TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

Genetic Algorithm with Chaotic Fruit Fly Optimization Algorithm for Discrete Wavelet Transform based Secret Sharing Cryptography Model

[1]A. Sivasankari, [2]S.Krishnaveni
[1]Research Scholar, [2]Assistant Professor
[1,2]Department of Information Technology, Pioneer College of Arts and Science,Coimbatore, Tamil Nadu, India.
Email: [1]shivashankari.may28@gmail.com, [2]sss.veni@gmail.com

Article Info
Volume 82
Page Number: 5186 - 5198
Publication Issue:
January-February 2020

Article History
Article Received: *18 May 2019*
Revised: *14 July 2019*
Accepted: *22 December 2019*
Publication: *25 January 2020*

Abstract:
At present times, secure data transmission becomes essential to safeguard the images while communicating with other people through Internet.Image Stegnography defines the way of concealing data in an image. The image chosen for this task is referred by cover image and the image attained next to stegnography is known as stegno image. This paper presents an effective secret sharing cryptography method for secure data transmission by incorporating discrete wavelet transform (DWT) and secret sharing (SS) model. Initially, discrete wavelet transform (DWT) is employed for transforming the region. For optimal selection of the parameters involved in DWT, Genetic algorithm with Chaotic FruitFly Optimization algorithm (GACFFOA) is employed. Then, SS gets executed for lower band stegno images with highly secure process. At the same time, Visual Cryptography is applied for encrypting a secret data. A detailed experimental validation has ensured the superior features of the GACFFOA over the compared models.

Keywords: *Secret sharing, Genetic algorithm, Image stegnography, DWT*

1. Introduction

Stegnography is a model used to hide data within digital media. It is said to be hiding the previous information in alternate transmitting substance to attain private interaction. An individual technique to provide maximum security for any data could be offered by information hiding [1]. It may be named as cryptography which provides secured communication of information where it has data encryption from the client side and decryption at user side. The difference among stegnography and cryptography is said to be suspicion factor. Stegnography as well as cryptography might be executed collectively which results in improved security. It is unable to replace the cryptography rather to enhance the security under the application of obscurity parameters. It is the function of hiding data secretly inside the specific information. The main objective of Stegnography is to cover the data with sufficient participants which does not suspect stegnography medium that has hidden details [2]. Alternatively, Steganalysis is considered as the art of predicting the hidden data. It mainly focuses on breaking stegnography as well as to detect the stegno image. In stegnography, the hidden image might be enveloped with cover image and forwarded where the present data may be unpredictable. Generally, digital images, audios, sound files as well as alternate system files could be applied in embedding the data. An object that is used to hide secret data is termed as covert object. The Stego image is said to be an image which is formed by covering the secret image within covert image.

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

The, the hidden data might be in forms of plain text, cipher text and images. The Stegnography, copyright protection in digital medium as well as data coverage are assumed to be data hiding methods. There are several other stegnography approaches are, Substitution, Transform domain, Spread spectrum, Statistical and Distortion technique [3].

Substitution technique has least important bits from cover object which might be interchanged in absence of full-fledged cover object. It is considered as simple approach used for hiding data; however it is vulnerable in maintaining easier attacks like compression, transformations respectively. Transform Domain technique is composed with different methods like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) as well as Fast Fourier Transform (FFT) that are employed for hiding data in transform coefficients within cover images which makes stronger for specific attacks like compression, filtering and so on. The Spread Spectrum Technique helps to spread messages across wider frequency bandwidth when compared with lower bandwidth to pass the data. The existence of SNR in each frequency band might be small. Therefore, with no presence of cover image it is hard to eliminate the complete data. Next, the Statistical technique is segmented as blocks as well as message bits have been hidden in every block. Therefore, the data undergoes encoding with the application of modifying several arithmetic features of cover image. This operation tends to remain as same cover blocks whenever the message block becomes zero. Followed by, the Distortion technique is applicable in storing data with the help of signal distortion. Here, the encoding device includes a series of alterations to embed as well as to decode the differences among actual cover and distorted cover which is helpful in recovering the hidden data. Stegnography is mainly applied to obtain maximum ability, trust, robustness etc.

A color image stegnography model which is relied on Finite Ridgelet Transform (FRT) as well as Discrete Wavelet Transform (DWT) has been presented by [4]. Here, FRT is linked with cover color image for acquiring Ridgelet coefficients for every color channel of cover color image as well as individual DWT might be used to obtain unique wavelet coefficients that is modified by already encrypted channel of secret color image that tends to earn stegno color image. Consequently, the projected model attempts to be effective in diverse sorts of distinct color images and simulation outcome implements the improved location of stegno image that is against the present system. Sharma and Sharma [5] established a stegnography on the Red side along with DCT and DWT techniques. This model applies two images which are required in wrapped images. In advanced approach, the red component is removed. Among the 2 elements, the significant one is 3-DWT and alternative is said to be DCT. As the modified outcome is based on PSNR measures which has the scope around 60%.

A new model for image stegnography is based on DCT as well as data mining classifying principles that is proposed by [6]. The DCT is determined on secret image as well as cover image. It is capable of applying ID3 method to identify the pixel number in such a way that secret image may be launched. The ID3 technique is able to form Decision tree(DT) for obtaining the optimal pixel. It can be achieved by implementing the contortion that should be with minimum value. The key is declared as pixel value of cover image where the secret image has been inserted. Hence, projected visual cryptographic approach might be divided as 3 levels, namely Division of color groups, Production of different shares and Optimized Encryption and Decryption. In order to get optimized encrypting and decoded images, a new technique has been proposed which is relied on

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

Elliptic Curve Cryptographic (ECC) mode [7]l. Initially, the data color images are separated into 3 collective groups, as R, G and B. Thus, various image shares have been generated on the basis of pixel values. According to test analysis, images which are decoded from PSNR is achieved with MSE as well as effective CC, in absence of investigating alleviations from first pixel.

For assuming that, DCT based stegnography with the application of DC blocks to hide secret bits with sequence order in Least Significant Bits (LSBs). Furthermore, the lower as well as centralized frequenciesare given for the purpose of examining PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) by [8]. The established model named as stegnographic devices are based on DCT [9] which is implemented classify information regarding an atomic reactor by the consumption of series of models from intermediate frequency.

MeghrajaniandMazumdar[10] applied the cover message as well as encrypted secret data which undergoes encoding as noise-like shares that applies (2, 2) VC in such a way that the programmable ink of stegnography may be combined with VC (DIIVC) for embedding the hidden message. In contrary, the general location of stegnography, shares has been modified for hiding secret message instead of cover image. From the receiver side, by decoding the shares with the help of common VC tends to produce worst cover image. It is already known that, the final outcome often denotes the unique secret is displayed using VC whenever the participant comes to know about hidden data. Therefore, Stegnography helps in hiding consecutive message with the application of covered details in alternate digital medium such as image, audio, video configuration as well as Cryptography is applied to manipulate the data as cipher text which may be identical for other users that is executed by [10]. The upcoming model states that, the main objective is to reduce in size and required data should be converted into cipher data by using AES cryptographic model. Then, the encrypted data is ineffective in image. The Hereditary technique could be employed for varied images, so that the data may be embedded along with the key objective of locating secret message which disappear in different ways.

Shankar andLakshmanaprabu[11] presented a research work as Homomorphic Encryption (HE) including best key choice in image security has been applied. The histogram which is adapted must be acquainted to exploit the image powers to improve the difference. In order to elongate the trust level, it is employed with Ant Lion Optimization (ALO) which has the Fitness Function(FF) with maximum entropy along with best-encrypted image that is shown as image respectively.

This paper presents an effective secret sharing cryptography method for secure data transmission by incorporating DWT and secret sharing (SS) model. Initially, DWT is employed for transforming the region. For optimal selection of the parameters involved in DWT, Genetic algorithm with Chaotic FruitFly Optimization algorithm (GACFFOA) is employed. Then, SS gets executed for lower band stegno images with highly secure process. At the same time, Visual Cryptography is applied for encrypting a secret data. A detailed experimental validation has ensured the superior features of the GACFFOA over the compared models.

2. Proposed model

2.1 Image Stegnography

Generally, images are applied in the form of normal cover objects within stegnography. The hidden message could be added in a medicinal image by various embedding techniques as well as secret keys. Subsequently, next stegno image has been transmitted for the user. On the other hand, it has been determined with the help of extraction model which applies same key. While transmitting

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

stegnoimage, the unauthorized customers are also capable of pointing image transmission. But, the absence of secret message is because of stegnography. The presented technique as spatial domain transform is applied for implanting the hidden information within the clinical image.

2.2 Domain Transformation

From the transform region, the primary level is to convert the cover image as different applications. In this case, transform coefficients undergoes computation for the purpose of hiding secret information. The transform coefficients are then converted across spatial space to obtain stegno image. Followed by, wavelet-based transform including optimized system that is assumed to be stegno image for the purpose of transform domain principles which has maximum capability of meeting image processing operations. The domain transform process is shown in Fig. 1.

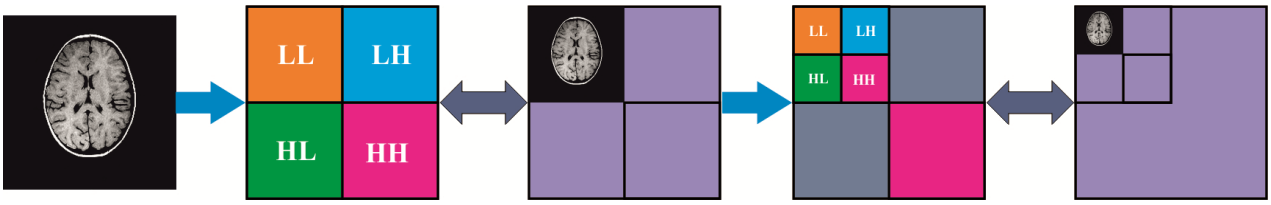


Fig. 1.Domain transform process

Here, the wavelets have been labeled with the application of interpretations and expansions obtained from stable capacity that is named as mother wavelet. The Stegnography offers points of interest by using DWT in contrast with other transform as well as stegno image formation and domain transform is shown in Fig. 1.

The Daubechies wavelet coefficients has been assumed in domain transform operation, while DWT is linked with another image; then it is decomposed into 4 subsets like LL, HL, LH, and HH. The LL portion is composed with important features. Whenever, the information is embedded with LL part of stegno image. Hence, mother wavelet function may be implied as

$$\delta_{m,n}(z) = u^{-\frac{m}{2}}\delta(u^{-m}z\text{-}nv) \quad (1)$$

$$S(z) = \sum_{u\in k}\sum_{v\in k}(\alpha_{u,v}) \cdot \alpha_{u,v}(z) \quad (2)$$

The discrete subset for a plane has every points in the form of (u^k, v^k). Also, wavelet transform is comprised with some of the benefits as attaining spatial as well as frequency domains and function-based images are transformed as frequency to spatial domain operation.

The Ingrid Daubechies which is considered to the well-known objective in the field of wavelet research that is named as minimalistically supported orthonormal wavelets which leads to experience the discrete wavelet analysis. The above wavelet applies covered windows to obtain maximum frequency coefficient radius mirrors for every higher frequency modifications. Therefore, it is denoted by

$$\delta(z) = \sum_{n=0}^{N-1} S_v\,\varphi(2S— v)$$

where$(S_0, S_1 \ldots S_{v-1})$ is the real numbers that is said to be scaling sequence. Here, proper wavelet is accomplished with the application of sane sequential integration. It is assumed to be successor of degradations along with difference of filter length which has maximum value. Thus, it is said to be localized as well as smooth, to increase the size of PSNR optimizing model is applied.

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

2.3.Genetic algorithm with Chaotic Fruit Fly Optimization Algorithm (GACFFOA)

It is notable, only one variable is preferred in the fundamental FOA, they attempt to search the technique to several variables, thus appears to possibility the distance metrics in tradition. Usually, fundamental FOA is a powerful technique in swarm intelligent (SI) techniques through the features of easy computation with higher efficiency. The effect of basic FOA, some local optimization is obtained rather than global optimization. Intended at this absence, chaotic mapping is accepted to enhance the execution of fundamental FOA escaping from the local optimization in this paper. The changed FOA presented in this paper is marked as chaotic fruit fly optimization algorithm (CFOA) [12].

Distance Metric

Distance is the metric for 2 variables in likeness, the bigger distance, the more variation is. Some distance metrics are utilized repeatedly namely Mahattan distance, Euclidean distance, Mahalanobis distance and Minkowski distance. Euclidean distance is taken benefit for computation the distance resultant in variable one dimension; as experiments illustrate Mahalanobis distance executes fit in higher dimension as a result of vector variable. In above, higher dimension problems are not included in the fundamental FOA. It develops clearly that Euclidean distance is not suitable to higher dimension problems; meanwhile the difficulty to compute is a much sustained procedure. So, distance metric is re-planned for creating the technique executes to problems in higher dimension with decrease the calculation difficulties. Because of indefinite location of the food source, we suppose that it locates in 0 in manages, afterward the absolute distance is accepted in every dimension to lessen the computation difficulties with covering the output vector needed. Specifically to declare, smell concentration judgment value (S) is a multi-dimensional variable to higher dimension problems in CFOA rather than single dimension smell concentration judgment value in FOA.

New Location Update

The new location of the fruit fly set is joint the optimal location in the fundamental process (i_v) and the optimal chaotic location (i_c) in logistic mapping (LM). The new location is described as:

$$i(z+1) = i(z) + ui_v(z) + (1-u)i_c(z)r. \quad (4)$$

where$t$ denotes the iteration, r is a arbitrary number, u indicates the balance parameter range from [0, 1]. If$u = 1$, new location based on the progress of the fruit group separately; when$u = 0$, new location only based on the chaotic mapping. To obtain exceed, arbitrary number r is initiated to keep away from the absoluteness with enhance the chance of searching to global optimization.GACFFOA involves various steps as given below and also shown in Fig. 2.

- **Initialization**. Initialized the locations of the primary fruit fly group, where uniform distribution is utilized to experiments for creating the arbitrary locations among the maximum as well as minimum values in the actual methods. The highest iterationt_{mx}, group size n, problem dimension$d$, and the bound values must be provided in beginning.
- **Fly group progress**. Based on new location computation technique, utilize Eq. (4) to obtain the new location. Let the optimal location in the fundamental progress be equivalent to the optimal chaotic location $(i_v = i_c)$ in the early stage of technique.
- **Computation for smell concentration**. The absolute distance is established to compute the smell concentration judgment value (S). Smell is the objective function value is too.
- **First selection**. Find out the optimal location (i_v) in fruit group through minimum smell

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

concentration; mark the value of smell ($smell_1$) as similar operation of 5th step of fundamental FOA.

- **Chaotic process**. Let the entire fruit group in LM. On account of data in LM ranges from$[0, 1]$, variables in fruit group must be standardized to equivalent variable t in LM. Assumed that variables of fruit group (i) range from the low bound (low) to up bound (up), standardized variable (t') describes as:

$$t' = \frac{i - low}{up - low} i \in [low, \quad up]. \qquad (5)$$

$t'$is corresponding the variable t in LM, to convert $t'(n)$ to $t'(n+1)$, where n indicating the iteration n in searching space.

- Behind the chaotic process, the variable $t'(n+1)$ ranges from [0, 1] so, inverse replacement must be use to convert $t'(n+1)$ in LM to data in fruit group. Related to Eq. (5), the replacement is proposed under:

$$i' = t'(up — low) + lowt' \in (0,1) \qquad (6)$$

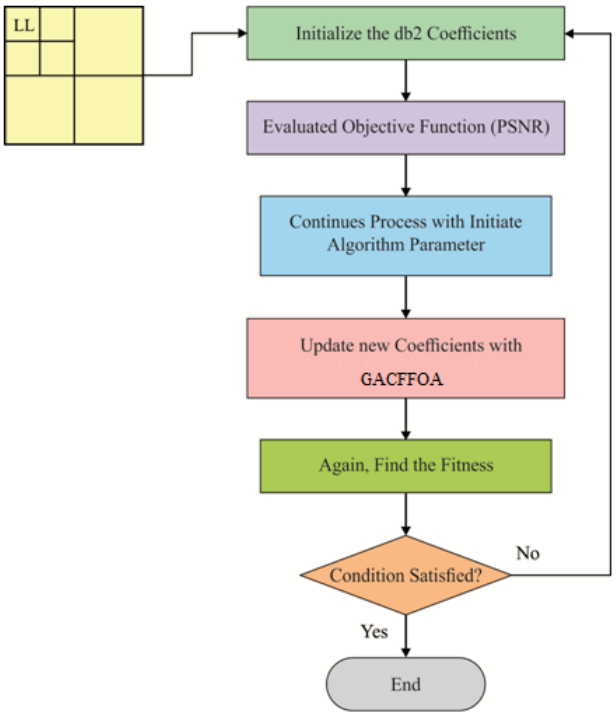


Fig. 2. DWT with GACFFOA algorithm

- **Optimal selection**. Subsequent the chaotic process, Observe the optimal i' in fruit group through the minimum smell concentration, to mark the best chaotic location (i_c) and value of smell $(smell_2)$ related to the 3th step over. Evaluate the value of optimal smell in the basic and chaotic progress; mark the lesser as the optimal smell$(bestsmell)$.
- Enter iterative optimize to review whether the iteration attain n_{mx} otherwise, when archives, finish up optimize obtain rid of loops and outcome global optimization. Or else, go to the *Step* 2.

Genetic algorithm (GA)

To overcome the local optima problem of CFFOA, GA is applied by the use of three major genetic operators namely selection, crossover and mutation [13]. GA operates with a population of coded variable known as chromosome. Every artificial chromosome includes a set of binary strings of particular length. Every individual gene has the respective variables. By the use of selection chromosomes indicating optimal solutionsrepresent effective solutions based on the objective function chosen from population. Once the reproduction process gets completed, crossover operation continues to produce a new offspring. Finally, mutation is given with required possibility.

2.4 Stegno Image

Once the image undergoes processing with the help of best wavelet transform, a maximum part of information is composed within host image that is mapped into LL image. The LH sub band has important region of vertical data that is related with similar edges. It is pointed that, optimal wavelet coefficients, LLB images are implemented along with hidden data when the security analysis of SS is integrated with encryption, decryption models has been completed.

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

2.5. Visual Cryptography

By enlarging the trust of originated stegno image by using cryptographic procedure which is used to form a "n" number of shares. Therefore, shares are always based on the region of stego image as diverse segments. In addition, hidden sharing pattern is used to encrypt secret message as n unwanted share images. It has significant performance by decrypting the hidden image acquires primary data regarding cryptography; otherwise difficult evaluation respectively. Before dividing the shares, basic grids has been designed on the basis of share numbers which should be created as well as SS pattern used in stegno image is visible for underneath section.

Secret Share (SS) Creation

The Visual Secret Sharing procedure strategy of stegno image undergoes encoding and produces nshares which are termed as transparencies. All the final shares are composed with maximum contrast pixels, in terms of noise and comprehensive in evaluating the opposite hidden image. This strategy states that, selected stegno image could be separated into 2 identical shares for the purpose of security. Hence, distinct pixel of hidden image has been improved within n adopted forms that is declared as shares which is known to be collecting sub-pixels for grey scale images. Subsequently, the shares might be formed and encrypted with converted server that is helpful in prolonging user end and decrypt the shares for stacking grey scale stego images. In this point, IDWT is applied for extricating hidden information. Therefore, share of stego image could be denoted as

$$Stego\text{—}Share = \int_{1}^{n} \lim_{n \to Noofpixel} Grey - Stego_{RGB} \quad (7)$$

In Eq. (7) it is noted that, shares has been used for stegno images in SS method. Here, shares are transmitted from client to receiver with the objective of achieving enough shares using interloper that reduces the mislabeled shares. Furthermore, the shares of stegno image undergo encryption by applying the key to provide higher security for this technology. The Secret providing model is attempted to encrypt a hidden image as n unwanted offer images. It might not be satisfied in draining the initial image till entire images are attained. These facilities might be required from standard secret image in prior to encryption as well as decryption operation.

Cryptographic Technique for SS Security

With the improved security for confidential information, shares undergo encryption and decryption operation be applying cryptographic system. Here, image encryption method is employed for transmitting the image in a secured manner. It mainly focus in removing the exploiting client that leads in proliferation of decrypting information. Thus, Public Key encryption technique assures the authorization for people present in public key to be in a definite manner. The ECC could be determined using various arithmetic operations that is used to create a scope for Elliptic Curve values [15-20]. Hence, the security model is composed with key generation of shared images that is processed with encryption as well as decryption strategy which is explained in the upcoming section.

Elliptic Curves and Base Point Generation

The Elliptic curve-based share trust is computed with cryptographic system as well as elliptic curves. The feature of ECC pattern has prime number as well as 2-integer values which may be reduced in key size [14]. This process could attain the identical phase in security that is provided in customary public key cryptography which is developed and constraint of curve is given as

$$E^2|m| = u^3 + um + v|m| \quad (8)$$

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

The above equation m denotes the prime number, u and v are said to be integer values.

The security is produced from ECC Logarithm, which is Discrete variable while collecting the parameterized elliptic curve across a restricted application.

SS security operates the hidden images and public keys has been produced from the client and receiver side. To originate the keys, it selects a specific range of prime numbers as well as S_k and P_k are assumed to be keys. Hence, the essential measures have been manufactured on the basis of shares produced. Thus, public key can be denoted by Eq. (9).

$$P_k = S_k * L \tag{9}$$

The above notation is used to forward data from sender side respectively.

The encoding as well as decoding patterns of SS images are denoted by number squares. The count of shares obtained from image might be differentiated and reform the image which is acquired from client side. Also, encryption is used to divide the images as n number of shares in terms of k number of shares is sufficient in recreating these image. This strategy explains that, each sections of information have been provided as encrypting pattern.

$$CipherShare\ 1 = L * S_k \tag{10}$$

$$CipherShare\ 2 = (S_i, S_j) + Ciphershare\ 1 \tag{11}$$

From this experiment, the client and receiver applies another key of technique which is named as public key encryption. The decryption model is contrast to encryption method that is applied to transform across the encrypted medium as interesting plain context which is defined as

$$PlainImage = L \times CipherShare\ 1\ orCiphershare\ 2 \tag{12}$$

The cryptographic system has cipher images which are obtained from encrypted images and proceed with decryption. If the secret data is secured in stego image environment, the reverse transformation helps to eliminate the image as well as secret image from spatial space transform which is IDWT that is used to attain optimal matrix. Therefore, the pattern explains that, text record has been encrypted with possible way and the same image is retained with stegnography criteria that tend to improve the security level of presented techniques.

3. Performance Validation

A detailed set of simulation processes takes place for ensuring the effectual performance of the GACFFOA. The results are assessed with respect to PSNR, Mean Square Error (MSE), Bit Error Rate (BER) and hiding capacity (HC). Table 1 visualizes the results produced by the proposed method on the application of covering the secret image during transmission. The second row in the table indicates the cover image and secret information. The stego image created by the proposed method is exactly same as the input image and secret information does not even visible at all. Similarly, all the rows in the table shows the exact conciliation of the secret data on the cover image.

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

Table 1 Cover image, Secret Image and its Stego Image

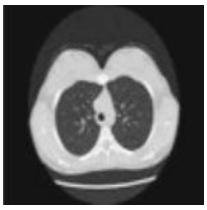
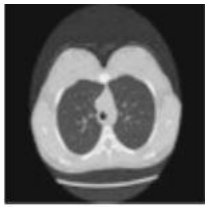
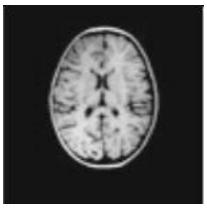
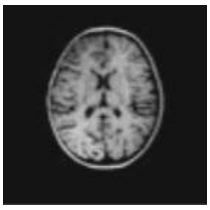
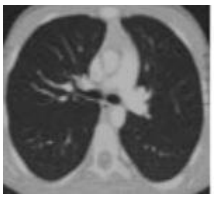
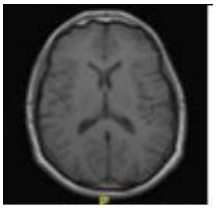
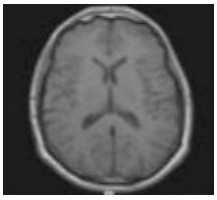
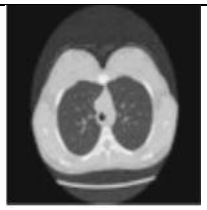
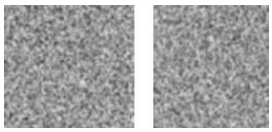
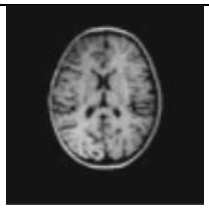
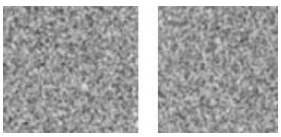
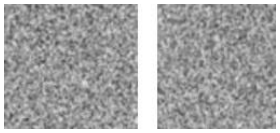
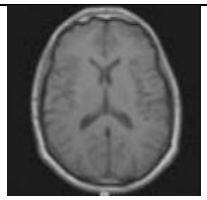
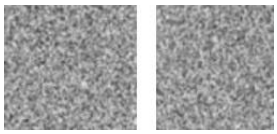
Image Name	Cover Image	Secret Information	Stegno Image
Image 1			
Image 2		Cryptography	
Image 3		Data	
Image 4			

Table 2 provides a neat analysis of the results attained by the proposed model on the applied test images. The table values clearly denoted the PSNR, BER and hiding capacity terms. Under the application of the proposed method on the first input image, a maximum PSNR value of 52.65dB, BER of 0.076 and hiding capacity of 84.89bytes is obtained. Under the application of the proposed method on the second input image, a maximum PSNR value of 59.48dB, BER of 0.412 and hiding capacity of 86.43bytes. Under the application of the proposed method on the third input image, a maximum PSNR value of 54.30dB, BER of 0.098 and hiding capacity of 77.42bytes is reached. Atlast, under the application of the proposed method on the fourth input image, a maximum PSNR value of 49.19dB, BER of 0.145 and hiding capacity of 90.98bytes is attained.

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

Table 2 Performance analysis for image security

Lower band stego image	Cipher shares	PSNR (dB)	BER	Hiding capacity (byte)
		52.65	0.076	81.89
		59.48	0.412	86.43
		54.30	0.098	77.42
		49.19	0.145	90.98

A comparison of the results offered by the proposed model interms of PSNR is shown in Table 3and Fig. 3. On the applied image 1, it is depicted that the GACFFOA offers maximum PSNR values of 53.87 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower PSNR values of 26.6, 38.7, 43.4, 50 and 51.3correspondingly. On the applied image 2, it is depicted that the GACFFOA offers maximum PSNR values of 59.65 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower PSNR values of 32.4, 43.5, 53.55, 56.85 and 57.98 correspondingly.

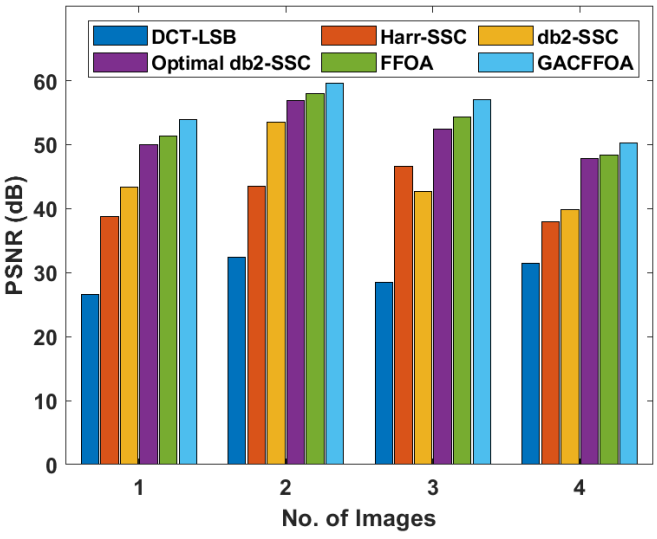


Fig. 3. PSNR analysis of various methods

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

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

No. of Images	DCT-LSB	Harr-SSC	db2-SSC	Optimal db2-SSC	FFOA	GACFFOA
1	26.6	38.7	43.4	50	51.3	53.87
2	32.4	43.5	53.55	56.85	57.98	59.65
3	28.55	46.67	42.7	52.45	54.30	56.98
4	31.45	37.9	39.8	47.8	48.42	50.32

On the applied image 3, it is depicted that the GACFFOA offers maximum PSNR values of 56.98 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower PSNR values of 28.55, 46.67, 42.7, 52.45, 54.30and56.98correspondingly. On the applied image 4, it is depicted that the GACFFOA offers maximum PSNR values of 50.32 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower PSNR values of 31.45, 37.9. 39.8, 47.8 and 48.42 correspondingly.

Table 4 Comparative analysis of existing with proposed in terms of Hiding capacity

No. of Images	DCT-LSB	Harr-SSC	db2-SSC	O…	SSC	FFOA	A…
1	55.4	59.8	66.2		79.8	80.46	81.37
2	47.6	58.8	77.4		86.4	87.49	89.32
3	59.9	66.6	70		77.6	79.34	81.46
4	54.5	55	79.7		91	92.46	94.35

A comparison of the results offered by the proposed model interms of HC is shown in Table 4 and Fig. 4. On the applied image 1, it is depicted that the GACFFOA offers maximum HC values of 81.37 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower HC values of 55.4, 59.8, 66.2, 79.8 and 80.46correspondingly.

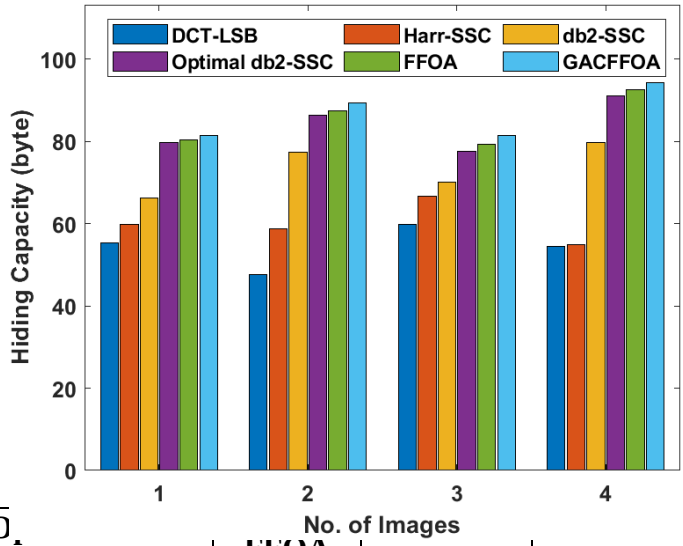


Fig. Hiding capacity analysis of different methods

On the applied image 2, it is depicted that the GACFFOA offers maximum HC values of 89.32 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower HC values of 47.6, 58.8, 77.4, 86.4 and 87.49 correspondingly. On the applied image 3, it is depicted that the GACFFOA offers maximum HC values of 81.46 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

lower HC values of 59.9, 66.6 70, 77.6, and 79.34 correspondingly. On the applied image 4, it is depicted that the GACFFOA offers maximum HC values of 94.35 whereas the other models such as DCT-LSB, Harr-SSC, db2-SSC, Optimal db2-SSC and FFOA reaches to a lower HC values of 54.5, 55, 79.7, 91 and 92.46 correspondingly. The above presented tables and figures portrayed the goodness of the presented GACFFOA model.

4. Conclusion

In stegnography, the hidden image might be enveloped with cover image and forwarded where the present data may be unpredictable.This paper has introduced an effective secret sharing cryptography method for secure data transmission by incorporating DWT and SS model. Initially, DWT is employed for transforming the region. For optimal selection of the parameters involved in DWT, GACFFOA is employed. Then, SS gets executed for lower band stegno images with highly secure process. At the same time, Visual Cryptography is applied for encrypting a secret data. A detailed experimental validation has ensured the superior features of the GACFFOA over the compared models.The above presented tables and figures portrayed the goodness of the presented GACFFOA model.

References

[1] Gupta S, Dhanda N (2015) Audio stegnography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT). J ComputEng 17(2):32–44

[2] Bhardwaj R, Khanna D (2015, Dec) Enhanced the security of image stegnography through image encryption. In: India conference (INDICON), 2015 annual IEEE, pp 1–4. IEEE

[3] Subhedar MS, Mankar VH (2016) Image stegnography using redundant discrete wavelet transform and QR factorization. ComputElectrEng 54:406–422

[4] Thanki R, Borra S (2018) A color image stegnography in hybrid FRT–DWT domain. J InfSecurAppl 40:92–102

[5] Sharma P, Sharma A (2018, Jan) Robust technique for stegnography on Red component using 3-DWT-DCT transform. In: 2018 2nd international conference on inventive systems and control (ICISC), pp 1049–1054. IEEE

[6] Vasoya DL, Vekariya VM, Kotak PP (2018, Jan) Novel approach for image stegnography using classification algorithm. In: 2018 2nd international conference on inventive systems and control (ICISC), pp 1079–1082. IEEE

[7] Geetha P, Jayanthi VS, Jayanthi AN (2018) Optimal visual cryptographic scheme with multiple share creation for multimedia applications. ComputSecur 78:301–320

[8] El_Rahman SA (2016) A comparative analysis of image stegnography based on DCT algorithm and stegnography tool to hide nuclear reactors confidential information. ComputElectrEng 70:380–399

[9] Meghrajani YK, Mazumdar HS (2015) Hiding secret message using visual cryptography in stegnography. In: India conference (INDICON), 2015 annual IEEE, pp 1–5. IEEE

[10] Sethi P, Kapoor V (2016) A proposed novel architecture for information hiding in image stegnography by using genetic algorithm and cryptography. ProcediaComputSci 87:61–66

[11] Shankar K, Lakshmanaprabu SK (2018) Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. Int J EngTechnol 7(9):22–27

[12] Mitić, M., Vuković, N., Petrović, M. and Miljković, Z., 2015. Chaotic fruit fly optimization algorithm. *Knowledge-Based Systems*, *89*, pp.446-458.

[13] Sivanandam, S.N. and Deepa, S.N., 2008. Genetic algorithms. In *Introduction to genetic algorithms* (pp. 15-37). Springer, Berlin, Heidelberg.

[14] Sivasankari, A. and Krishnaveni, S., 2019. Optimal Wavelet Coefficients Based Stegnography for Image Security with Secret Sharing Cryptography Model. In *Cybersecurity and Secure Information Systems* (pp. 67-85). Springer, Cham.

[15] Shankar, K. (2018). An optimal RSA encryption algorithm for secret images. International

January - February 2020
ISSN: 0193 - 4120 Page No. 5186 - 5198

Journal of Pure and Applied Mathematics, 118(20), 2491-2500.

[16] Shankar, K., Devika, G., &Ilayaraja, M. (2017). Secure and efficient multi-secret image sharing scheme based on boolean operations and elliptic curve cryptography. International Journal of Pure and Applied Mathematics, 116(10), 293-300.

[17] Shankar, K., &Eswaran, P. (2016). RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. Journal of Circuits, Systems and Computers, 25(11), 1650138.

[18] Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Transactions on Reliability.

[19] Shankar, K., Lakshmanaprabu, S. K., Gupta, D., Khanna, A., & de Albuquerque, V. H. C. (2018). Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, e5122.

[20] Shankar, K., &Ilayaraja, M. (2018, January). Secure Optimal k-NN on Encrypted Cloud Data using Homomorphic Encryption with Query Users. In 2018 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE.