



A Novel Image Steganography Method using Optimal Pixel Selection with Discrete Wavelet Transform

Sivasankari,
Research Scholar,
Department of Computer Science,
Pioneer College of Arts and Science,
Coimbatore, Tamil Nadu, India.
shivashankari.may28@gmail.com

Krishnaveni Sakkarapani,
Assistant Professor,
Department of Computer Science,
PSGR Krishnammal College for Women,
Coimbatore, Tamil Nadu, India.
sss.veni@gmail.com

Abstract

Data security comprises of concealing secret image, documents, audio or video on any other files with an intention of preserving the secret data from the attacker. Several works available in the literature reported that the steganography have the risk of secret information being repossessed by an unidentified person. Therefore, an effective encryption-based image steganography technique is essential. This paper presents a new Optimal Pixel Selection with Discrete Wavelet Transform (DWT) based Image Steganography Method called OPSDWT-ISM. The presented OPSDWT-ISM model involves both encryption and steganography processes. Primarily, the discrete wavelet transform (DWT) technique is applied for the image decomposition process. Afterward, the optimal pixel points will be chosen using butterfly optimization algorithm (BOA). At the same time, the secret image is also decomposed into three individual R, G, and B elements which are then encrypted using data encryption standard (DES), blowfish, and Arnold cat map techniques respectively. Finally, the encrypted images are embedded to the chosen pixel points of the cover image. At the receiver side, inverse DWT process is employed followed by decryption and extraction for the retrieval of secret image. A detailed experimentation analysis showcased the betterment of the presented model over the existing methods under distinct dimensions.

Keywords: Data security, Steganography, Encryption, DWT, Pixel selection

DOI Number: 10.14704/nq.2022.20.8.NQ44374

NeuroQuantology 2022; 20(8): 3482-3495

1.

Introduction

Steganography is defined as the process of fabricating the computerized information to the cover media [1]. The cycle of authentication includes cryptographic methodology, hashing, digital signature, or set a fixed value to embed secret data [2]. The advancements of the Internet advancements regarding digitalization prompt increasing the information sharing utilization. Indeed, there are numerous effective and highly secure

techniques are available, and there is a movement to guarantee the security of the method regarding its presentation. Image steganography is applied in various applications like communication, internet relied vote casting, appropriate secure image recovery as well as security of clinical records [3]. Data encryption is alluded to as cryptography which transforms the secret data so it isn't perceptible by third parties [4]. Security is the essential challenge in the



present digital world and hiding a secret data from interlopers and programmers turned into a troublesome process [5].

Developers have not considered the issues in steganography, and when cover image measurements are imbalanced to generate image blocks to incorporate in performing data concealing and eliminate various factors of stego assaults. Subsequently, some extra methods should be utilized, for example, alterations to minimal pixel counter change coefficients, utilization of encoded form of secret message to be inserted and so forth. In this strategy, embed secret message in the records is moved to the client at the opposite end, where the message is unhidden [6]. In spite of the fact that there is a lot of programming accessible online for information security, there is a lot other programming that is being used by programmers to decode the concealed information [7].

Atee et al. [8] expressed an image steganography approach that demonstrated viable execution, in which the modification was presented in an extreme learning machine (ELM) calculation to make an effective technique. Prior to validation process, the ELM calculation on any regression technique, it was first tried separated from an image. This prompted the determination of ideal area to message with optimal positions correlated in anticipated performance metrics. The experimental assessment of the altered ELM was directed through the calculation of correlation, SSIM, etc. Douglas et al. [9] indicated the new steganography model utilized in making sure about biometric information as to fingerprints. The investigation assessed the preferences and hindrances of focused just as blind steganalysis to break steganography. The fundamental benefit is distinguishing individuals dependent on their biometric information, which has received more attention. To ensure additional assurance and security of the data, watermarking and steganography procedures have additionally been executed. On account of watermarking, the data is installed into a transporter, for security reasons, while steganography alludes

to the craft of concealing fundamental information.

Duan et al. [10] presented a coverless image steganography procedure which depends upon a generative method. The confidential image is implanted with a data base from generative model and develop independent image that has affected the private image. Next, the confidential image is shipped off beneficiary and included the database to compare the secret image. This plan was contrasted with the customary plan, where the image that was moved didn't contain any secret information in the image so that steganalysis apparatuses were adequately limited. Priyanka et al. [11] introduced a new steganography technique where a secret image is inserted to the secret text, which undergo additional encryption with an individual cover image. The embedding of the secret textual data is made on a spatial domain utilizing the Least Significant Bit (LSB) strategy which produced a stego portion. Since spatial domain techniques are susceptible against programmers; the secret content information was encoded utilizing the Advanced Encryption Standard (AES) calculation for security reasons. The Lifting Wavelet Transform (LWT) and Dual-Tree Complex WT(DTCWT) were utilized for image payload just as different sections of the cover image, separately. For image embedding, the coefficient substitution and versatile scaling techniques were actualized, for attaining the stego images. Next to the embed stage, a similar degree of strength and security was seen alongside acceptable signal-to-noise ratio (SNR) and relationship coefficient value; consequently, it guaranteed reduced capacity characteristic. For limiting the least square representation (LSR) issue proficiently, gray wolf optimization (GWO) based Face image super-resolution (FSR) (FSR-GWO) methodology is proposed. For making the searching task for compatible with the FSR, the upper and lower boundaries are defined in [12].

This paper presents a new Optimal Pixel Selection with Discrete Wavelet Transform (DWT) based Image Steganography Method named OPSDWT-ISM. The presented



OPSDWT-ISM model comprises encryption and steganography processes. Principally, the discrete wavelet transform (DWT) method is used for the image decomposition process. Subsequently, the greater pixel points might be referred under the application of butterfly optimization algorithm (BOA). Meantime, the secret image is decayed as 3 different R, G, and B components which are encrypted with the help of DES, blowfish, and Arnold cat map methodologies correspondingly. Lastly, the encrypted images are embedded to the chosen pixel points of the cover image. At the receiver side, inverse DWT process is employed followed by decryption and extraction for the retrieval of secret image. A comprehensive validation exhibits the

betterment of the presented model over the existing methods under distinct dimensions.

2. The Proposed OPSDWT-ISM model

The workflow involved in the projected OPSDWT-ISM model is displayed in Fig. 1. The figure shows that an input cover image is decomposed under the application of DWT method and maximum pixel points are decided using BOA. Additionally, the confidential images are portioned as R G B units. At last, the encrypted images are embedded to the picked pixel points in the cover image. At the receiver side, inverse DWT process is employed followed by decryption and extraction for the retrieval of secret image.

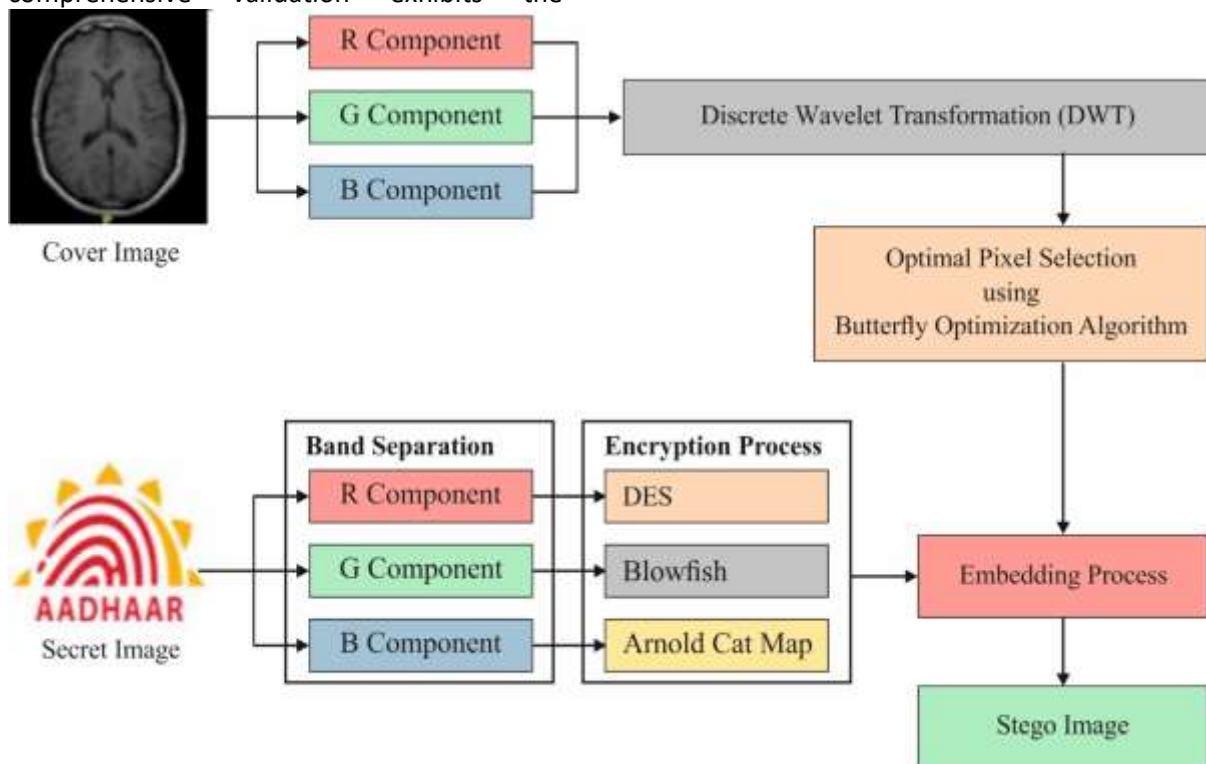


Fig. 1. Block diagram of OPSDWT-ISM model

2.1. Image Decomposition

The cover image is divided as R, G and B units [13]. In RGB mode, the cover image has been isolated according to the LL, LH, HL and HH subbands for estimating the pixels' location. A process in multilevel DWT is illustrated in Fig. 2. The 2-D DWT are essential spatial fields in frequency field transformation mechanism. A splitting is completed using 2 operations like Horizontal and Vertical processes. Initially, horizontal process decomposes the image as Low L and H bands. Afterward, the vertical

function reduces the image as LL_1, LH_1, HL_1 and HH_1 frequency bands. Afterwards, LL_1 band is again mitigated as $LL_2, LH_2, HL_2,$ and HH_2 . Then, consider the image size as $M \times N$. At the initial stage, filter and down sample is applied while horizontal decay mitigates the image into $M \times \frac{N}{2}$ size. The vertical one limits the instance of image as $\frac{M}{2} \times \frac{N}{2}$. The single-level decay results are attained from:



$$= \text{DWT}(d) \quad [d_1 d_2 d_3 d_4] \quad (1)$$

where 'd₁', 'd₂', 'd₃', and 'd₄' indicates the coefficient measures of decay frequency bands. 'd₁' shows L band as illustrated in the following:

$$= \text{DWT}(d) \quad [d_1^{LL1} d_1^{LH1} d_1^{HL1} d_1^{HH1}] \quad (2)$$

A coefficient in low frequency band d₁^{LL1} is decomposed again as it is capable of providing

the texture and edge-based data of an image. Alternatively, level of decomposition is implemented on low band LL₁ which is defined in the following:

$$= \text{DWT}(LL) \quad [d_1^{LL2} d_1^{LH2} d_1^{HL2} d_1^{HH2}] \quad (3)$$

where d₁^{LL2} depicts the low-level frequency band of 2-level decomposition.

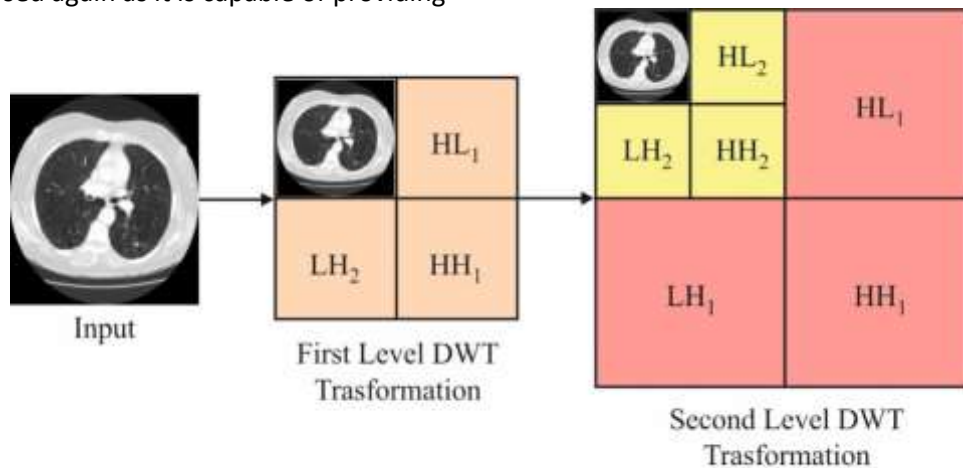


Fig. 2. Multilevel DWT transformation

2.2. BOA based Pixel Selection

Once the cover image is completely decomposed by DWT, the BOA is executed to find out the optimum pixel points in the cover image, which will be helpful for the embedding phase. BOA is defined as novel nature-based metaheuristic approach implied by Arora [14]. It depends upon food-foraging principle of butterflies (BFs). Butterflies use the sense receptors to sense and find the food source. It is named as chemoreceptors which are applicable to predict the aroma and it is scattered on the entire body of the BF. In BOA, the BFs are facilitated as searching agents that computes the optimization task. The produced fragrance of a BF denotes the fitness of a BF. It refers that of a BF modifies its position, the fitness or fragrance might also be changed. Followed by, if a BF predicts voluminous fragrance secreted by other BF, then its files toward that BF which is so called as global search. Alternatively, when a BF is unable to predict the fragrance, then it moves randomly which is named as local search phase.

In order to learn the modulation, sensing task is processed by predicting sound, aroma, heat, light is computed by a stimulus of a living object. The entire concept of predicting and computing the modality depends upon 2 effective norms namely, sensory modality (c), stimulus intensity (I) and power exponent (a). The sensory modality is defined as concepts based on calculating the power and compute them. Stimulus intensity is defined as a magnitude of physical and actual stimulus. In BOA, stimulus intensity is related with fitness of BF or solution. It refers that if a BF is generating massive aroma then other BFs could sense and attracted to the respective direction. Power is an exponent to intensity. The basic nature of BFs depends upon 2 essential factors: the difference of I and formulation of f. Hence, f is relative and it is sensed by all other BFs. Under the application of these models, the fragrance is defined as a function of external intensity of stimulus in the following:

$$= cI^a \quad f \quad (4)$$



where f denotes the attained magnitude of a fragrance.

In BOA, there are 2 phases namely, Global search phase as well as Local search phase. Initially, BF moves forward to the optimal BF or solution g^* as depicted in the following:

$$x_{i,t+1} = x_i^t + \text{Lévy}(\lambda) \times (g^* - x_i^t) \times f_i \quad (5)$$

where x_i^t signifies a solution vector x_i for i thBF in iteration value t . In this approach, g^* indicates the recent optimal solution from recent iteration. F_i indicates the aroma of i thBF, and λ refers the step size. Fig. 3 shows the flowchart of BOA technique.

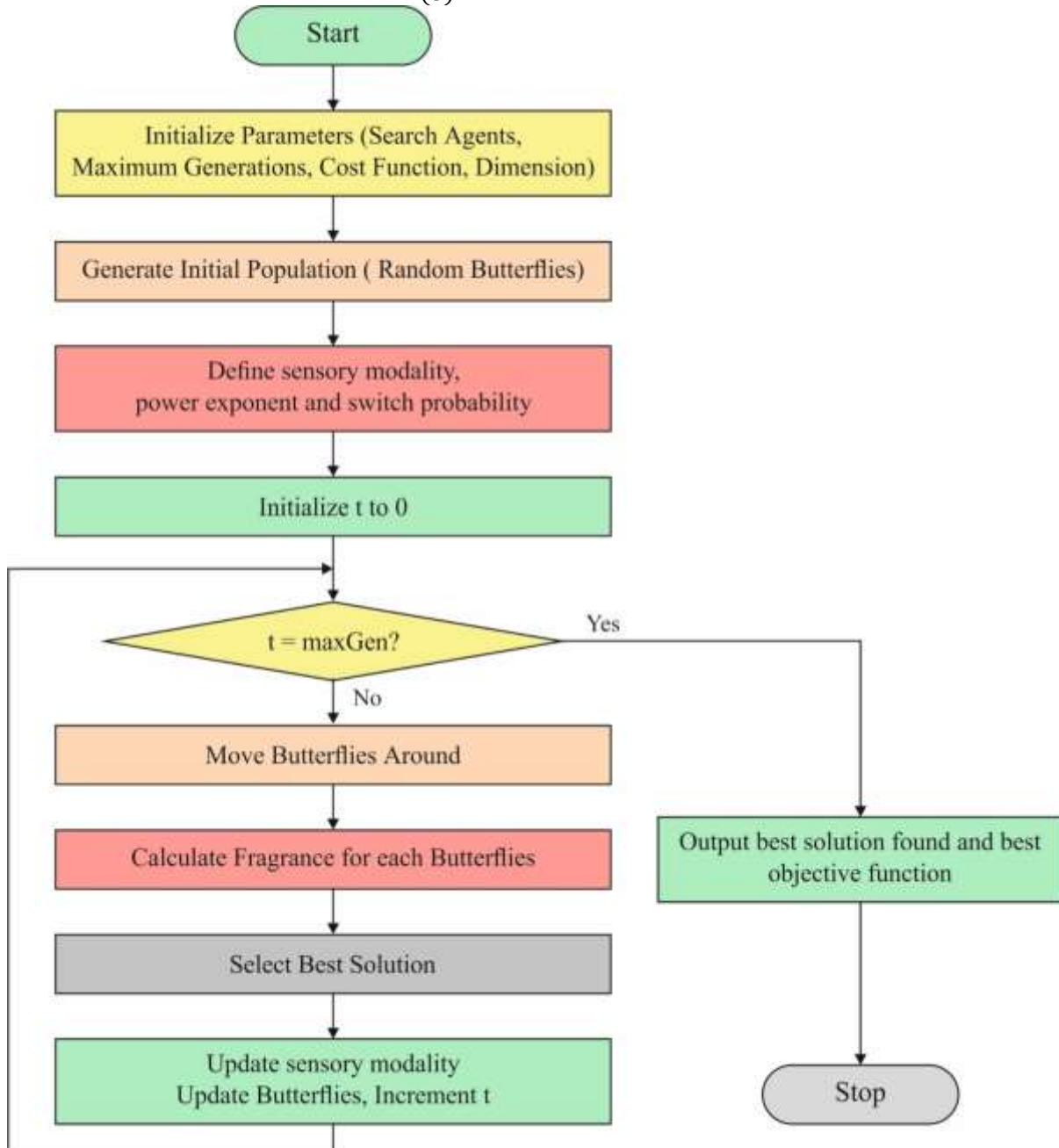


Fig. 3. Flowchart of BOA

Local search phase is illustrated as,

$$x_{i,t+1} = x_i^t + \text{Lévy}(\lambda) \times (x_j^t - x_k^t) \times f_i \quad (6)$$

where x_j and x_k implies arbitrarily selected BF from a solution space. When x_j and x_k belongs to sub-swarm and λ denotes a step size, while Eq. (7) is considered as stochastic function for random walk.

$$\text{Lévy} \sim u = t^{-\lambda}, (1 < \lambda \leq 3), \quad (7)$$



The steps of BF are developed as random walk operation which depends upon the power-law step-length distribution in conjunction with heavy tail and indefinite variance and infinite mean are presented. The application of Lévy flights in movement of BFs enhances the local search by making novel solutions over the optimal solutions generated.

Searching for food and mating partner in BFs exist in local as well as global search. By assuming physical proximity and alternate aspects such as rain, wind, searching for food have essential fraction p in food- or mating partner-searching function of BFs. Thus, a switch probability p has been applied in BOA to move from global to local search significantly. Hence, the above key steps (global and local) as well as switch condition are consolidated in a pseudo code as depicted in Algorithm 1.

2.3. Image Encryption

In this stage, the secret image is converted as RGB components more significantly and three individual encryption techniques such as DES, blowfish, and Arnold cat map are applied to encrypt it. Encrypting RGB units make sure the security of embedding principle.

2.3.1. 'R' encryption using DES

At this point, the R elements in secret image undergoes encryption with the help of DES. It shows a symmetric-key block cipher which was originated by National Institute of Standards and Technology (NIST). In this application, encryption, decryption has been identified in set of blocks. In case of encryption, DES is composed of 64-bit plaintext and make them are 64-bit ciphertext along with 16 steps named round key. Encryption has 2 phases namely, permutations (P-boxes), where primary and secondary permutations have maximum Feistel rounds. Every round applies diverse 48-bit round key originated from a cipher key [15].

These permutations are performed in 64-bit input and permutes on the basis of predefined rule. The straight and keyless permutations are converse by default. Followed by, left as well as right plain texts are re-formed and the inversion of initial

permutation results in consequent permutation.

The strategy of encryption model in DES computes 56 bits by excluding parity bits in the following:

$$\text{ciphertext} = (E_K(\text{plaintext})) \quad (8)$$

This refers that DES is capable of encrypting a plaintext with K. Decryption of inverse K is illustrated as:

$$\text{Plaintext} = (D_K(\text{ciphertext})) \quad (9)$$

2.3.2. 'G' encryption using Blowfish

Here, the G components of the secret image are encrypted using Blowfish technique. It is defined as a symmetric encryption method [16] which is composed of a single key applied for encryption and decryption operations. When the range of key is 448 bits, then it requires 2448 groupings for defining all other keys. Moreover, the key has a permanent 64-bit block size along with variable length key block cipher. Here, cipher is often a 16-round Feistel system which applies password-based S-boxes for developing the structure of encryption and decryption.

There are 2 major sub-key groups such as P-boxes (permutation boxes) applied in computing bit-shuffling and S-boxes (substitution boxes) used for computing simple nonlinear functions. In this framework, S-boxes gains 8-bit as input and attained 32-bit output. The function F is defined as Feistel Function of Blowfish which divides 32-bit block into 8-bit segments which is then induced as input for S-box. Inversely, the decryption task is processed by reversing blowfish method which is conducted by inverting P_{17} and P_{18} ciphers blocks and by using P-entries in converse order. It is classified into 2 classes namely, key-expansion as well as data encryption.

Key-expansion: Here, a 448-bit key has been transformed as various sub-key groups of 4168 bytes. Generally, P-array has 18 as well as 32-bit sub-keys (P_1, P_2, \dots, P_{18}) and 32-bit S-Boxes, have 256 entries.

The steps involved in key expansion are provided in the following:



Step1: Fix and allocate S-box and P-box with values from hexadecimal numbers of pi (< *initial 3*)

Step2: The variable length of user input key is XOR^{ed} along with P-entries till the P-array is XOR^{ed} using input key bits.

Step3: A block of 0s are encrypted; and simulations are used for P₁ and P₂ entries.

Step4: Then, encrypt a ciphertext gained from encrypted zero block, and applied for P3 and P₄.

Step5: Repeat the process until every P-box entry and S-box entry is changed; and numerous iterations are essential to produce the required sub-keys.

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{N} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{N} \quad (10)$$

where N implies the size of an image, p and q denotes positive integer and det(A) = 1. (x_n, y_n) refers the position of instances in N × N data in which image is represented as (x_n, y_n) ∈ {0, 1, 2, ..., N - 1}

Followed by, (x_{n+1}, y_{n+1}) defines transformed position of a cat map. It is composed of 2 common factors which refers the chaotic actions, tension as well as fold.

Eq. (10) is applied to change the pixel coordinates of an image. If all coordinates are changed, the image is resembled as scrambled one. Additionally, when the resulted image has attained anticipated

Data-Encryption: It is performed by 16 iterations. Furthermore, a round computes key-related permutation as well as key- and data-based substitution by applying XORs. In addition, excess processes are computed on 32-bit words. Blowfish sums the features as effective and dominant models are depicted in the following.

2.3.3. 'B' encryption using Arnold cat map

The B components in the secret image are encrypted using Arnold cat map technique. Therefore, when the iteration is processed, actual image is appeared again. The count of iterations is named as Arnold's period. It is relied on image size and it is varied from [17]

destination then the ordered scrambled image is attained. Also, image decryption depends upon transformation periods.

3. Experimental Evaluation

This section validates the performance of the OPSDWT-ISM model on the applied benchmark images in terms of distinct aspects. The visualization of the results offered by the OPSDWT-ISM model is shown in Fig. 4. The images in Fig. 4a depict the cover image, the secret data is displayed in Fig. 4b and the stego image is depicted in Fig. 4c.

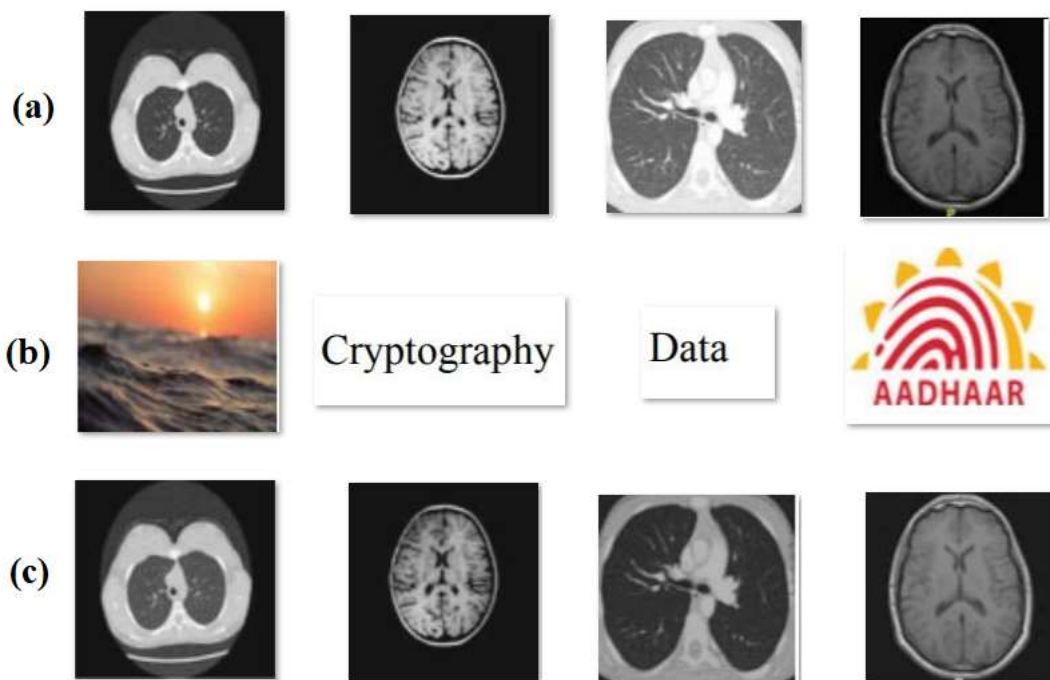


Fig. 4. a) Cover image b) Secret Information c) Stego Image

Table 1 also investigates the analysis of the results attained by the OPSDWT-ISM model with respect to PSNR, BER, and hiding capacity. From the table, it is noticed that the OPSDWT-ISM model has reached to a better performance by achieving higher PSNR and hiding capacity with minimal BER. The first row denotes that the stego image has resulted to a higher PSNR of 57.34dB and hiding capacity of 83.27bytes with the minimum BER of 0.053. In the same way, the second row refers that the stego image has

resulted to a maximum PSNR of 59.62dB and hiding capacity of 91.73bytes with the minimum BER of 0.221. Along with that, the third row indicates that the stego image has resulted to a superior PSNR of 59.02dB and hiding capacity of 86.9bytes with the minimum BER of 0.075. Concurrently, the fourth row refers that the stego image has resulted to a higher PSNR of 54.87dB and hiding capacity of 93.65bytes with the minimum BER of 0.110.

Table 1 Performance Analysis for Proposed OPSDWT-ISM Image Security




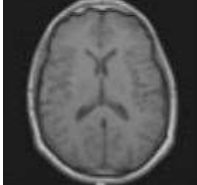
Stego image	PSNR (dB)	BER	Hiding capacity (byte)
	57.34	0.053	83.27
	59.62	0.221	91.73
	59.02	0.075	86.90
	54.87	0.110	93.65

Table 2 examines the results attained by the OPSDWT-ISM model in terms of PSNR and BER under the salt and pepper attack and brute force attack. The decrypted stego image is shown in the table along with the respective PSNR and BER values. The first row indicates that the OPSDWT-ISM model has attained a PSNR of 43.88dB and BER of 0.110 under salt

and pepper attack whereas PSNR of 47.90dB and BER of 0.267 have been achieved under brute force attack. Likewise, the second row indicates that the OPSDWT-ISM model has achieved a PSNR of 42.9dB and BER of 0.421 under salt and pepper attack while PSNR of 39.45dB and BER of 0.642 have been attained under brute force attack. In line with, the



third row denotes that the OPSDWT-ISM model has obtained a PSNR of 43.16dB and BER of 0.298 under salt and pepper attack whereas PSNR of 35.21dB and BER of 0.710 have been obtained under brute force attack.

Also, the fourth row refers that the OPSDWT-ISM model has achieved a PSNR of 45.32dB and BER of 0.327 under salt and pepper attack whereas PSNR of 33.08dB and BER of 0.265 have been reached under brute force attack.

Table 2 Result analysis of proposed method in terms of attacks


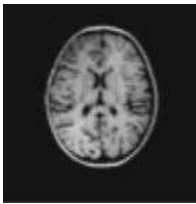
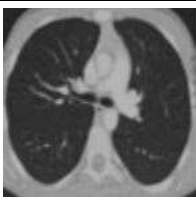

Decrypted stego image	Salt and pepper attack		Brute force attack	
	PSNR	BER	PSNR	BER
	43.88	0.110	47.90	0.267
	42.90	0.421	39.45	0.642
	43.16	0.298	35.21	0.710
	45.32	0.327	33.08	0.265

Table 3 and Fig. 5 investigate the PSNR analysis of the OPSDWT-ISM model on the distinct set of images [18, 19]. The resultant values indicated that the OPSDWT-ISM model has reached to a higher PSNR value on all the applied test images. For instance, on the applied test image 1, the OPSDWT-ISM model has obtained a higher PSNR of 57.34dB whereas the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have achieved a lower PSNR values of 38.70dB, 43.40dB, 50.03dB, 51.30dB, and 55.65dB respectively. Likewise, on the applied test image 2, the OPSDWT-ISM model has attained a maximum PSNR of 59.62dB but the Harr-

SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have attained a lower PSNR values of 43.50dB, 53.55dB, 56.88dB, 57.98dB, and 58.48dB correspondingly. Along with that, on the applied test image 3, the OPSDWT-ISM model has obtained a superior PSNR of 59.02dB while the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have reached a lower PSNR values of 46.67dB, 42.70dB, 52.44dB, 54.30dB, and 58.30dB correspondingly. Eventually, on the applied test image 4, the OPSDWT-ISM model has attained a maximum PSNR of 54.87dB whereas the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have



achieved a lower PSNR values of 37.90dB, correspondingly, 39.80dB, 47.77dB, 48.42dB, and 52.19dB

Table 3 Comparative analysis of existing with proposed in terms of PSNR

Test Images	Harr-SSC	db2-SSC	Optimal db2-SSC	FFOA	GACFFOA	OPSDWT-ISM
Image 1	38.70	43.40	50.03	51.30	55.65	57.34
Image 2	43.50	53.55	56.88	57.98	58.48	59.62
Image 3	46.67	42.70	52.44	54.30	58.30	59.02
Image 4	37.90	39.80	47.77	48.42	52.19	54.87

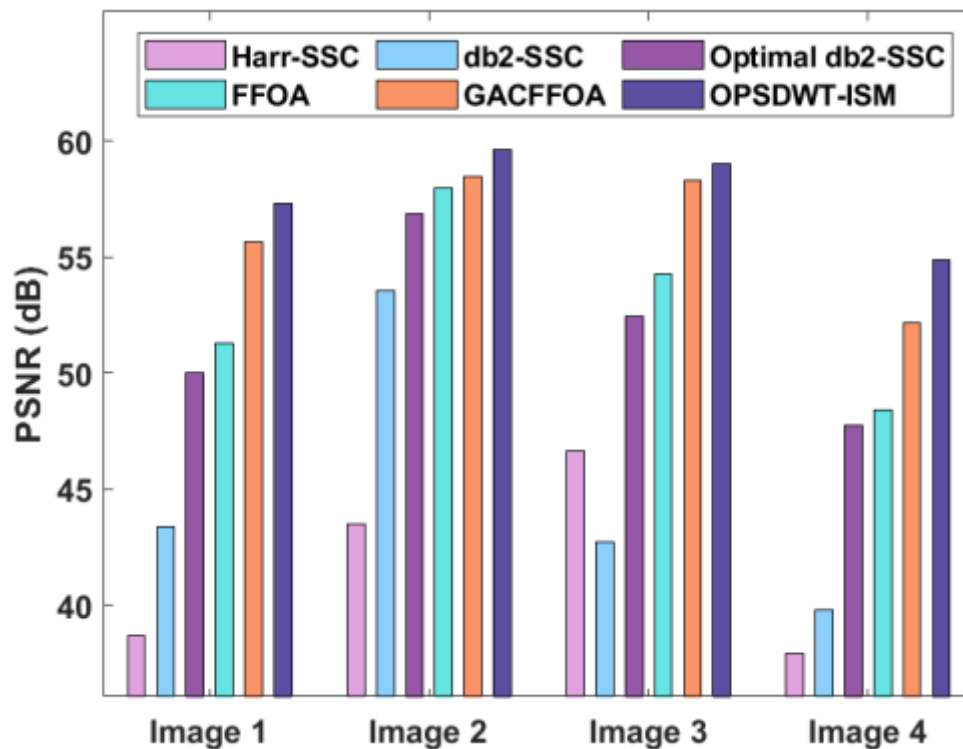


Fig. 5. PSNR analysis of OPSDWT-ISM model

A BER analysis of the presented OPSDWT-ISM model with the existing techniques on the different images is demonstrated in Table 4 and Fig. 6. The BER values signified that the OPSDWT-ISM model has exhibited effective outcome through the achievement of minimum BER values. For instance, on the

applied image 1, the OPSDWT-ISM model has accomplished effective outcome with the least BER of 0.053 whereas the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have reached a higher BER values of 0.571, 0.562, 0.088, 0.076, and 0.063 respectively.

Table 4 Comparative analysis of existing with proposed in terms of BER

Test Images	Harr-SSC	db2-SSC	Optimal db2-SSC	FFOA	GACFFOA	OPSDWT-ISM
Image 1	0.571	0.562	0.088	0.076	0.063	0.053



Image 2	0.713	0.813	0.456	0.321	0.243	0.221
Image 3	0.821	0.912	0.124	0.109	0.101	0.075
Image 4	0.967	0.836	0.213	0.156	0.124	0.110

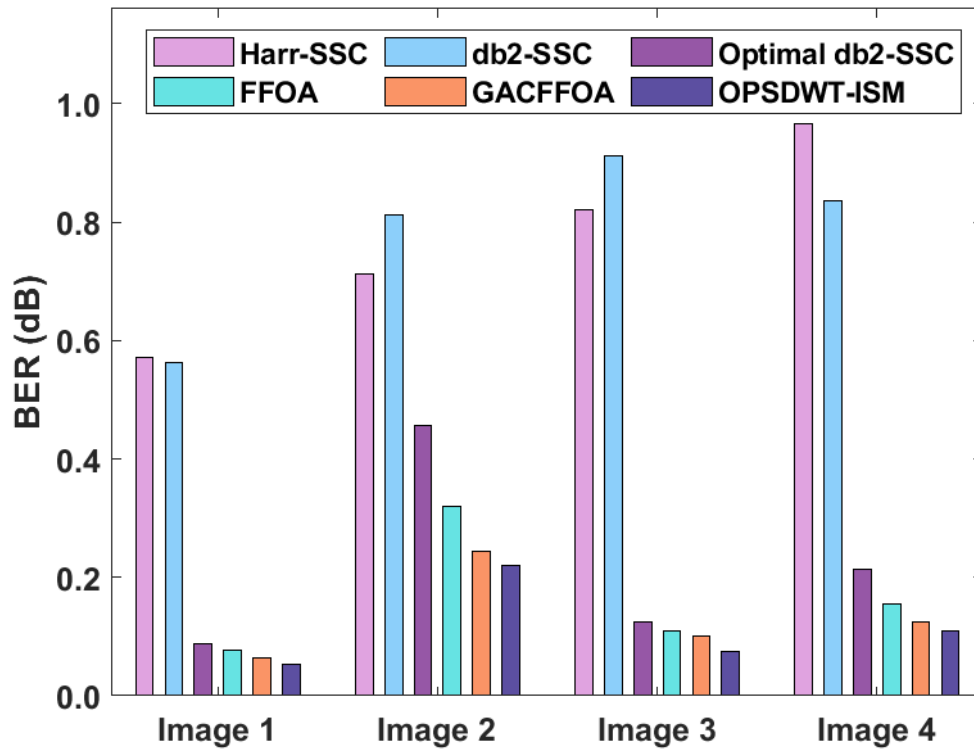


Fig. 6. BER analysis of OPSDWT-ISM model

Furthermore, on the applied image 2, the OPSDWT-ISM model has accomplished effective result with the minimum BER of 0.221 while the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have reached a superior BER values of 0.713, 0.813, 0.456, 0.321, and 0.243 correspondingly. Additionally, on the applied image 3, the OPSDWT-ISM model has accomplished effective result with the least BER of 0.075 whereas the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have reached a higher BER values of 0.821, 0.912, 0.124, 0.109, and 0.101 respectively. Simultaneously, on the applied image 4, the OPSDWT-ISM model has accomplished effective outcome with the least BER of 0.110

while the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA methods have attained a maximum BER values of 0.967, 0.836, 0.213, 0.156, and 0.124 correspondingly.

Table 5 and Fig. 7 examine the hiding capacity analysis of the OPSDWT-ISM model on the diverse set of images. The resulting values specified that the OPSDWT-ISM model has got to an advanced hiding capacity value on all the applied test images. For instance, on the applied test image 1, the OPSDWT-ISM model has gained maximum hiding capacity of 83.27 bytes whereas the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA models have achieved a lower hiding capacity value of 59.8, 66.2, 78.66, 80.46, and 81.89 bytes respectively.

Table 5 Comparative analysis of existing with proposed in terms of Hiding capacity

Test Images	Harr-SSC	db2-SSC	Optimal db2-SSC	FFOA	GACFFOA	OPSDWT-ISM
-------------	----------	---------	-----------------	------	---------	------------



Image 1	59.8	66.2	78.66	80.46	81.89	83.27
Image 2	58.8	77.4	85.55	87.49	90.43	91.73
Image 3	66.6	70	76.77	79.34	84.42	86.90
Image 4	55	79.7	89.78	92.46	92.98	93.65

Also, on the applied test image 2, the OPSDWT-ISM model has gained maximum hiding capacity of 91.73bytes while the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA approaches have attained minimum hiding capacity values of 58.8, 77.4, 85.55, 87.49, and 90.43bytes correspondingly. Besides, on the applied test image 3, the OPSDWT-ISM model has gained highest hiding capacity of 86.9bytes but the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA

manners have reached lower hiding capacity values of 66.6, 70, 76.77, 79.34, and 84.42bytes respectively. Moreover, on the applied test image 4, the OPSDWT-ISM model has gained superior hiding capacity of 93.65bytes but the Harr-SSC, db2-SSC, Optimal db2-SSC, FFOA, and GACFFOA methods have obtained a lower hiding capacity value of 55, 79.7, 89.78, 92.46, and 92.98bytes correspondingly.

3493

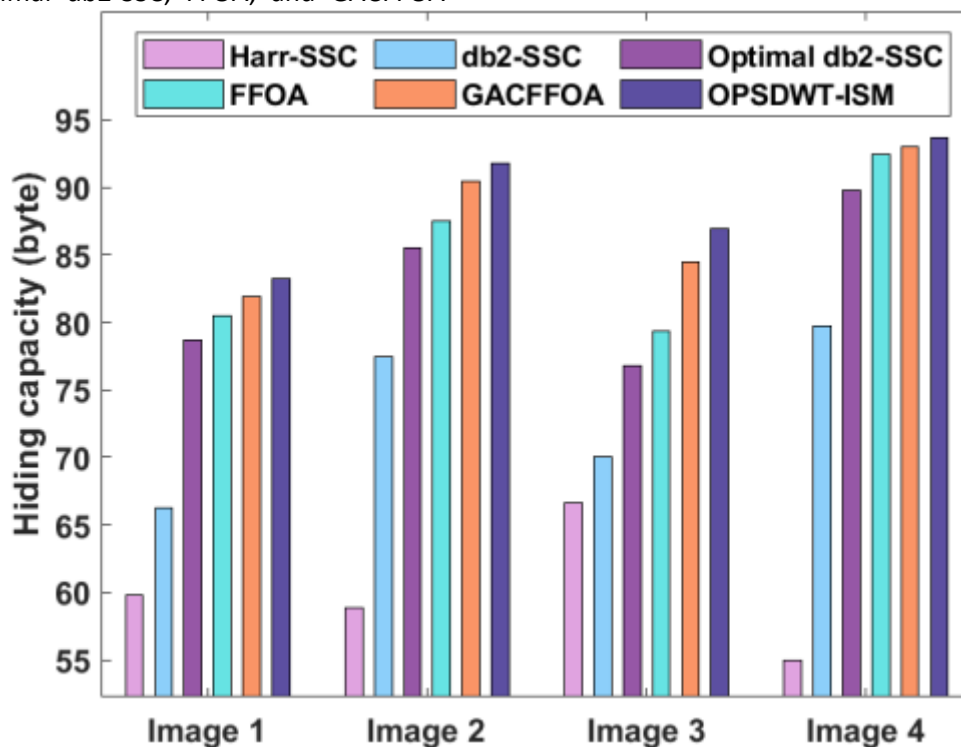


Fig. 7. Hiding capacity analysis of OPSDWT-ISM model

4. Conclusion

This paper has presented an effective OPSDWT-ISM model for securing the images. The presented OPSDWT-ISM model involves both encryption and steganography processes. The input cover image is initially decomposed using DWT technique and the

optimal pixel points are chosen by BOA. In addition, the secret image is partitioned into R, G, and B elements. Besides, the encryption process of the R, G, and B elements are carried out using three individual encryption techniques such as DES, blowfish, and Arnold cat map techniques respectively. At last, the



encrypted images are embedded to the picked pixel points in the cover image. At the receiver side, inverse DWT process is employed followed by decryption and extraction for the retrieval of secret image. A detailed experimentation analysis showcased the betterment of the presented model over the existing methods under distinct dimensions. In future, the OPSDWT-ISM technique has been incorporated to the real time applications.

References

- [1] Ghosal SK, Mandal JK. On the use of the Stirling transform in image steganography. *J Inf Security Appl.* 2019;46:320–330.
- [2] Pandey P, Tiwari P, Mishra S, et al. A steganography project-data hiding in encrypted image. *J Network Commun Em Tech (JNCET).* 2016;6(4).
- [3] Jain M, Kumar A. RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem. *Int J Machine Learning Cybernetics.* 2017;8(5):1695–1705.
- [4] Hussain M, Wahab AWA, Idris YIB, et al. image steganography in spatial domain: a survey. *Signal Process Image Commun.* 2018;65:46–66.
- [5] Teja JD, Rao ACS, Dara S. A new image steganography technique for hiding the data in multi layers of the PNG images. *Int J Ad Hoc Ubiquitous Comput.* 2017;2(7):104–112.
- [6] Kiran S, Reddy RPK, Subramanyan N. A novel high capacity data embedding image steganography using spiral scan. *International Journal of Engineering Technology Science and Research.* 2017;4(12):1363–1371.
- [7] Usha BA, Ksrinath N, Ravikumar CN, et al. Cognitive prediction of the most appropriate image steganography approach. *Int J Comput Appl.* 2015;121(8):42–45.
- [8] Atee HA, Ahmad R, Noor NM, et al. Extreme learning machine based optimal embedding location finder for image steganography. *PloS One.* 2017;12(2):e0170329.
- [9] Douglas M, Bailey K, Leeney M, et al. An overview of steganography techniques applied to the protection of biometric data. *Multimed Tools Appl.* 2018;77(13):17333–17373.
- [10] Duan X, Song H, Qin C, et al. Coverless steganography for digital images based on a generative model. *Comput Mater Continua.* 2018;55(3): 483–493.
- [11] Priyanka BG, SathyanarayanaSV. A steganographic system for embedding image and the encrypted text. In 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India. IEEE, 2014, p. 1351–1355.
- [12] Rajput SS, BohatVK, Arya KV. Grey wolf optimization algorithm for facial image super-resolution. *Appl Int.* 2019;49(4):1324–1338.
- [13] Ambika, Biradar, R.L. and Burkpalli, V., 2019. Encryption-based steganography of images by multiobjective whale optimal pixel selection. *International Journal of Computers and Applications*, pp.1-10.
- [14] Arora, S. and Singh, S., 2017. Node localization in wireless sensor networks using BF optimization algorithm. *Arabian Journal for Science and Engineering*, 42(8), pp.3325-3335.
- [15] Ambika, Biradar, R.L. and Burkpalli, V., 2019. Encryption-based steganography of images by multiobjective whale optimal pixel selection. *International Journal of Computers and Applications*, pp.1-10.
- [16] Blowfish Hybridized Weighted Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing
- [17] Abbas, N.A., 2016. Image encryption based on independent component analysis and arnold's cat map. *Egyptian informatics journal*, 17(1), pp.139-146.
- [18] A. Sivasankari and S. Krishnaveni, Genetic Algorithm with Chaotic Fruit Fly Optimization Algorithm for Discrete Wavelet Transform based Secret Sharing Cryptography Model,



- The Mattingley Publishing Co., Inc. ,
2020.
- [19] Sivasankari, A. and Krishnaveni, S.,
2019. Optimal Wavelet Coefficients
Based Steganography for Image
Security with Secret Sharing
Cryptography Model. In *Cybersecurity
and Secure Information Systems* (pp.
67-85). Springer, Cham.

