bands.
2. Process u = mod(s, b1) and d = u-F(g)mod b1, where s addresses the encoded bit esteems in the mysterious picture.
3. Then, the mysterious worth s is supplanted with (s-u)/b1, and the pixel esteems are changed by running the following k-pixel block. On the off chance that d > 0, move to stage 3.
4. On the basis of condition F(v) = d and ||v||1 ≤ ρ.Find vector v.
5. Compute $g^{'} = \left(g_1^{'}, g_2^{'}, \dots\dots.g_k^{'}\right)$ using $g^{'}$ = g + v and $g^{'} = \left(g_1^{'}, g_2^{'}, \dots\dots.g_k^{'}\right)$ is adjusted to $g^{''} = \left(g_1^{''}, g_2^{''}, \dots\dots.g_k^{''}\right)$,:

$$g^{''} = \begin{cases} g^{'}-b_1 & g^{'} > 255 \\ g^{'}+b_1 & g^{'} < 0 \\ g^{'} & 0 \le g^{'} \le 255 \end{cases} \tag{24}$$

Check if the LL-sub band block $g^{''} = \left(g_1^{''}, g_2^{''}, \dots\dots.g_k^{''}\right)$ belongs to smooth or edge block using the optimal threshold value derived from the suggested edge localization procedure. No change is required if the block $g^{''}$is equivalent to g. Then, at that point, the square g and the mysterious worth are supplanted with square and (s-u)/b1 separately. At the point when the square kind of g" isn't the same as g, a proficient extraction of the mystery digit is beyond the realm of the imagination on the collector side. Accordingly, one should move to adjust stage 6 (Fig. 2).

6. Embedding process contains two steps:

Occasion 1 Amend the pixels esteems to ensure a similar square sort as the square before inserting. Decide $v^1 = v_1^1, v_2^1, \dots\dots.v_k^1$ by thinking about the accompanying conditions.

i. block g and $g^{'}$ = g + v^1 ought to be in a similar square sort.
ii. F(g+ v^1) = u.
iii. 0 ≤ g+v^1 ≤ 255.
iv. the worth $\|v^1\|_2$ is limited.

Occasion 2 In the k-pixel block, change the inserted covert digit. If b_1 equals b_s, then b_2 equals b_e. Aside from that, b_2 = b_s. u' = mod(s, b_2) is a process. At that time, the digit u' is inserted into the square. Consider the following situations for determining v^2 = v $_1{}^2$, $v_2{}^2$,......$v_k{}^2$:

(i) block g and $g^{'}$ = g+ v^2should be in different block types.
(ii) F(g+ v^2) = $u^{'}$.
(iii) 0 ≤ g+ v^2 ≤ 255
(iv) worth of $\|v^2\|_2$ is minimized.

Here, on occasion 1 will give a higher payload least inserting mutilation when $\frac{log_2\ b_1}{\|v^1\|_2} > \frac{log_2\ b_2}{\|v^2\|_2}$. Then, at that point, the square g and the mysterious worth s are supplanted with block g + v^1

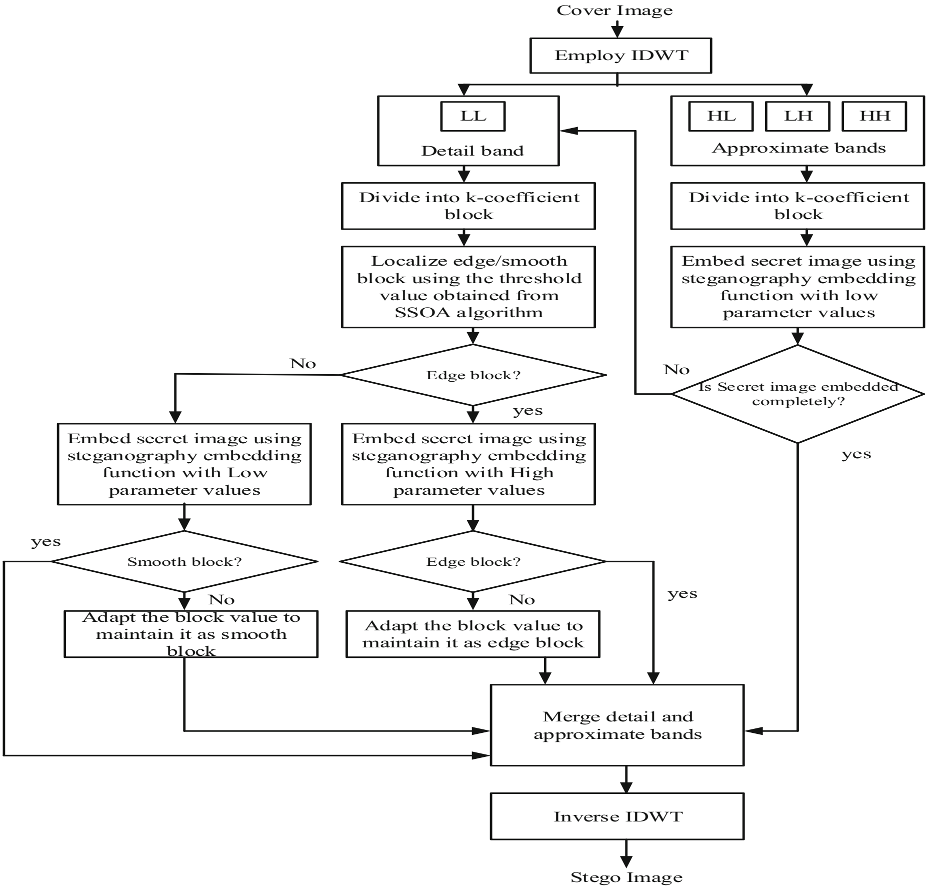

Cover Image
Employ IDWT
LL
Detail band
HL
LH
HH
Approximate bands
Divide into k-coefficient block
Divide into k-coefficient block
Localize edge/smooth block using the threshold value obtained from SSOA algorithm
Embed secret image using steganography embedding function with low parameter values
No
Edge block?
yes
No
Is Secret image embedded completely?
yes
Embed secret image using steganography embedding function with Low parameter values
Embed secret image using steganography embedding function with High parameter values
yes
Smooth block?
No
Edge block?
No
yes
Adapt the block value to maintain it as smooth block
Adapt the block value to maintain it as edge block
Merge detail and approximate bands
Inverse IDWT
Stego Image

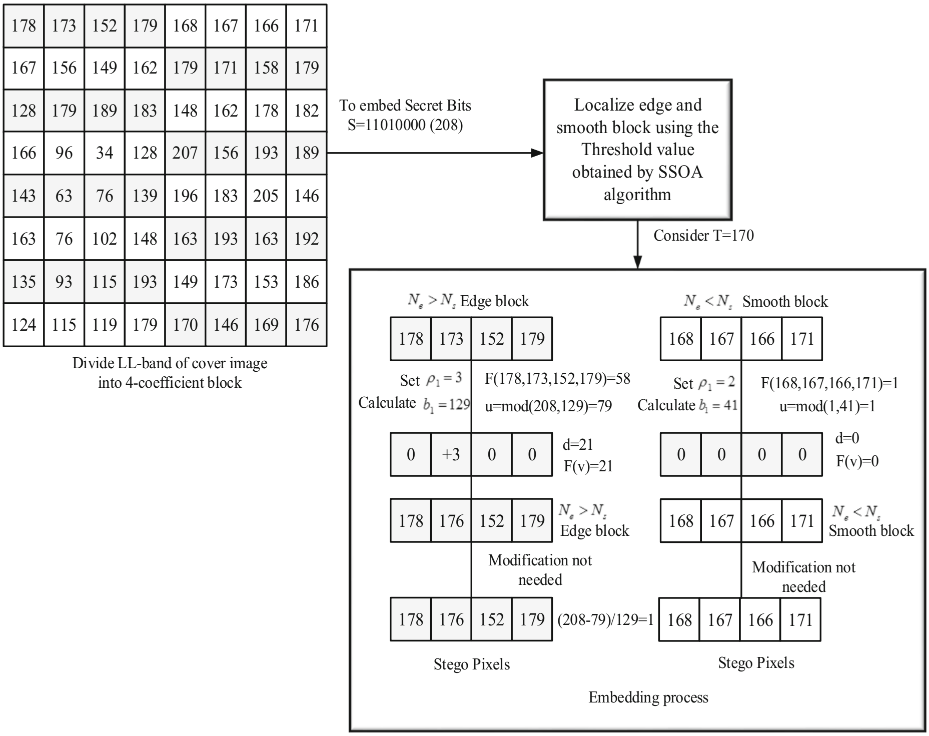
Fig. 2 Flow diagram of the proposed embedding process

and (s-u)/b_1. For the other condition, occasion two will furnish a higher payload with the least installing contortion. On this occasion, the square and the mysterious worth s are supplanted with block $g + v^2$ and (s-u)/b_2 individually.

7. Rehash the above moves forward to s = 0 for getting the stego picture.

The model for inserting utilizing SSOA upgraded versatile implanting measure is displayed in Fig. 3. In this model, the picture is separated into the 4-pixel block. Consequently, the nature of this stego picture is improved by utilizing DESAE with back proliferation learning calculation.

As shown in the flowchart, there is a DESAE model with Back Propagation Learning for Quality Enhancement after the embedding process. The nature of the acquired stego picture isn't sufficient. Subsequently, a post-handling strategy depends on the explicit innovative framework. This stage is needed to decrease the probabilities of real ID and different sorts of picture control assaults. A DESAE is a deep neural network (DNN) with unsupervised learning using a back propagation algorithm [31]. The diagram portrayal for stego picture quality upgrade utilizing DESAE is displayed in Fig. 4.



178	173	152	179	168	167	166	171
167	156	149	162	179	171	158	179
128	179	189	183	148	162	178	182
166	96	34	128	207	156	193	189
143	63	76	139	196	183	205	146
163	76	102	148	163	193	163	192
135	93	115	193	149	173	153	186
124	115	119	179	170	146	169	176

Fig. 3 Salp Swarm Optimization Algorithm optimized adaptive embedding in LL-sub band

Besides, the factual and visual elements are removed from the stego and cover pictures. Here, the chi-square likelihood and the Euclidian standard are utilized to individually address the measurable and graphic elements. The free bits support and the two provisions of the stego picture are given as a contribution to the DESAE. After that DESAE model gives an improved stego image.

Moreover, the factual and visual components are separated from both images. The objective of a DESAE is to transform given samples, including the free bit buffer values and features of stego and cover images, into a compressed form for learning hidden patterns through the minimization of distortion in reconstructed elements. Let$f\widetilde{f}$ be the raw input of DESAE and its reconstructed data.$\{\omega, \ \beta\}$ And $\left\{\widetilde{\omega}, \widetilde{\beta}\right\}$ represents the encoder and decoder parameters. Also, the activation function of the encoder and decoder can be defined as g and $\widetilde{g}$ respectively.

The first improved auto encoder's input layer gets the original data $f = f_1, f_2, \ldots\ldots, f_N$ for the construction of the hidden feature vector $h^1 = h_1^1, h_2^1, \ldots\ldots. h_N^1$ using the activation function g, whose weight and bias values are displayed $\{\omega_1, \ \beta_1\}$. Using the hidden feature vector h^1 and the activation function with, the first improved auto encoder reconstructs the input data $\widetilde{f}$ at the output layer. The concept function for reducing the reconstruction error at the first improved auto encoder is as follows:

The first improved auto encoder's input layer gets the original data $f = f_1, f_2, \ldots\ldots, f_N$ for the construction of the hidden feature vector $h^1 = h_1^1, h_2^1, \ldots\ldots. h_N^1$ using the activation function g, whose weight and bias values are displayed $\{\omega_1, \ \beta_1\}$. Using the hidden feature vector h^1 and

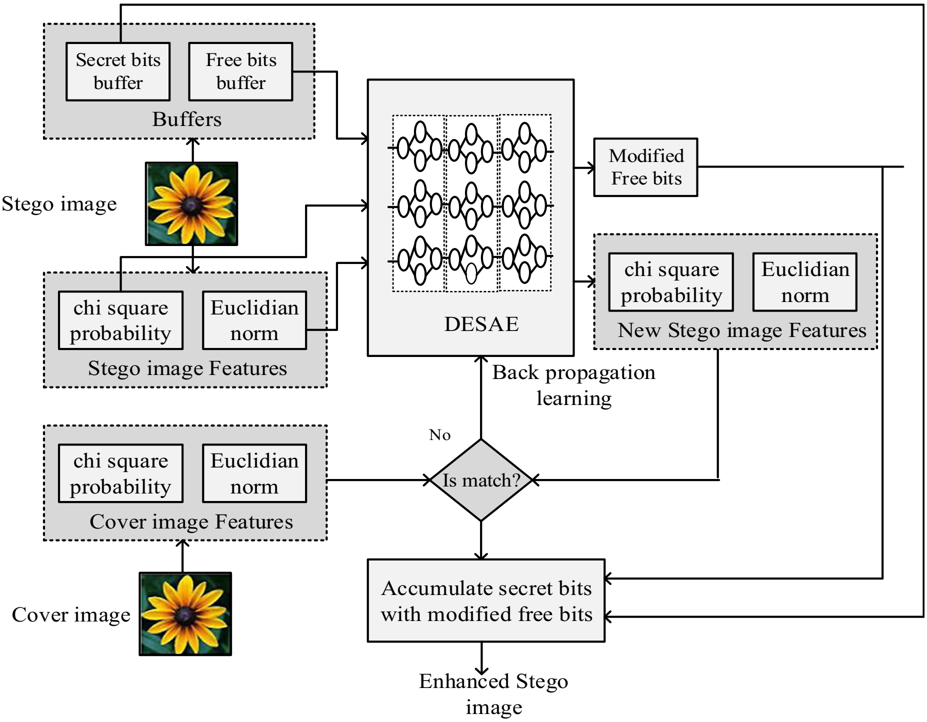


Fig. 4 Stego image quality enhancement using DESAE

the activation function $\widetilde{g}$ with $\{\widetilde{\omega}_1 , \widetilde{\beta}_1\}$, the first improved auto encoder reconstructs the input data $\widetilde{f}$ at the output layer. The concept function for reducing the reconstruction error at the first improved auto encoder is as follows:

$$J_1\left(\omega_1, \beta_1, \widetilde{\omega}_1, \widetilde{\beta}_1\right) = \frac{1}{2N} \sum_{j=1}^{N} \left\| \widetilde{f}_j - f_j \right\|^2 \tag{25}$$

Once the pre-training of the first enhanced auto encoder has been completed, its feature vector $h^1 = h_1^1, h_2^1, \ldots\ldots. h_N^1$ will be utilized for learning the second enhanced auto encoder. A similar process was repeated to obtain other feature vectors $h^1, h^2, h^3, \ldots.., h^m$. After pre-training m (m = 1, 2,…, M-1) number of the enhanced auto encoder, it gives the feature vector $h^m = h_1^m, h_2^m, \ldots\ldots. h_N^m$. The m + 1th level features $h^{m+1} = h_1^{m+1}, h_2^{m+1}, \ldots\ldots. h_N^{m+1}$. Can be obtained using the m-th level feature. The m + 1th auto encoder reconstructs the feature vector $\widetilde{h}^m$ and the original input data $\widetilde{f}^m$ to retain the inherent structure of the original data. For obtaining the enhanced auto encoder, there is a need to minimize the reconstruction error and the objective function can be represented as:

$$J_{m+1}\left(\omega_{m+1}, \ \beta_{m+1,}\omega_{m+1,}\widetilde{\omega}_{m+1}, \widetilde{\beta}_{m+1}\right) = \frac{1}{2N} \sum_{j=1}^{N} \left(\frac{\left\| \widetilde{f}_j^m - f_j^m \right\|^2}{+\| \widetilde{h}_j^m - h_j^m \|} \right) \tag{26}$$

In the receiver end, the secret picture extraction measure incorporates similar strides as inserting yet in reversible request. Here, the first cover picture isn't needed to extricate the mysterious picture. Here, the stego image initially decomposed using IDWT as same as embedding process for generating the approximate and detail bands. Then, these bands divided in k-blocks. The coefficient values of these blocks are equivalent to$g'' = (g''_1, g''_2, \ldots .g''_k)$. For the approximate bands, assign $b = b_s$ and $\rho = \rho_l$. In the LL sub band, the ideal edge esteem is determined by the SSOA calculation for the decrease of smooth and edge blocks in the stego picture. Check every k-pixel obstructs in LL-sub band utilizing the ideal edge esteem got from the proposed edge limitation calculation to distinguish whether it has a place with smooth block or edge block.

Assign $b = b_s$ and $\rho = \rho_l$ for smooth block and $b = b_e$ and $\rho = \rho_h$ for edge block. Compute F(g'') = $Ag'\,'\,^T$ *mod b*. Then, the secret digit u = F(g'') is extracted. This process is repeated until all the digits in the k-pixel blocks are extracted. Then, the decryption process is performed, which is the reverse encryption process. However, care should be given to the reverse process of the cyclic shift and swap.

4 Results and discussion

In this part, the presentation of the proposed steganography conspire is assessed as far as stego picture quality, payload limit, security and power to assaults. Likewise, the presentation investigation of the proposed conspire is approved by contrasting it and other existing works. The proposed steganography plot is recreated in Matlab R2019a climate under the Windows 10 activity framework. To approve the presentation of the proposed steganography strategy, 100 diverse covers and ten mystery pictures are chosen.

Hence, it provided 1000stego images. It includes the 8-bit grey-level images. The sample cover images taken from this dataset include Lena, Bell pepper, and Baboon. Set of cover images are shown in Fig. 5.

In this paper, the proposed steganography plot has been dissected by taking an instance of implanting of mystery Barbara picture into Lena's cover picture. At first, the mystery Barbara picture is encoded utilizing BBPD-based picture encryption calculation. Figure 6a shows the secret image of Barbara. Figure 6b shows the eight binary bit planes of the hidden image. And Fig. 6c shows the encrypted picture of Barbara.

Process used in this paper determine edge pixels of the LL-band of cover image. Here it delineates the inserting system yield of this strategy in Fig. 7.

While extracting the secret data, the installing system acted backward to extricate the scrambled stowed away picture. It doesn't need the original image. Then, at that point, the removed secret picture is unscrambled, as displayed in Fig. 8. As shown in the Fig., the proposed technique can productively remove the hidden image without influencing the nature of the picture.

4.1 Analysis of stego image

The stego image examination of our technique dependent on various execution measurements is clarified in this segment. The deformation and resemblance degree of a picture can be evaluated by Mean Square Error (MSE) to gauge the unwavering quality as given beneath:

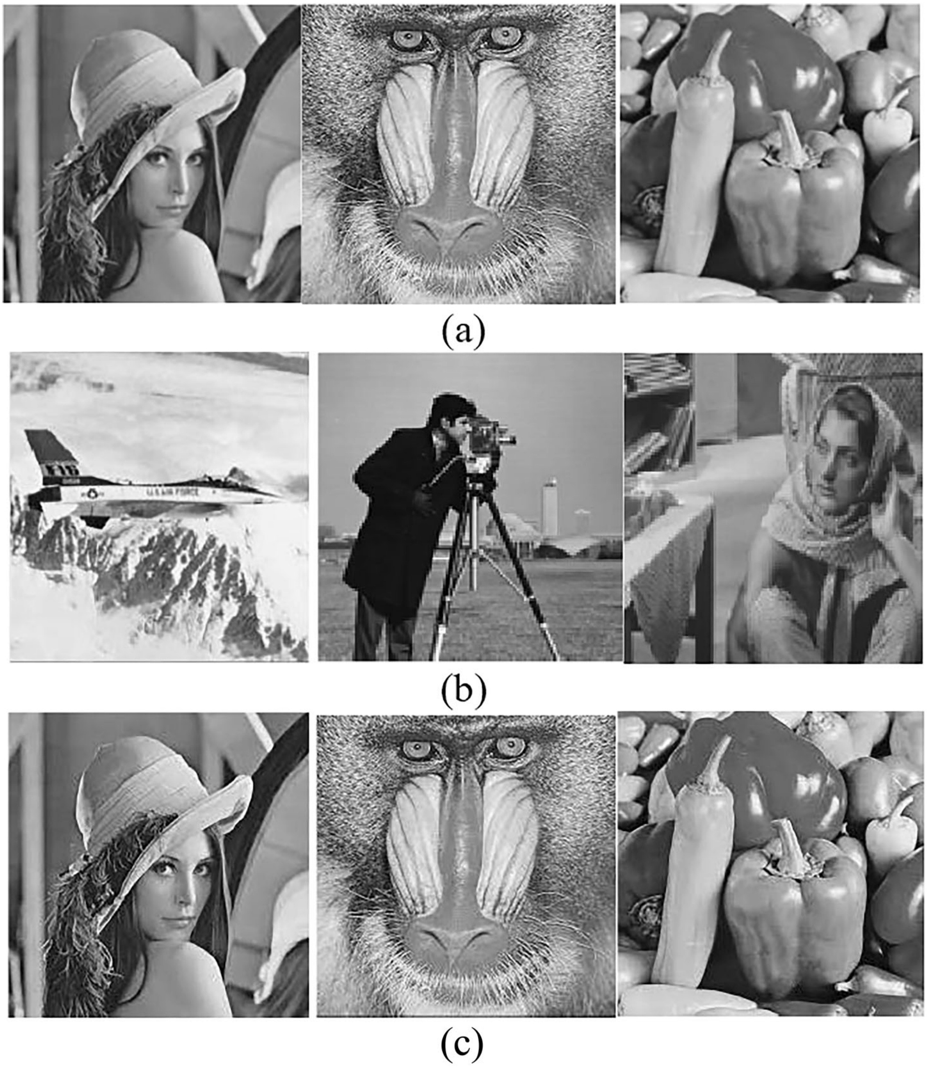


Fig. 5 Sample image sets (**a**) Cover images (**b**) Hidden images (**c**) Stego images

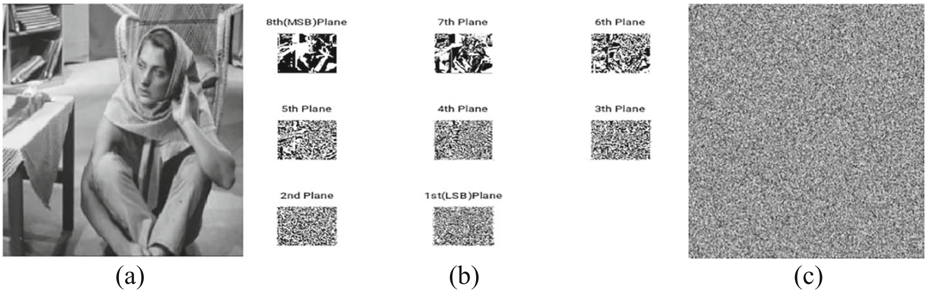


Fig. 6 Encryption Stage (**a**) Hidden image (**b**) Binary bit planes (**c**) Encrypted image

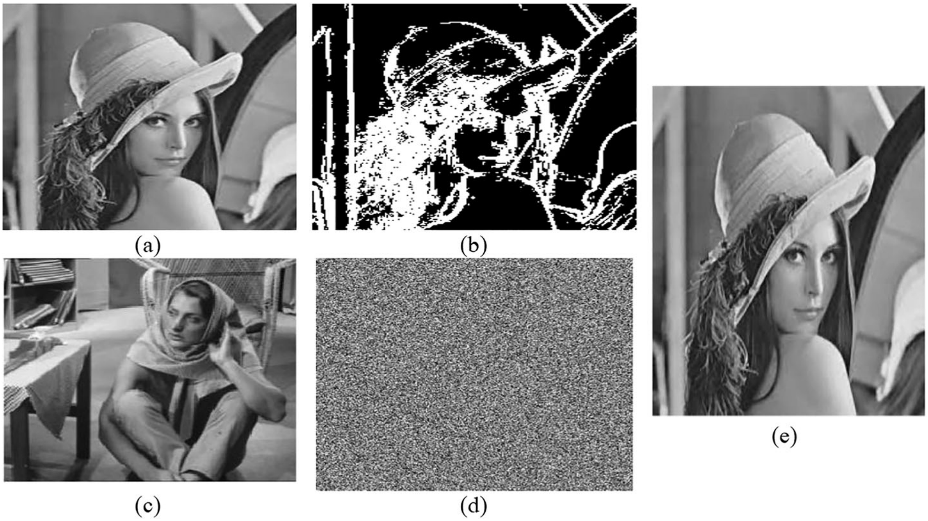


Fig. 7 Embedding process (**a**) Cover image (**b**) Edges of cover image (**c**) Secret image (**d**) Encrypted hidden image (**e**) Output Stego image

$$MSE = \frac{1}{m}\sum_{i=C,S}^{m}(C-S)^2 \tag{27}$$

The value of PSNR can be calculated as follows:

$$\boldsymbol{PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)} \tag{28}$$

Unfortunately, the aspects of HVS are not considered in PSNR measurement but it gives good validation for determining the deviation between the cover and stego images. Hence, we considered one more quality metric namely, weighted peak signal to noise ratio (WPSNR) that considers the objective measure and aspects of HVS. The sensitivity of human eye is low for variation in highly textural areas. Thus, WPSNR includes an extra parameter, namely noise visibility function (NVF). It estimates the visual quality of the image exactly. The following expression is used to calculate the WPSNR value:

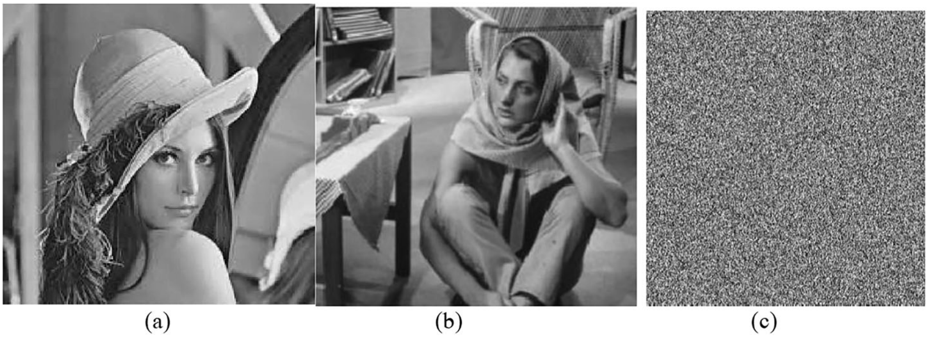


Fig. 8 Extraction phase (**a**) Received Stego image (**b**) Extracted hidden image (**c**) Decrypted hidden image

$$\boldsymbol{WPSNR} = \boldsymbol{20log_{10}}\left(\frac{\boldsymbol{255}}{\sqrt{MSE \times NVF}}\right) \tag{29}$$

Here, NVF used a Gaussian model for estimating the quantity of texture content of the image. The NVF value will be higher than o for the edge area, which will be higher than 1 for the smooth area. The NVF value can be computed as follows:

$$NVF = norm\left(\frac{1}{1 + \delta_{\boldsymbol{block}}{}^{2}}\right) \tag{30}$$

where δ represents block luminance changes and *norm* represents a normalization function.

A structural similarity index is used to measure the visual nature of stego image. The visual nature of the stego picture can be estimated by the structural similarity (SSIM) measure [16]. The SSIM is characterized as

$$\boldsymbol{SSIM}(C,S) = \ell(C,S)\cdot\zeta(C,S)\cdot\delta(C,S) \tag{31}$$

$$\ell(C,S) = \frac{2\mu_C\mu_S + b_1}{\mu_C^2 + \mu_S^2 + b_1}; \zeta(C,S) = \frac{2\sigma_C\sigma_S + b_2}{\sigma_C^2 + \sigma_S^2 + b_2}; \delta(C,S) = \frac{\sigma_{CS} + b_3}{\sigma_C\sigma_S + b_3} \tag{32}$$

Image fidelity is also used to check the robustness as given in Eq. 35:

$$IF = 1 - \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}\left(C(i,j) - S(i,j)\right)^2}{\sum_{i=0}^{M}\sum_{j=0}^{N} C(i,j) \times S(i,j)} \tag{33}$$

Further, based on various parameters, Tables 1 and 2 provide the result of stego images for the different hidden pictures of the cameraman, Airplane and Barbara, respectively.. The average performance of the 1000stego pictures generated from the entire cover and secret images selected from the USC-SIPI image database is illustrated in Table 3. Also, it proves the effectiveness of the proposed quality enhancement approach by comparing the parameters of PSNR, MSE, WPSNR, IF and SSIM "before" performing the enhancement and after enhancement. While considering the steganography methods, the visual quality plays an important

Table 1 Stego picture Quality investigation in terms of PSNR and MSE

Cover image	Hidden Image	Vernam Algorithm			LSB + PVD + EMD			Proposed		
		PSNR	MSE	WPSNR	PSNR	MSE	WPSNR	PSNR	MSE	WPSNR
Lena	Cameraman	48.132	0.999	51.369	51.637	0.445	55.147	61.448	0.031	81.589
	Airplane	47.036	1.286	55.136	50.290	0.608	57.397	61.807	0.032	80.878
	Barbara	45.588	1.795	52.718	49.419	0.743	56.138	61.722	0.032	80.732
Bell Pepper	Cameraman	48.555	0.906	57.189	51.865	0.423	58.173	61.512	0.046	77.849
	Airplane	47.448	1.170	55.174	50.518	0.577	59.723	61.696	0.042	79.296
	Barbara	45.996	1.634	52.167	49.647	0.705	60.137	61.927	0.043	78.834
Baboon	Cameraman	44.042	2.563	52.142	54.084	0.253	52.376	63.124	0.045	79.960
	Airplane	42.964	3.285	51.397	52.737	0.346	57.196	62.980	0.044	80.914
	Barbara	41.493	4.610	54.267	51.866	0.423	54.669	62.949	0.041	81.890

Table 2 Stego picture Quality investigation

Cover image	Hidden Image	Vernam Algorithm		LSB + PVD + EMD		Proposed	
		IF	SSIM	IF	SSIM	IF	SSIM
Leena	Barbara	0.746606	0.944072	0.944858	0.970474	0.999233	0.999223
	Airplane	0.747606	0.945113	0.945700	0.971474	0.999236	0.99922
	Cameraman	0.748606	0.946262	0.946779	0.972474	0.999265	0.999218
Bell Pepper	Barbara	0.755062	0.947878	0.948432	0.973402	0.998812	0.99936
	Airplane	0.756062	0.950150	0.950361	0.974032	0.998874	0.999344
	Cameraman	0.757052	0.950308	0.950483	0.975040	0.998773	0.999369
Baboon	Barbara	0.850663	0.933467	0.886584	0.974878	0.999145	0.998957
	Airplane	0.851665	0.934463	0.887701	0.975879	0.999096	0.998967
	Cameraman	0.851664	0.935501	0.888420	0.976878	0.999057	0.998978

role. Here, DESAE has been proposed for improvement. For enhancing the stego image, the proposed DESAE stacked three auto encoders. During the training phase, it reconstructs the training set features. After that, the trained DESAE model reconstructs the parts of testing images efficiently. The proposed DESAE requires only to enhance the quality of stego image 0.015 s after training.

When the PSNR value is high, the stego image holds less distortion. From the results, one can understand that the PSNR of the technique is improved than the existing method for all test cases. The image SSIM results of the proposed method show that it can embed more data with good quality. The results also show that quality of stego images of the proposed method is much better than the stego images obtained "before" performing the enhancement process. Hence, the steganography approach needs the quality enhancement approach as a post-processing step to improve the visual quality.

4.2 Payload capacity analysis

Payload capacity is the ratio of the number of covert bits installed to the total number of pixels in the cover image.

$$Payload\ capacity = \frac{number\ of\ \ secret\ bits\ embedded}{total\ number\ of\ \ pixels\ in\ cover\ image} \tag{34}$$

As we increase the hidden data capacity, the PSNR value decreases. Figure 9 presents the payload analysis of various cover images concerning the matter of PSNR. Likewise, it gives

Table 3 Average Quality and payload analysis of the 1000Stego images

Method	PSNR	WPSNR	MSE	IF	SSIM
Vernam Algorithm	45.223	52.369	1.998	0.874653	0.949751
LSB + PVD + EMD	50.777	58.136	0.501	0.931261	0.987762
Proposed without quality enhancement	58.326	63.483	0.184	0.998767	0.998463
HOG+PVD+LSB	44.824	57.476	0.447	0.997141	0.994781
DT-CWT + KNN	51.421	71.963	0.093	0.999950	0.999300
Proposed with quality enhancement	62.398	82.167	0.049	0.999742	0.999373

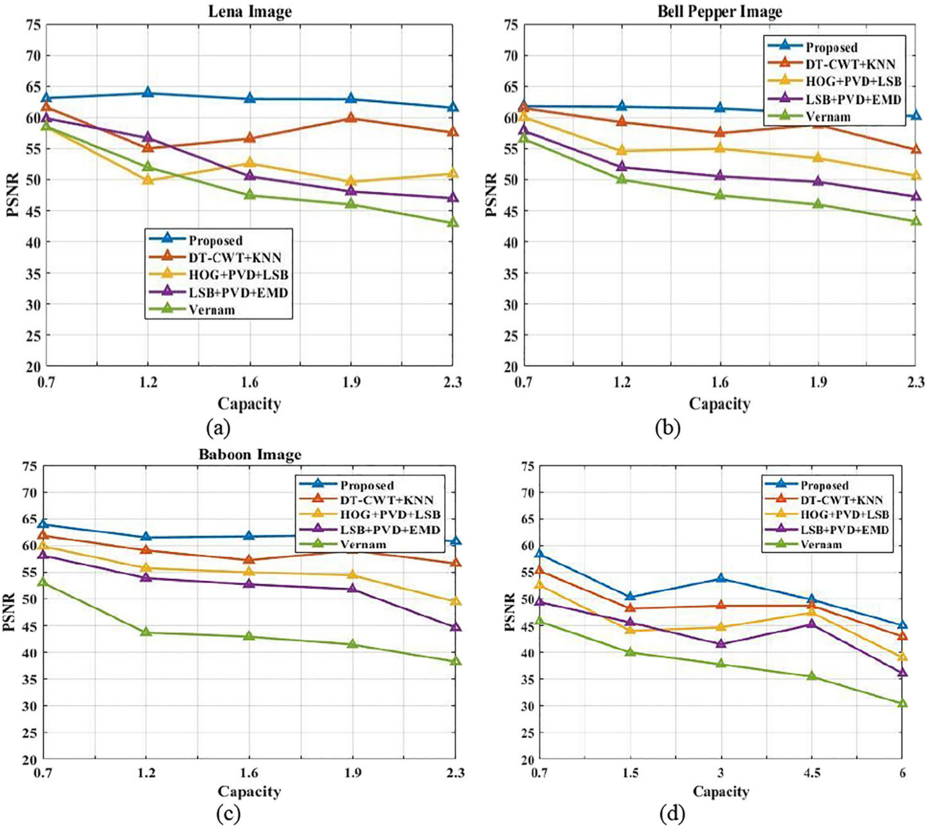


Fig. 9 Hidden capacity analysis for different cover images (**a**)-(**c**), (**d**) Average of 1000 stego images

the regular exhibition of all the 100 cover pictures by shifting the payload limit. The nature of stego picture got by the proposed strategy is suiTab. for different cover pictures. Meanwhile, the proposed conspire doesn't weaken the spirit of stego picture while expanding the payload limit. Assuming the payload limit is extended to 2.3bpp, the quality of stego images is higher than 60 dB for all experiments.

The progressions less influence the edges in the wake of concealing restricted information. Consequently, more knowledge is implanted in the edge districts utilizing higher boundary esteem. In the proposed work, the edges are distinguished dependent on the ideal thresholding technique. Subsequently, all edge pixels are recognized without losing any edge pixel. Along these lines, the payload limit is consequently improved.

4.3 Security analysis

KL divergence analysis is utilized for the security check analysis [30, 34]. This is the fundamental strategy for estimating the robustness on the grounds that it precisely gauges the contrast between two disseminations [21]. Consider H1 is the cover picture histogram and

H2 is the stego picture histogram. The accompanying articulations are utilized to appraise the K-L uniqueness from H1 to H2 and from H2 to H1.

$$KLD_1 = \sum_{i=0}^{255} H_1(i) \times log \frac{H_1(i)}{H_2(i)} \tag{35}$$

$$KLD_2 = \sum_{i=0}^{255} H_2(i) \times log \frac{H_2(i)}{H_1(i)} \tag{36}$$

Here, values of KLD$_1$ and KLD$_2$ are measured for the security evaluations. When there is no change in the cover picture and stego picture, then it means that the K-L divergence worth will be identical to nothing. The aggressors can't perceive the mysterious picture when the K-L disparity esteem is closer to nothing. Accordingly, the security level of such a steganography strategy is exceptionally high. Figure 9 shows the KL divergence analysis for various cover images.

Figure 10 indicates that the proposed method is more secure than the other techniques. This is due to the inclusion of efficient encryption algorithms for hidden images and adaptive embedding processes.

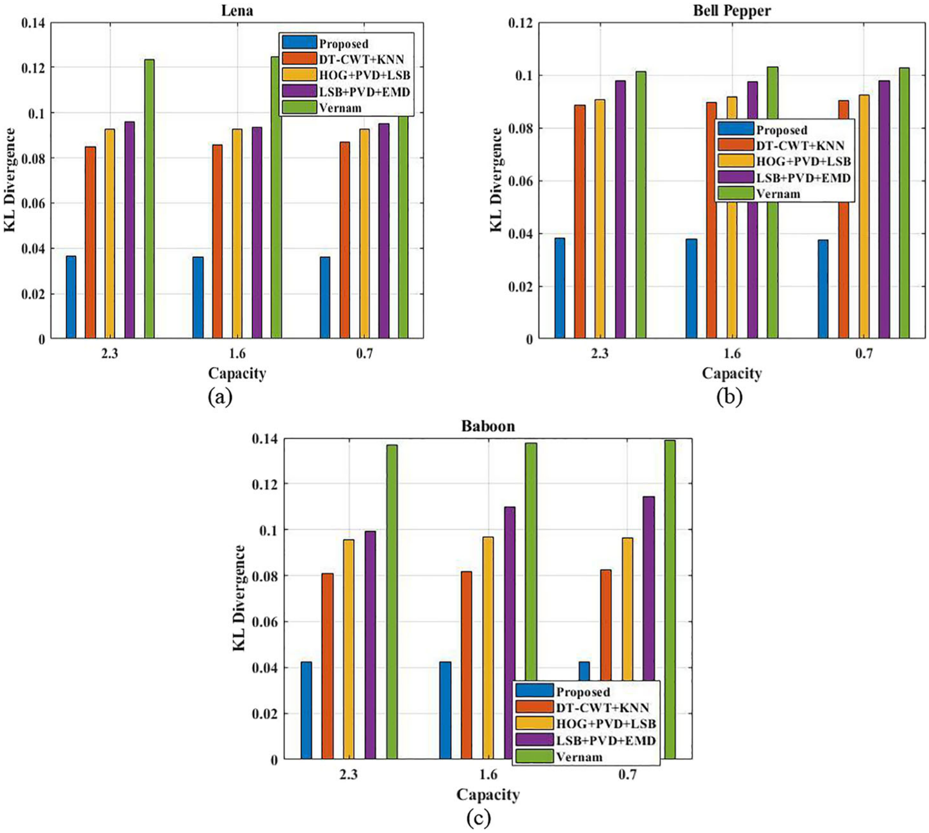


Fig. 10 Security analysis for various cover images

4.4 Robustness analysis

The encryption algorithm used for converting the hidden image into a cipher image and the wavelet domain-based steganography approach used for data hiding have been validated against the differential attack and specific image processing or manipulation attacks.

4.4.1 Differential attack analysis for the encryption algorithm

Two factors may be used to assess the influence of plain text variation on the cypher image: UACI and NPCR. If only one pixel in the main image is changed, the NPCR measure may be used to calculate the number of pixels changed in the cipher picture. If it reached 100%, then the cipher's sensitivity level to the variation in the plain image is high. Furthermore, the higher value of UACI validates the resistance of the algorithms against differential attacks. Table 4 shows the variation in UACI & NPCR.

$$\boldsymbol{NPCR} = \frac{D(C_1, C_2)}{M \times N} \times \boldsymbol{100\%} \tag{37}$$

Where

$$D(C_1, C_2) = \begin{cases} 0 \text{ if } C_1(i,j) = C_2(i,j) \\ \quad 1 \text{ otherwise} \end{cases} \tag{38}$$

$$\boldsymbol{UACI} = \frac{\boldsymbol{1}}{M \times N} \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{\boldsymbol{255}} \times \boldsymbol{100\%} \tag{39}$$

4.4.2 Robustness of the proposed steganography method against common image processing attacks

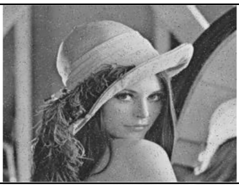
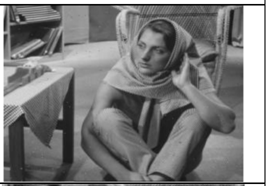
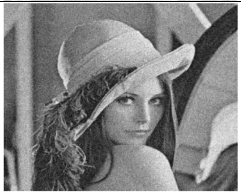
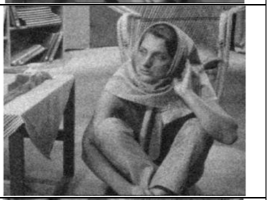
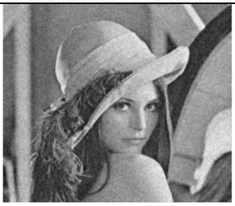
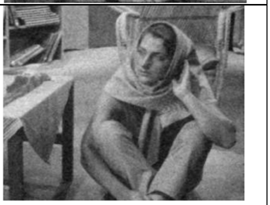
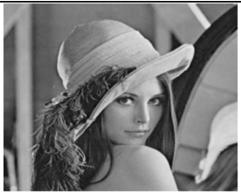
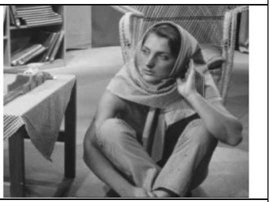
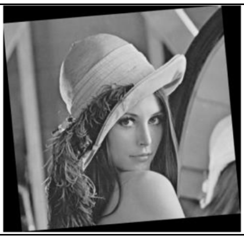
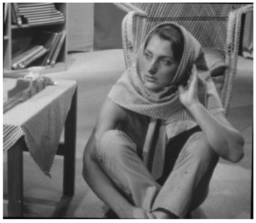
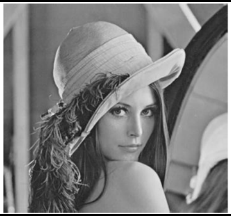
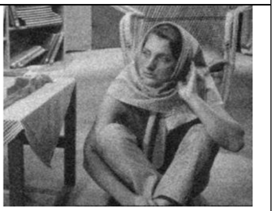
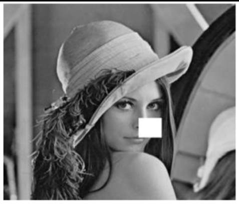
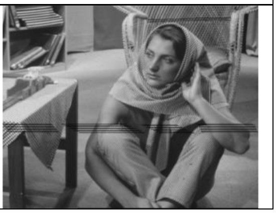
Image scathing attack The attackers can degrade the images by adding salt and pepper noise and Gaussian noise. Table 5's first and second rows show the hidden image's retrieved output from the salt and pepper and Gaussian noise assaulted images. Because of the block-based embedding strategy, the suggested method effectively recovered the concealed picture.

Image enhancement attack Some filtering techniques, such as the median filter, can be used to improve the image. The stego picture was assaulted here by using a median filter with parameters [5 × 5] and a repetition time of 10. The skeleton of the stego picture was softened using the median filter, as seen in the third row of Table 5. The suggested steganography

Table 4 Differential attack analysis of the encryption algorithm

Test image	Size	NPCR (%)	UACI (%)
Cameraman	(64×64)	99.862	36.22329
Airplane	(128×128)	99.862	36.17619
Barbara	(192×192)	99.862	36.13102

Table 5 Experimental results for various image processing attacks

Attack	Attacked stego image	Extracted secret image
Salt and pepper noise (density=0.02)		
Gaussian noise (standard deviation 0.04)		
Gaussian + Median filter (5x5)		
JPEG compression (QF=50)		
Rotation (20^0 anti-clockwise)		
Scaling (0.25 up)		
Cropping (50x50)		

approach, on the other hand, extracts the secret picture without mistake. As a result, our method is resistant to median filtering.

Image compression attack The attacker may also use the JPEG compression approach to degrade the stego image. Here, the quality factor of JPEG compression is chosen as 50. As shown in Table 5, we can observe that secret image can be extracted with high definition under this kind of attack. Hence we can say that ptoposed technique has high security.

Geometrical transformation attack A specific geometrical attack can be used to alter the form of the pictures. Certain transformations, such as rotation, scaling, and cropping, are included in this geometrical assault. The stego pictures were assaulted by these transformations, which added or removed certain pixels. The Tab. shows the stego picture that different geometrical transformations have attacked. These transformations have had a direct impact on the embedded data. By rotating the stego picture 20^0 in an anti-clockwise direction and scaling it up to 0.25 times its original size, the robustness of the suggested steganography methods against geometric attack has been demonstrated.

In addition, the cropping attack eliminates a specific area of stego pictures. Even so, the secret information may be extracted from the stego picture. As a result, our method is resistant to the Geometrical transformation attack.

In Table 5 it shows that it extracts the secret image inefficient and readable format. Table 6 shows the comparison of various image processing attacks through different algorithms of steganography.

It shows the average performance of the extracted secret images from 1000 attacked stego images. Table 6 shows that the proposed scheme delivers improved values of PSNR, WPSNR, IF and MSE for the extracted secret images even in image processing attacks. It achieved an average PSNR of 58.365%, 56.616%, 49.957%, 52.886% and 49.145% for the Salt and pepper noise, Gaussian noise, JPEG compression, Scaling and Cropping attacked stego images, respectively. This proves that the extracted secret images' quality is much improved compared to existing methods. Hence, several image processing attacks do not affect the proposed method heavily. The proposed approach can extract the hidden data without affecting their visual quality and statistical measurements when the stego image undergoes specific image manipulation attacks.

4.5 Time complexity analysis

The software setup utilized for computing the average execution time is MATLAB 2017a with a Pentium 4 GB RAM under the Windows XP operation system. Table 7 compared the average execution time of the proposed method and the existing methods, including the vernam algorithm, LSB + PVD + EMD, HoG+PVD + LSB and DT-CWT + KNN by considering the maximum payload capacity. Here, the embedding and extraction time denotes the meantime of seven grayscale images. It shows that the proposed method comes after the LSB + PVD + EMD and HoG+PVD + LSB due to incorporating the quality enhancement module in the embedding phase. The total execution time of LSB + PVD + EMD is 3.9 seconds, which is very small compared to other steganography methods due to its easiness in both embedding and extraction phases. The steganography scheme of DT-CWT + KNN takes more time for the embedding and extraction process due to the incorporation of edge

Table 6 Statistical measures of extracted secret images under different attacks

Methods	Image processing attacks	PSNR	WPSNR	IF	SSIM
Vernam Algorithm	Salt and pepper noise	42.257	50.471	0.85843	0.93962
	Gaussian noise	42.843	49.941	0.83923	0.93671
	Gaussian + median filter	41.419	48.953	0.82845	0.92745
	JPEG compression	32.510	42.844	0.78473	0.88613
	Rotation	40.583	47.995	0.81735	0.91941
	Scaling	40.128	47.294	0.82952	0.90481
	Cropping	31.743	41.940	0.77588	0.87353
LSB+PVD+EMD	Salt and pepper noise	47.368	56.652	0.91238	0.97871
	Gaussian noise	47.932	55.589	0.89812	0.97583
	Gaussian + median filter	46.508	53.844	0.88734	0.96164
	JPEG compression	37.427	48.731	0.84981	0.86568
	Rotation	47.682	53.873	0.87653	0.95618
	Scaling	45.114	54.731	0.87112	0.94329
	Cropping	36.657	47.548	0.83610	0.86254
HOG+PVD+LSB	Salt and pepper noise	41.457	55.541	0.95373	0.96783
	Gaussian noise	41.821	53.973	0.94123	0.97446
	Gaussian + median filter	40.413	52.701	0.95810	0.96025
	JPEG compression	31.982	42.916	0.87916	0.87417
	Rotation	41.772	52.793	0.91358	0.94891
	Scaling	39.981	53.978	0.92174	0.95940
	Cropping	30.929	41.872	0.82058	0.86094
DT-CWT+KNN	Salt and pepper noise	48.279	70.633	0.99901	0.98745
	Gaussian noise	48.043	66.806	0.99510	0.99118
	Gaussian + median filter	47.617	65.341	0.98411	0.97489
	JPEG compression	38.536	62.723	0.95833	0.94157
	Rotation	48.773	65.185	0.97225	0.97116
	Scaling	46.415	66.036	0.97218	0.97920
	Cropping	37.816	62.114	0.96824	0.95492
Proposed	Salt and pepper noise	58.365	77.138	0.99812	0.99856
	Gaussian noise	56.616	74.917	0.99326	0.99136
	Gaussian + median filter	55.719	73.432	0.98518	0.98464
	JPEG compression	49.957	70.834	0.97112	0.96425
	Rotation	53.721	73.715	0.98931	0.98867
	Scaling	52.886	73.412	0.98316	0.98112
	Cropping	49.145	70.881	0.97913	0.96154

detection, complex feature extraction algorithms and KNN models in the block classification. At the same time, the execution time for the Vernam Algorithm is5.3 seconds. However, the proposed approach is better than the Vernam Algorithm and DT-CWT + KNN with a total execution time of 5.0 seconds. Even though the proposed method's time complexity is slightly increased compared to LSB + PVD + EMD [29] and HoG+PVD + LSB, the quality,

Table 7 Analysis of Time complexity

Methods	Embedding time (s)	Extraction time (s)	Total time (s)
Vernam Algorithm	2.6	2.7	5.3
LSB+PVD+EMD	2.3	1.6	3.9
HoG+PVD+LSB	2.6	2.1	4.7
DT-CWT+KNN	3.5	3.8	7.3
Proposed	2.9	2.1	5.0

security, and payload capacity of the proposed method are reduced much better than all the existing methods.

4.6 Advantages & Limitation of the proposed method

- The proposed technique of such steganography strategy gives an exceptionally high-security level by combining the BBPD image encryption method and embedding phase using the frequency domain.
- This technique utilized the IDWT and SSOA technique for edge and smooth blocks of LL-sub-band by deciding the ideal edge as an incentive for keeping up with the excellent stego quality.
- This technique also gives the image encryption algorithms good resistance against differential attacks by increasing the average value of UACI is 36.17681, and NPCR is 99.862%.

The limitation of the proposed technique is that it may increase the time complexity of the proposed method.

5 Conclusion

This paper proposes a protected and new steganography structure for safe communication of covered picture. This strategy determined the picture quality, payload limit, and security of the picture steganography technique. The proposed method utilized BBPD, chaotic framework and bit-level changes to work on the protection of the mysterious picture. The proposed SSOA enhanced versatile inserting technique has chosen reasonable consideration for edge and smooth squares of LL-sub-band by deciding ideal edge an incentive for keeping up with the good stego quality. The trial result gives that the presentation is greatly improved in alternate points of view like security, payload limit and stego-picture quality. It proved the resistance of the image encryption algorithms against differential attacks by increasing the average value of UACI is 36.17681 and NPCR is 99.862%. Also, the quality and payload analysis results illustrate that the proposed method has a higher PSNR than 60 dB, even for the payload capacity of 2.3bpp in all test cases. In addition, the robustness analysis validated the resistivity of the proposed technique against other manipulation attacks or various other unknown attacks. By this process, stego image will not be observed by the unapproved attacker, and therefore the confidential image will remain safe. The proposed steganography method can also be used for hiding multiple images by considering the secret image one after another. This will further increase the time complexity to some extent. In future scope, more work can be done on proposed steganography, like steganography can be used for hiding multiple hidden image simultaneously on the cover image with respect to certain features of hidden images.

Acknowledgements This work was supported by PMU Cybersecurity Center Research Grant (PCC-Grant-202222), Prince Mohammad Bin Fahd University, Kingdom of Saudi Arabia.

Data availability The data that support the findings of this study are available from the first author upon reasonable request.

Code availability The code is available from the first author upon reasonable request.

Declarations

Conflicts of interest/competing interests The authors declare no conflict of interest.

Informed consent None.

References

1. Bailey K, Curran K (2006) Erratum: an evaluation of image based steganography methods using visual inspection and automated detection techniques (multimedia tools and applications). Multimed Tools Appl 31(3):327
2. Bhat S, Kapoor V (2019) Secure and Efficient Data Privacy, Authentication and Integrity Schemes Using Hybrid Cryptography, vol. 870. Springer, Singapore
3. Biswas C, Gupta UD, Haque MM (2019) "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2nd Int. Conf Electr Comput Commun Eng ECCE 2019, pp. 1–5
4. Bukhari S, Arif MS, Anjum MR, Dilbar S (2017) "Enhancing security of images by Steganography and Cryptography techniques," 2016 Sixth Int. Conf Innov Comput Technol (INTECH), 2016, pp. 531–534. https://doi.org/10.1109/INTECH.2016.7845050
5. Chauhan S, Jyotsna KJ, Doegar A (2017) "Multiple layer text security using variable block size cryptography and image steganography," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), 2017, pp. 1–7. https://doi.org/10.1109/CIACT.2017.7977303
6. Cogranne R, Giboulot Q, Patrick B (2021) Efficient Steganography in JPEG Images by Minimizing Performance of Optimal Detector, in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1328–1343, 2022. https://doi.org/10.1109/TIFS.2021.3111713
7. Dhar PK, Kaium A, Shimamura T (2018) Image Steganography Based on Modified LSB Substitution Method and Data Mapping. Int J Comput Sci Netw 18(3):155–160
8. Dhawan S, Gupta R (2019) "Comparative Analysis of Domains of Technical Steganographic Techniques," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 885–889
9. Dhawan S, Gupta R (2020) Analysis of various data security techniques of steganography : a survey. Inf Secur J A Glob Perspect 30(2):1–25
10. Dhawan S, Gupta R (2021) High-quality steganography scheme using hybrid edge detector and Vernam algorithm based on hybrid fuzzy neural network. Concurr Comput Pract Exp John Wiley Sons, Inc. 33(17):e6448
11. Dhawan S, Chakraborty C, Frnda J, Gupta R, Rana A, Pani S (2021) SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. IEEE Access 9:1–1
12. Febryan A, Purboyo TW, Saputra RE (2017) Steganography methods on text, audio, image and video: a survey. Int J Appl Eng Res 12(21):10485–10490
13. Geng J, Li W-CHM-W, Wang Y-T (2021) Chaos cloud quantum bat hybrid optimization algorithm. Nonlinear Dyn, Springer 103:1167–1193
14. Hameed MA, Hassaballah M, Aly S, Awad AI (2019) An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques, in IEEE Access, vol. 7, pp. 185189–185204, 2019, https://doi.org/10.1109/ACCESS.2019.2960254
15. Hasheminejad A, Rostami MJ (2019) A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. Optik (Stuttg) 184(March):205–213
16. Horé A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. Proc - Int Conf Pattern Recognit:2366–2369
17. Hosam O (2019) Attacking Image Watermarking and Steganography - A Survey, International Journal of Information Technology and Computer Science(IJITCS), Vol.11, No.3, pp.23–37, 2019. https://doi.org/10.5815/ijitcs.2019.03.03
18. Irfan P, Prayudi Y, Riadi I (2015) Image encryption using combination of chaotic system and Rivers Shamir Adleman (RSA). Int J Comput Appl 123(6):11–16
19. Juhi S; Mukesh S (2021) "A Novel Method of high-Capacity Steganography Technique in Double Precision Images," in 2021 International Conference on Computational Performance Evaluation (ComPE)
20. Kadhim IJ, Premaratne P, Vial PJ (2020) High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cogn Syst Res 60:20–32
21. Kapoor R, Gupta R, Son LH, Jha S, Kumar R (2018) Boosting performance of power quality event identification with KL Divergence measure and standard deviation, Measurement, Volume 126, 2018, Pages 134-142, https://doi.org/10.1016/j.measurement.2018.05.053. (https://www.sciencedirect.com/science/article/pii/S0263224118304433)

22. Kovalchuk A, Izonin I, Gregush MM, Lotoshynska N (2019) An approach towards image encryption and decryption using quaternary fractional-linear operations. Procedia Comput Sci 160:491–496
23. Kovalchuk A, Izonin I, Gregush MM, Kustra N (2019) Information protection service using topological image coverage. Procedia Comput Sci 160:503–508
24. Kovalchuk A, Izonin I, Gregush MM, Riznyk O (2019) An efficient image encryption scheme using projective transformations. Procedia Comput Sci 160:584–589
25. Kumar V, Kumar D (2018) A modified DWT-based image steganography technique. Multimed Tools Appl 77(11):13279–13308
26. Kumar S, Dhaka V, Nolkha A (2019) Image Steganography Using LSB Substitution: A Comparative Analysis on Different Color Models. In: Smart Systems and IoT Innovations Computing. Springer, Singapore, pp 711–718
27. Liao X, Yu Y, Li B, Member S (2019) "A New Payload Partition Strategy in Color Image Steganography," IEEE Trans. Circuits Syst. Video Technol, vol. PP, no. c, p. 1
28. Mirjalili S, Gandomi AH, Mirjalili SZ, Saremi S, Faris H, Mirjalili SM (2017) Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems, Advances in Engineering Software, Volume 114, 2017, Pages 163–191, https://doi.org/10.1016/j.advengsoft.2017.07.002. (https://www.sciencedirect.com/science/article/pii/S0965997816307736)
29. Nipanikar SI et al (2018) A sparse representation based image steganography using particle swarm optimization and wavelet transform. Int J Comput Appl 771(4):2343–2356
30. Pradhan A, Sahu AK, Swain G, Sekhar KR (2016) "Performance evaluation parameters of image steganography techniques," Int Conf Res Adv Integr Navig Syst RAINS 2016, no. May 2018
31. Punyani P, Gupta R, Kumar A (2019) Neural networks for facial age estimation : a survey on recent advances. Artificial Intelligence Review, Springer, Netherlands
32. Saleh FAO, Marwa E, Abdelmgeid A, Aly (2016) Data security using cryptography and steganography. Int J Adv Comput Sci Appl 7(06):390–397
33. Sharma VK, Srivastava DK (2017) Comprehensive data hiding technique for discrete wavelet transform-based image steganography using advance encryption standard. Lect Notes Networks Syst 12:353–360
34. Song H, Tang G, Sun Y, Gao Z (2019) Security security measure for image steganography based on high dimensional KL divergence, Security and Communication Networks, vol. 2019, Article ID 3546367, 13 pages, 2019. https://doi.org/10.1155/2019/3546367
35. Tan J, Liao X, Liu J, Cao Y, Jiang H (2022) Channel attention image steganography with generative adversarial networks. IEEE Trans Netw Sci Eng 9(2):888–903
36. Veerashetty S, Patil NB (2019) "Manhattan distance-based histogram of oriented gradients for content-based medical image retrieval," Int J Comput Appl, 43(9):924–930, https://doi.org/10.1080/1206212X.2019.1653011
37. Vishwas GK, Kini GNG (2019) "A Secured Steganography Algorithm for Hiding an Image in an Image," Integr Intell Comput Commun Secur Stud Comput Intell, pp. 539–546
38. Zhang J, Zhao X, Xiaolei H, Zhang H (2021) Improving the robustness of JPEG steganography with robustness cost, in IEEE Signal Processing Letters, 29:164–168, 2022, https://doi.org/10.1109/LSP.2021.3129419
39. Zichen Zhang WCH (2021) "Application of variational mode decomposition and chaotic grey wolf optimizer with support vector regression for forecasting electric loads," Knowledge-Based Syst, vol. 228

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

Affiliations

Sachin Dhawan[1] **· Rashmi Gupta**[2] **· Hemanta Kumar Bhuyan**[3] **· Ravi Vinayakumar**[4] **· Subhendu Kumar Pani**[5] **· Arun Kumar Rana**[1]

Sachin Dhawan
ersachind@gmail.com

Rashmi Gupta
rashmi.gupta@nsut.ac.in

Hemanta Kumar Bhuyan
hmb.bhuyan@gmail.com

Subhendu Kumar Pani
skpani.india@gmail.com

Arun Kumar Rana
ranaarun1@gmail.com

[1] Panipat Institute of Engineering and Technology, Samalkha, India

[2] NSUT East Campus, Geeta Colony, Delhi, India

[3] Department of Information Technology, Vignan's Foundation for Science, Technology and Research (Deemed to be University), Kurnool, Andhra Pradesh, India

[4] Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar 34754, Saudi Arabia

[5] Krupajal Computer Academy, Biju Patnaik University of Technology, Bhubaneswar, Odisha, India