A Hybrid Transform Based Grey Scale Image Watermarking Method Using an Extended Fruit Fly Optimization Algorithm

Dr. G. Nagaraju[1], P. Udaya Bhanu[2], T. Vidya Pravallika[3], P. Durga Rao[3], V. Kumara Sankara[3], S. Teja Naga Krishna Varma[3]

[1,2]Assistant Professor, [3]B. Tech Students

[1,3]Department of ECE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.

[2]Department of EEE, S.R.K.R. ENGINEERING COLLEGE (A), BHIMAVARAM, Andhra Pradesh, India.

***Abstract*: This paper proposes a hybrid image watermarking method based on discrete wave transformation (DWT), singular value decomposition (SVD), Fruit fly optimization algorithm (FOA), and Hessenberg decomposition (HD). The process begins with the decomposition of the cover image into many sub-bands using multiple-level DWT until the size of the sub-band is compatible for inserting the watermark image. The watermark image is processed using the singular value decomposition method before its insertion into the cover image. The outputs of DWT which are in the form of coefficients are given as inputs for HD. For achieving a good trade-off between invisibility and robustness an optimized scaling factor must be obtained, which can be done by employing the Fruit fly algorithm (FOA). This method works for various sizes of watermark images e.g., 256X256, 512X512, 1024X1024. This method works under various attacks such as JPEG compression, noise, sharpening, and filter attacks.**

***Keywords:* Image watermarking, Hessenberg decomposition (HD), Singular value decomposition (SVD), Fruit fly algorithm, Discrete wave transformation (DWT).**

1 INTRODUCTION:

The right to digital property is very important. Hence it needs to be protected. Watermarking is a technique used for the authentication of ownership over information. It protects the original digital data from copying [1], modifying [2], [35] and being distributed illegally [4], [5]. G. Nagaraju, et. al. presented a paper based on watermarking mechanism [3], in which patient's personal information is encrypted and embedded into the patient's medical image. Results from simulation shows that the security of watermarked image transmission is increased. In image watermarking methods the watermark must be invisible and robust enough to resist various attacks. The watermarking techniques are classified into three types based on these parameters, they are robust, fragile, and semi-fragile watermarking techniques [1]. The integrated watermark image can resist various attacks without a significant loss in robust watermarking. The use of fragile watermarking is to detect if any changes were made to the original image [4]. The semi-fragile technique has combined properties of both robust and fragile watermarking techniques. The robust watermarking is most widely used compared to the other two.

The easy way to embed a watermark image into the cover image is by spatially modifying the pixels [4]. But it doesn't resist image processing attacks and geometric attacks [4]. In the frequency domain, the embedding process can be done by transforming the pixels into discrete Fourier transforms (DFT) [6]-[8], discrete cosine transforms (DCT) [9]-[14], and discrete wave transforms (DWT) [15]-[17]. [12] Ernawan proposed a digital watermarking method that provides which has high imperceptibility and robustness. It uses an optimal DCT psychovisual threshold. In order to provide additional security, the watermark is scrambled and then embedded into the cover image. The method is tested under various image processing attacks and geometric attacks and the output shows that the proposed method provides high invisibility and robustness. [14] A.K Singh proposed a robust hybrid watermarking technique. The method uses the fusion of DCT (discrete cosine transform) and DWT (discrete wavelet transform) and SVD. Multiple watermarks are embedded into a single cover image for increasing security and authentication. In the method [14], the vector S of watermark information is embedded into the component S of the cover image. The text watermark is embedded in the second level of D (diagonal sub-band) of the cover image. The text data is encrypted before embedding it into the cover image to improve security.

Human vision is sensitive at low frequencies hence embedding is done at low frequencies. The method proposed uses DWT-based watermarking due to its advantages of good energy compression, insignificant visual quality and multi-resolution. But the main disadvantage is that it does not resist geometric attack [18], to avoid this DWT is followed by matrix decomposition [18]-[19], [30]. The watermarking method mentioned in the paper [18] is based on partial pivoting lower and upper triangular (PPLU) decomposition. In PPLU decomposition a digital watermark image is divided into permutation matrix, upper triangular matrix and lower triangular matrix, out of these three the permutation matrix is responsible in authenticating the legal ownership of the watermark. The scaling factor for maximum robustness which

can be obtained against image processing pirate attacks and processing attacks is obtained using the weightage-based differential evolution algorithm.

G. Nagaraju, et. al., [20] proposed an algorithm using transform domain approach. It involves improving the efficiency of watermarking by combining DWT and discrete cosine transform (DCT). [21] I A Ansari proposed a watermarking method based on integer wavelet transform (IWT) and singular value decomposition (SVD). To avoid the false positive problem that occurs due to SVD, the cover image undergoes IWT before undergoing SVD. The scaling factor is optimized using an Artificial bee colony (ABC). The properties of IWT and SVD increase the robustness. [22] is based on discrete wave transform (DWT) and singular value decomposition (SVD). The invisibility of the method is evaluated by the peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) values while the normalization correlation (NC) values help to determine the robustness of the method.

SVD and HD are used most commonly for performing matrix decomposition. The Singular Value Decomposition is used in retaining important singular values that the image needed which is important in determining the image quality. The problem faced during SVD processing is the false positive problem, which can be corrected by encrypting the components of SVD using chaotic systems. HD determines the method to embed the watermark. FOA improves the performance and helps in maintaining the balance between invisibility and robustness of the watermarking model, objective evolution function (*oefunc*) assists FOA in order to find an optimized scaling factor. When performance of this method is tested, the result shows that this method works for multiple sizes of watermarks, it has a good trade-off between invisibility and robustness and it is robust enough against different attacks of filter, noise, sharpening, JPEG, and JPEG2000 compressions.

[26] is based on using the Firefly algorithm which can be used in a watermarking technique based on DWT-QR transform. Performance measures like SSIM and bit error rate were used in computing the objective function which is used in achieving trade-off between the invisibility and robustness. G. Nagaraju, et. al., [28] implemented an algorithm on Image Watermarking Scheme which is built by using both IWT and DCT transforms and also demonstrates an optimised scaling factor that decides the watermarked image imperceptibility along with achieving a better capacity and robustness. [29] S. Thakur proposed a watermarking technique that uses redundant discrete wavelet transform (RDWT) and singular value decomposition (SVD). In order to optimize its invisibility and robustness nonsubsampled contourlet transform (NSCT) is used additionally. In the method [29], after embedding multiple watermarks into the cover image, then a lightweight cryptographic mechanism is applied on it. The method is then checked under different wavelet filters and using 5 various types of non-medical filters and 10 various types of medical filters.

[30] proposes a watermarking method of images which is robust in nature and is built using LWT and QR decomposition using LSVR. The results show that the method also achieves high perceptibility and robustness against different Image processing operations. G. Nagaraju, et. al., [31] implemented an image watermarking technique for images that contain details of the patient. It is built using the combination of NSCT and RDWT transforms with SVD, which gave best results in achieving the robustness against different signal processing and geometric attacks. Results of the model [31] shows that it has attained good safety against unintentional attacks and exhibits enough imperceptibility.

G. Nagaraju, et. al., [34] proposed a paper which deals with the secrecy of images where the key images are generated for the process of encryption. The Key image will be generated using a secret keyword which should be alphanumeric. With the help of a binary key table, every alphanumeric key will be generated where it consists of an 8-bit unique value. Playfair cipher and the Vigenere cipher algorithms are combined and a hybrid algorithm is introduced which gave better results. The results also showed that the correlation between the pixels of the image before and after the proposed encryption process is reduced. It shows that on an average, the rate of change of image components is very high and therefore the cipher image is very hard to be identified. By applying the reverse process, we get the decrypted image.

G. Nagaraju, et. al., [36] proposed a paper in which it introduces a hybrid encryption model for providing security of the patient's medical data which is been diagnosed. Here, either the 2D-DWT-1L or the 2D-DWT-2L stenography technique is used. The combination of RSA and XOR Cipher algorithms is used here to build a hybrid algorithm. Here the patient's information will be encrypted. After that, the confidential data is then embedded into an image using 2D-DWT-1L or 2D-DWT-2L. Based on five statistical parameters; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM) and Correlation, the performance of the method will be evaluated.

2 MAJOR CONTRIBUTIONS OF THE WORK:

The four techniques which will be in this proposed method are introduced in this section. The techniques are HD, SVD, DWT and FOA. The watermarking performance under robustness attacks can be improved by the time-scale signal multi-resolution. When HD is performed, which is a transform in matrix form, the robustness will be improved furtherly. Additionally, the watermarking method based on SVD when defending the geometric attacks has a performance improvement. For the invisibility and robustness trade-off to be balanced, the scaling factor optimization must be performed while developing the watermarking method. In this method, FOA is used for optimization.

2.1 DISCRETE WAVE TRANSFORMATION:

Discrete Wave transformation is one of the most effective frequency domain transformation methods and it has many applications in the field of Image processing [21]. DWT represents energy concentration of the image. DWT provides good defence against attacks in image processing [17]. The cover image is divided into four sub-bands, which include low-low(LL), low-high(LH), high-low(HL), high-high(HH). After performing one level of DWT, most of the cover image information is retained in the LL sub-band. This sub-band can be further decomposed until the size of the sub-band satisfies the requirement of the watermark image. Compared to the other three sub-bands or levels, the LL sub-band will have a better performance against the image processing attacks. Due to this reason, the LL sub-band is more suitable as it has more significant information about the cover image and is used for further operations.

Here we will be performing k-level DWT. Here k means the logarithmic ratio of the length of the cover image to the length of the watermark image. The value of k is computed as

$$k = log_2 \frac{A}{B} \tag{1}$$

where A is the length of the cover image and B is the length of the watermark image. Depending on the value of k, DWT will be performed, either once or twice or so on.

2.2 HESSENBERG DECOMPOSITION:

HD is one of the methods which is used in the decomposition of a square matrix [22]. Suppose a square matrix Y of size $m \times m$ which is decomposed using HD as shown by

$$OHO^T = HD(Y), \tag{2}$$

here O represents orthogonal matrix, H represents upper Hessenberg matrix, and $h_{i,j} = 0$ if $i > j + 1$. Hessenberg matrix is calculated using a householder matrix P, which is also an orthogonal matrix and it is represented as

$$P = (I_m - 2uu^T)/u^T u, \tag{3}$$

Where I^m is an identity matrix of size $m \times m$ and u is a non-zero vector in V^m. There are $m - 2$ steps involved in this process. Hence, Hessenberg Decomposition is calculated as

$$O = (P_1 P_2 \ldots\ldots P_{m-2})^T Y (P_1 P_2 \ldots\ldots P_{m-2}), \tag{4}$$

$$H = O^T Y O, \tag{5}$$

$$Y = OHO^T \tag{6}$$

Therefore, the robustness will be improved further as a better accurate component of the cover image can be found using HD [22], [23].

2.3 SINGULAR VALUE DECOMPOSITION:

SVD will decompose a symmetric matrix and three sub matrices are obtained as an output. Diagonal matrix are used for obtaining singular values [24]. The three decomposed matrices include right singular matrix (*R)*, left singular matrix (L) and singular matrix (S). Assume X as asymmetric matrix, then SVD is computed as

$$LSR^T = SVD(X)\ , \tag{7}$$

where $LL^T = I_m$ and $RR^T = I_m$. Orthonormal eigenvectors of XX^T are the column of L and for $X^T X$ are the columns of R. Square roots of the eigenvalues from R or L are present in the diagonal matrix S in descending order. Assume g $(g \leq n)$ as the rank of X, then the elements present in the diagonal matrix S follows the condition which is given in Eq. 8.

$$\sigma_1 \geq \sigma_2 \geq \cdots\cdots \geq \sigma_g \geq \sigma_{g+1} = \sigma_{g+2} = \cdots = \sigma_n = 0, \tag{8}$$

$$X = \sum_{i=1}^{g} \sigma_i \mu_i \vartheta_i \tag{9}$$

Where ϑ_i, μ_i are the i_{th} eigenvector of R and L, σ_i represents the i_{th} singular value. The value S of SVD of watermark image is embedded into the cover image by using an optimal scaling factor.

2.4 FRUIT FLY OPTIMISATION ALGORITHM

FOA is based on the behaviour of the fruit fly in search of food [25], and the signalling system that is used in attracting other fruit flies. In the proposed method of watermarking FOA is used for optimization rather than other biomimetic

algorithms such as ABC, genetic algorithm, PSO and colony optimization algorithm due to their complexity in computational processing and using too many variables [25]. The implementation of FOA is explained in detail in below steps.

Step.1: Let X_a, Y_a represent the positions of the fruit fly swarm. Initialize these variables randomly.

Step.2: Let $X_i = X_b + x_r$, $Y_i = Y_b + y_r$, where x_r and y_r are the variables for random values. And let the location coordinates be X_b and Y_b, where X_a, Y_a are the initial values of these location coordinates. X_i, Y_i gives information about distance and random direction of the individual fruit fly.

Step.3: let $D_i = \sqrt{X_i^2 + Y_i^2}$ is the distance measured from the origin. D_i is calculate first and then the reciprocal of D_i is calculated which is called as the smell concentration $S_i = 1/D_i$.

Step.4: At individual location of the fruit fly the smell concentration is given as $Smell_i$. Find $Smell_i$ which is a function

of S_i, and it is denoted as $Smell_i$ =Function(S_i). Function(S_i) is the smell concentration judgment function

Step.5: Find the maximal value of the smell concentration in the swarm of fruit flies, and it is given as $[bestSmell, bestIndex]$ = max ($Smell_i$).

Step.6: The best values of the smell concentration and the coordinate is recorded, then the swarm of the fruit flies will move towards the final location using vision $Smellbest = bestSmell,\ X_b = X(bestIndex),\ Y_b = Y(bestIndex)$.

Step.7: Perform iterative optimization and repeat Steps 2-5 if the iterative smell concentration is better than its previous value. Otherwise, return to Step 6.

3 PROPOSED SCHEME OF WATERMARKING:

The Embedding algorithm of watermark-image is explained in detail in section 3.1 and the extraction algorithm of watermark image is explained in detail in section 3.2. Section 3.3 contains details of how FOA is utilized in achieving a better trade-off between invisibility and robustness.

3.1 EMBEDDING ALGORITHM OF THE WATERMARK IMAGE INTO THE COVER IMAGE:

Cover image *f* and watermark image *Z* are given as the inputs to the embedding algorithm of the watermark image and the output here obtained is watermarked cover image *f**. The respective sizes of *f*, *Z*, *f** are A × A, B × B and A × A. The method that is proposed here can be implemented on watermark images of different sizes, by decomposing the cover image using *k*-level DWT and the procedure for the embedding the watermark image into the cover image is displayed in Fig-1. Detailed steps in embedding algorithm are as follows

Step-1: Based on the k-level Discrete Wave Transformation, *f* will be decomposed into four sub bands that are LL, HL, LH, HH and $k = log_2 \frac{A}{B}$.

Step-2: Hessenberg Decomposition is performed on the LL component. It is represented as

$$OHO^T = HD(LL). \tag{10}$$

Step-3: Applying Singular Value Decomposition on H.

$$HL_z HS_z HR_z^T = SVD(H). \tag{11}$$

Step-4: Apply Singular Value Decomposition on Z.

$$L_z S_z R_z^T = \text{SVD(Z)}. \tag{12}$$

The components L_z, R_z^T are encrypted by a Chaotic-System. It is generated by a Logistic-map based equation. Details

of the encryption process will be in the section 4.2. The two encrypted components are represented as L_{z1}, R_{z1}^T.

Step-5: An embedded singular value HS_z^* is calculated by the addition of HS_z and S_z with the help of a scaling factor a and it is represented as

$$HS_z^* = HS_z + aS_z. \tag{13}$$

Step-6: H^*, which is the watermarked sub band, is generated by applying the inverse Singular Value Decomposition

$$H^* = HL_z HS_z^* HR_z^T. \tag{14}$$

Step-7: LL^* which is a newer low frequency sub band, will be reconstructed by applying the inverse Hessenberg Decomposition which is represented as

$$LL^* = OH^*O^T. \tag{15}$$

Step-8: f^*, which is the watermarked cover image, is obtained by applying the inverse k-level Discrete Wave Transformation.

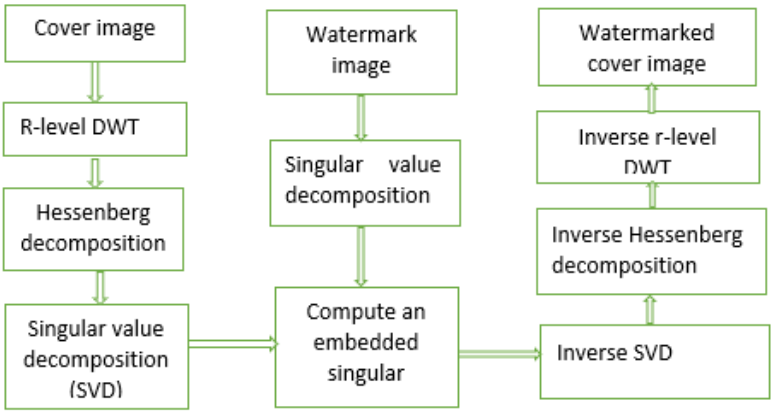

Fig-1: Embedding of Watermark image

3.2 EXTRACTION ALGORITHM OF THE WATERMARK IMAGE:

The input to the extraction algorithm of the watermark image is, the watermarked cover image f^*. The output obtained here is extracted watermark image Z^*. The obtained output size of Z^* is B×B and the procedure for the extraction of watermark image was displayed in Fig-2. The detailed extracting steps are shown as follows.

Step-1: Decomposition of the watermarked cover image f^*, into the four sub bands that are LL_z, HL_z, LH_z, HH_z is done by k-level Discrete Wave Transformation.

Step-2: Hessenberg Decomposition will be performed on LL_z sub band, i.e,

$$O_z H_z O_z^T = HD(LL_z). \tag{16}$$

Step-3: Applying Singular Value Decomposition on H_z which is represented as

$$HL_z^* HSb_z^* HR_z^{*T} = SVD(H_z) \tag{17}$$

Step-4: An extracted singular value HS_z^* is calculated using the equation

$$S_z^* = (HSb_z^* - HS_z^*)/a \tag{18}$$

Step-5: The encrypted components L_{z1} and R_{z1}^T are now decrypted of course, by the same Chaotic-System which is used in the encryption process and are now marked as L_{z2} and R_{z2}^T. Now, by applying the inverse Singular Value Decomposition, the extracted watermark image Z* is obtained.

$$Z^* = L_{z2} S_z^* R_{z2}^T \tag{19}$$

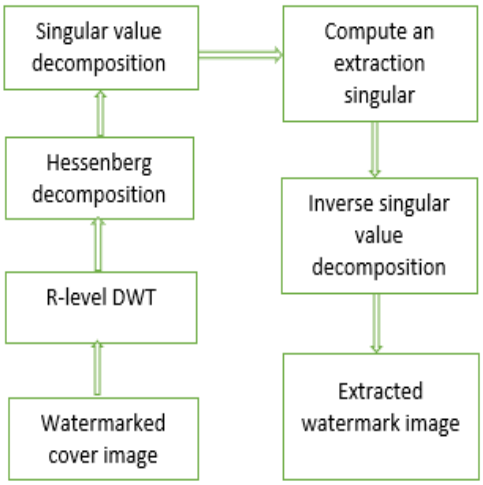

Fig-2: Watermark extracting procedure.

3.3 OPTIMIZATION OF THE PROPOSED ALGORITHM USING FOA:

The FOA algorithm is used in this work to actually produce the best possible results that is to maintain the balance between both the invisibility and the robustness of the algorithm. Invisibility of the proposed algorithm is determined by both the performance measures that are the Peak signal-to-noise ratio (PSNR) and the Structural similarity index measure (SSIM). PSNR is computed as

$$PSNR\,(f, f^*) = 10\lg\frac{f_{max}^2}{MSE}, \tag{20}$$

$$MSE=\frac{1}{M^2}\sum_{i=1}^{M}\sum_{j=1}^{M}\left(f_{i,j} - f_{i,j}^*\right)^2, \tag{21}$$

Where, *MSE* is the mean square error between both cover image and watermarked cover image and f_{max} is the maximum pixel value in the cover image. *SSIM* is computed as

$$SSIM\,(f, f^*)=\frac{\mu_f\mu_{f^*}+h_1}{\mu_f^2+\mu_{f^*}^2+h_1}\cdot\frac{\sigma_{ff^*}+h_2}{\sigma_f^2+\sigma_{f^*}^2+h_2}, \tag{22}$$

where μ_f and μ_{f^*} are the mean values of f and f^*, σ_f^2 and $\sigma_{f^*}^2$ are the variances of f and f^*, σ_{ff^*} is covariance of f and f^*, h_1, h_2 variables are used for stabilizing the divisions with weak denominator.

Normalized correlation (NC) helps to measure the robustness between the original watermark image and the obtained watermark image after the extraction procedure. NC is calculated as

$$NC=\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} Z_{i,j}Z_{i,j}^*}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} Z_{i,j}^2}\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N} Z_{i,j}^{*2}}} \tag{23}$$

Assume that the watermarked cover image is subjected to K various types of attacks, Objective Evaluation Function(*oefunc*) is introduced to help the FOA algorithm in optimizing the scaling factor a and is computed as

$$oefunc\,(a_i, wf, \alpha_i)=\alpha_1\frac{1}{wf}PSNR(f, f^*) + \alpha_2 SSIM(f, f^*) + \alpha_3 K\sum_{i=1}^{K} NC(Z, Z_i^*), \tag{24}$$

Where Z_i^* is the watermark extracted after i_{th} attack, a_i is the array containing different scaling factors, where i =1,2,…,t where t is maximum index number, wf is the weight factor, α_1, α_2, α_3 are adjustable proportionality coefficients which represent quantization coefficients and directly proportional to invisibility and robustness. For an acceptable image quality, the *PSNR* must be greater than *33db*. The detailed procedure of finding an optimized scaling factor which is shown in Fig-3. The following are the steps for implementing this process.

Step-1: Initialize *oefunc* parameters $a_i(i = 1,2,\dots,t), wf, \alpha_i(i = 1,2,\dots,t)$ and FOA parameters

Step-2: For calculating the values of *oefunc*,

a. consider the watermarked cover image f^* obtained by embedding watermark Z in cover image f with a_i.
b. Then apply K different attacks on the watermarked cover image and now extract the watermark image Z_i^*.
c. Compute *PSNR* (f, f^*), *SSIM* (f, f^*), $NC(Z, Z_i^*)$ based on the outcomes of a, b and d.

d. Compute the Objective Evaluation Function (*oefunc*) values for each respective location using the Eq. 24 and the obtained values are ready to be used in smell concentration judgement function $Smell_i$ =Function(S_i).

Step-3: The optimal scaling factor is obtained as mentioned in Fruit Fly optimization algorithm of section 2.4.

4 EXPERIMENTAL RESULT AND ANALYSIS:

The invisibility and robustness of the proposed method are analysed here. For different sizes of watermarks used, the optimal adaptive scaling factor is produced by using PSNR, SSIM and NC. The performance measures that are the robustness and the invisibility of the proposed model are estimated by objective quantitative analysis and subjective visual observation. The cover image used here is the size of 512×512 which is shown in the fig-4(a). The watermark images used in the method of sizes 256×256, 128×128 and 64×64 is shown in fig-4(b), 4(c) and 4(d) respectively. For all the experiments carried out the fruit fly initial population is 20 and the maximum iteration is 100. Different types of attacks used to test the robustness are mentioned in table 1. The main objective of introducing these attacks is to build and check the robustness of the proposed watermark model. These attacks include noise, filter, compression, motion blur and sharpening attacks. The noise attacks include salt &pepper, Gaussian and speckle noise attacks of variance 0.001. The filter attacks include median filter, Gaussian low-pass filter and average filter with filter size 3×3. JPEG2000 compression and JPEG compression are the compression attacks used to evaluate the robustness in this model. For motion blur attack Theta=4 and Len=7. The threshold for sharpening attack is 0.8.

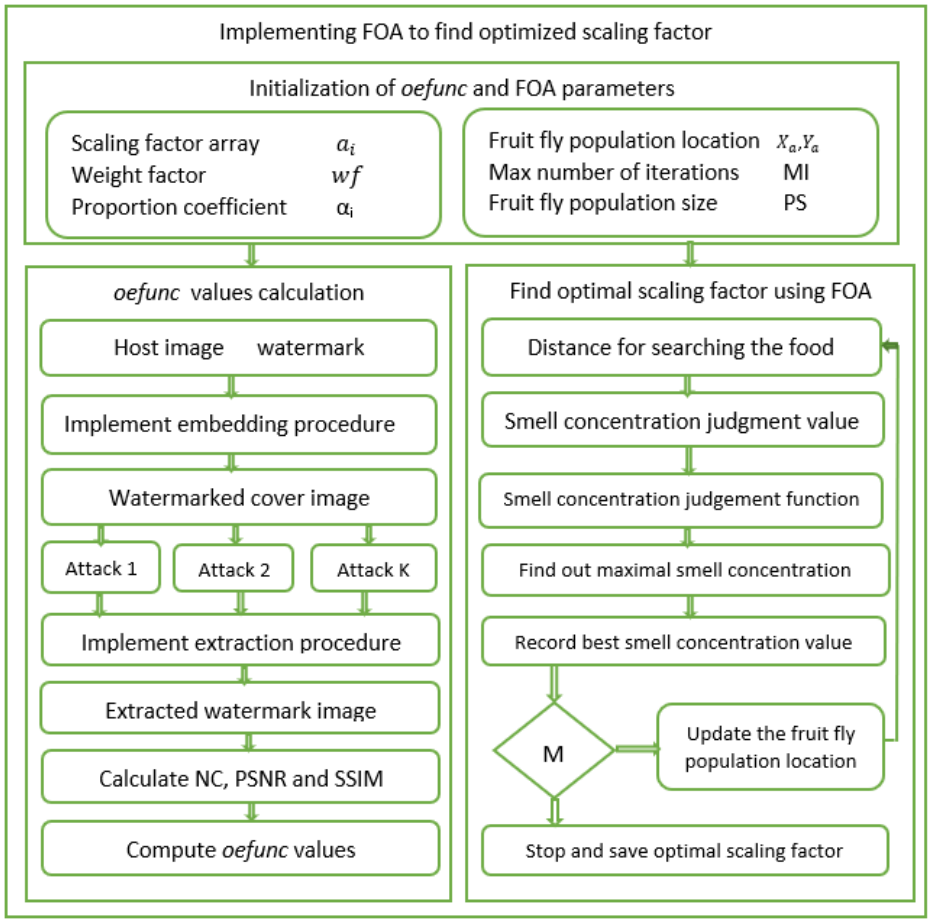

Fig-3: Optimization of the Scaling Factor using Fruit Fly Optimization Algorithm

4.1 INVISIBILITY AND ROBUSTNESS ANALYSIS:

For the information to be safe the watermark image that is embedded in the cover image should be invisible to the human eye. Hence the invisibility of the watermark image that is embedded will determine the performance of any watermarking method. The watermarked cover images with watermarks of sizes 64×64, 128×128 and 256×256 with their respective PSNR and SSIM values are shown in Fig-5(a), 5(b) and 5(c). The extracted watermarks of sizes 64×64, 128×128 and 256×256 with their corresponding NC values are displayed in Fig-6(a), 6(b) and 6(c) respectively. The watermarked cover image is only satisfied if the watermark is invisible. Hence only if PSNR>33(without any attacks), SSIM>0.93(without any attacks) is obtained, then the visual difference between the cover image and the watermarked

cover image is very insignificant [26]. These result shows that proposed watermarking method satisfies the requirements of invisibility.

If invisibility is acceptable then robustness must be further evaluated. In watermarking method for the system to be robust the watermark must be extracted without any changes or degradation of quality after attacking using various attacks. Therefore, the watermark image quality evaluates the robustness of the model. NC values determine the robustness. Tables 2, 3 and 4 shows the PSNR, SSIM and NC values of watermarks of sizes 64×64, 128×128 and 256×256 respectively. From the NC values shown in the Table 2, 3 and 4 it can be analysed that method is highly robust. Therefore, the proposed watermarking method has performed well and satisfied the requirements of both the invisibility and robustness.

4.2 FALSE POSITIVE PROBLEM ANALYSIS:

It is one of the important concerns, in the Singular Value Decomposition based watermarking method. Here a feigned watermark could be assumed as the original watermark image. In order to avoid this problem, the watermark image components, L and R^T of the Singular Value Decomposition should undergo encryption to be able to resolve the above problem. Here a simple and faster encryption method is proposed, where L and R^T will undergo encryption by a chaotic system which can be generated by the Logistic map equation which is expressed by

$$x(n+1) = rx(n)\big(1 - x(n)\big), x(i)\epsilon(0,1), \quad (25)$$

Algorithm to encrypt the components of SVD:

Input: component of SVD

Output: encrypted component of SVD

1.Initialize the values of r and $x(1)$ as 3.62 and 0.7

2.Compute the size of both the row and column of the input.

3.Calculate total number of elements in the input i.e., $s = row \times column$.

4.Iterate $(s-1)$ times the logistic equation and a chaotic sequence vector x will be obtained.

5. Sort the x vector in the ascending order and return the sorted x values and the original location of the values in the unsorted, original vector by using the sort function i.e., [so,in] = sort(x)

6.Then shuffle the elements or the pixel values of the input, according to the order that has been obtained by using the sort function. Now as the pixels are reshuffled the image is encrypted.

7.Finally, reshape the obtained encrypted image according to the dimensions of the original input image which will be our required encrypted component of SVD

The decryption procedure is the inverse of the encryption procedure. Hence, by including this in the model, the FPP can be avoided.

Attack	Specifications
Filter attack	Median filter (3X3) Gaussian low-pass filter (3X3) Average filter (3X3)
Noise attack	Gaussian noise (V=0.001) Salt & Pepper noise (0.001) Speckle noise (0.001)
Compression attack	JPEG compression (QF=50) JPEG2000 compression (CR=12)
Motion blur attack	Motion blur (Theta=4, Len=7)
Sharpening attack	Sharpening (0.8)

Table 1: attacks used in this model

Fig-4(a): Cover image of size 512 ×512

Fig-4(a)

Fig-4(b)

Fig-4(c)

Fig-4(d)

Fig-4(b): Watermark image of size 256×256
Fig-4(c): Watermark image of size 128×128
Fig-4(d): Watermark image of size 64×64

Table 2: PSNR, SSIM and NC values for Watermark of size 64×64

Attack	Watermark of size 64×64		
	PSNR	SSIM	NC
No Attack	34.8743	0.998	0.99997
Median filter	32.1805	0.92168	0.99949
Gaussian low-pass filter	31.4468	0.9135	0.99591
Average filter	31.3769	0.91154	0.99575
Gaussian noise	28.778	0.694	0.99972
Salt & Pepper noise	32.1344	0.9711	0.99989
Speckle noise	32.1016	0.87033	0.99991
JPEG compression	32.3018	0.917	0.99989
JPEG2000 compression	33.2283	0.93403	0.99983
Motion blur	27.8309	0.83063	0.95965
Sharpening	31.8899	0.96199	0.99792

Fig-5(a): Watermarked image (64×64)

Table 3: PSNR, SSIM and NC values for Watermark of size 128×128

Attack	Watermark of size 128×128		
	PSNR	SSIM	NC
No Attack	40.4099	0.99896	0.9035
Median filter	34.3523	0.92328	0.98002
Gaussian low-pass filter	33.2581	0.91526	0.9035
Average filter	33.1478	0.91332	0.90025
Gaussian noise	29.6167	0.69577	0.99563
Salt & Pepper noise	34.4272	0.97123	0.99937
Speckle noise	34.2988	0.87426	0.99903
JPEG compression	34.4857	0.91831	0.99945
JPEG2000 compression	36.2285	0.93573	0.99885
Motion blur	28.5276	0.83281	0.55344
Sharpening	33.6903	0.96242	0.95649

Fig-5(b): Watermarked image (128×128)

Table 4: Watermark of size 256×256

Attack	Watermark of size 256×256		
	PSNR	SSIM	NC
No Attack	34.4444	0.99739	1
Median filter	32.1216	0.92429	0.9732
Gaussian low-pass filter	31.5599	0.9167	0.89205
Average filter	31.4917	0.91481	0.88919
Gaussian noise	28.669	0.6967	0.98183
Salt & Pepper noise	31.7861	0.96862	0.99775
Speckle noise	31.8613	0.87041	0.99703
JPEG compression	32.0661	0.91794	0.99978
JPEG2000 compression	32.921	0.9344	0.99859
Motion blur	27.9727	0.83418	0.67044
Sharpening	31.1292	0.95818	0.94254

Table 5: Comparison with [21]

Attacks	[21]	In this work
No Attack	1.0000	1.0000
Median filter (3×3)	0.9734	0.9732
Gaussian low-pass filter (3×3)	0.9784	0.89205
Gaussian noise (M=0, V=0.005)	0.8018	0.98183
Salt & pepper noise (0.001)	0.9783	0.99775
JPEG compression (QF=40)	0.9808	0.99978
JPEG compression (QF=50)	0.9852	0.99978
Sharpening (0.8)	0.9239	0.94254

Fig-6(a): Extracted watermark (64×64)

Fig-6(b): Extracted watermark (128×128)

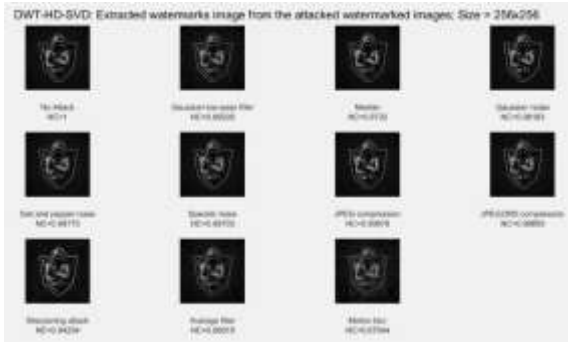

Fig-6(c): Extracted watermark (256×256)

Table 6: Comparison with [32]

Attacks	[32]	In this work
No Attack	1	0.99997
JPEG compression (QF=95)	1	0.99989
3×3 Gaussian filter with deviation 0.5	0.9910	0.99591
Sharpening (0.2)	0.9957	0.99792

Table 7: Comparison with [26]

Attacks	[26]	In this work
JPEG compression (QF=25)	1	0.99945
Gaussian noise with variance 0.002	0.9920	0.99563
Salt and pepper noise with density 0.001	0.9975	0.99937
3×3 Gaussian filter with deviation 3	1	0.9035
4 ×4 median filter	1	0.98002

Table 8: Comparison with [33]

Attacks	[33]	In this work
JPEG compression (QF=70)	0.9993	0.99983
Gaussian noise with variance 0.001	0.9833	0.99972
3×3 median filter	0.9933	0.99949

4.3 COMPARISION OF PERFORMANCE WITH OTHER RELATED WORKS:

The proposed method is compared with the ABC-based watermarking [21], FOA based watermarking [33] and firefly algorithm based watermarking method [32], [26]. The comparison with swarm intelligent optimization-based ABC algorithm [21] is shown in Table 5, for this comparison the cover image size is 512×512 and the watermark image size is 256×256. Table 5 show that the Normalized Correlation values of the proposed method under the attack of median filter and Gaussian low pass filter are slightly less than [21], but NCs under remaining attacks are greater than [21]. Hence the proposed method has overall strong robustness.

In comparison with [32], [26], [33] the cover image size is 512×512 and the watermark image size is 64×64. Table 6 shows comparison of the proposed method with [32]. NCs under the 3×3 Gaussian filter attack with deviation 0.5 and the Sharpening (0.2) attack which are greater in the proposed method compared to [32]. Table 7 shows comparison between the proposed method with [26]. The proposed method's NCs under the attack of Gaussian noise with variance 0.002 and Salt and pepper noise with density 0.001 are higher compared to [26]. The NCs of the proposed method under other attacks are slightly small or approximately to the NCs of [32] and [26]. Table 8 show the comparison of the proposed method with [33]. The proposed method's NCs under the attack of JPEG compression (QF=70), Gaussian noise attack with the variance of 0.001 and 3×3 median filter is higher compared to [33].

5 CONCLUSIONS:

In this paper, an image watermarking method is proposed based on DWT-HD-SVD transformations. The Fruit fly optimization algorithm is employed in obtaining the optimized scaling factor. The performance measures, both the invisibility and the robustness were analysed and observed with the help of numerical simulation experiments. From the results we can observe that the watermarked cover image has a good visual quality, PSNR and SSIM values. The NC values obtained are relatively good and the watermark extracted is clear after attacking with different attacks. In this model, a good amount of both the invisibility and robustness are achieved for watermarks of different sizes. The proposed model proves to be highly robust enough to defend filter, compression, noise and sharpening attacks, but the method must further improve in future to resist more attacks like cropping attack and rotation attack.

REFERENCES:

1. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, ''Secure spread spectrum watermarking for multimedia,'' IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
2. X. Li, S.-T. Kim, and I.-K. Lee, ''Robustness enhancement for image hiding algorithm in cellular automata domain,'' Opt. Commun., vol. 356, no. 1, pp. 186–194, 2015.
3. G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, (2018), "A new watermarking scheme for medical images with patient's details", International Journal of Engineering and Technology (UAE), 7, pp:25–29.
4. N. Nikolaidis and I. Pitas, ''Robust image watermarking in the spatial domain,'' Signal Process., vol. 66, no. 3, pp. 385–403, 1998.
5. J. Song, J. Song, and Y. Bao, ''A blind digital watermark method based on SVD and chaos,'' in Proc. Int. Workshop Inf. Electron. Eng., 2012, pp. 285–289.
6. T. K. Tsui, X.-P. Zhang, and D. Androutsos, ''Color image watermarking using multidimensional Fourier transforms,'' IEEE Trans. Inf. Forensic Security, vol. 3, no. 1, pp. 16–28, Mar. 2008.
7. V. Solachidis and L. Pitas, ''Circularly symmetric watermark embedding in 2-D DFT domain,'' IEEE Trans. Image Process., vol. 10, no. 11, pp. 1741–1753, Nov. 2001.
8. P. Tao and A. M. Eskicioglu, ''An adaptive method for image recovery in the DFT domain,'' J. Multimedia, vol. 1, no. 6, pp. 36–45, 2006.
9. S. D. Lin and C.-F. Chen, ''A robust DCT-based watermarking for copyright protection,'' IEEE Trans. Consum. Electron., vol. 46, no. 3, pp. 415–421, Aug. 2000.
10. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, ''A DCT-domain system for robust image watermarking,'' Signal Process., vol. 66, no. 3, pp. 357–372, May 1998.
11. J. C. Patra, J. E. Phua, and C. Bornand, ''A novel DCT domain CRTbased watermarking scheme for image authentication surviving JPEG compression,'' Digit. Signal Process., vol. 20, no. 6, pp. 1597–1611, 2010
12. F. Ernawan and M. N. Kabir, ''A robust image watermarking technique with an optimal DCT-psychovisual threshold,'' IEEE Access, vol. 6, pp. 20464–20480, 2018.
13. A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, ''Multiple watermarking technique for securing online social network contents using back propagation neural network,'' Future Gener. Comput. Syst., vol. 86, no. 1, pp. 926–939, 2018.
14. A. K. Singh, ''Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images,'' Multimedia Tools Appl., vol. 76, no. 6, pp. 8881–8900, 2017.
15. Y. Wang, J. F. Doherty, and R. E. V. Dyck, ''A wavelet-based watermarking algorithm for ownership verification of digital images,'' IEEE Trans. Image Process., vol. 11, no. 2, pp. 77–88, Feb. 2002.
16. M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, ''Hiding digital watermarks using multiresolution wavelet transform,'' IEEE Trans. Ind. Electron., vol. 48, no. 5, pp. 875–882, Oct. 2001.
17. Z. H. Wei, P. Qin, and Y. Q. Fu, ''Perceptual digital watermark of images using wavelet transform,'' IEEE Trans. Consum. Electron., vol. 44, no. 4, pp. 1267–1272, Nov. 1998.
18. N. Muhammad and N. Bibi, ''Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain,'' IET Image Process., vol. 9, no. 9, pp. 795–803, Sep. 2015.
19. X. Ye, X. Chen, M. Deng, and Y. Wang, ''A SIFT-based DWT-SVD blind watermark method against geometrical attacks,'' in Proc. 7th Int. Congr. Image Signal Process., Oct. 2014, pp. 323–329.
20. G. Nagaraju, M. Venkata Pullarao, P. V. Ramaraju, (2019), "A compound transform domain-based watermarking scheme for colour images", Journal of Advanced Research in Dynamical and Control Systems, 11(1), pp:1687–1694.
21. I. A. Ansari, A. Pant, and C. W. Ahn, ''Robust and false positive free watermarking in IWT domain using SVD and ABC,'' Eng. Appl. Artif. Intell., vol. 49, pp. 114–125, Mar. 2016.
22. Q. Su, ''Novel blind colour image watermarking technique using Hessenberg decomposition,'' IET Image Process., vol. 10, no. 11, pp. 817–829, Nov. 2016.
23. Q. Su and B. Chen, ''A novel blind color image watermarking using upper Hessenberg matrix,'' AEU-Int. J. Electron. Commun., vol. 76, no. 6, pp. 64–71, 2017.
24. R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, ''An improved SVD-based watermarking technique for copyright protection,'' Expert Syst. Appl., vol. 39, no. 1, pp. 673–689, 2012.
25. W.-T. Pan, ''A new fruit fly optimization algorithm: Taking the financial distress model as an example,'' Knowl.-Based Syst., vol. 26, pp. 69–74, Feb. 2012.
26. Y. Guo, B. Z. Li, and N. Goel, ''Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain,'' IET Image Process., vol. 11, no. 6, pp. 406–415, Jun. 2017.

27. S. Thakur, A. Singh, and S. Ghrera, ‘‘NSCT domain–based secure multiple-watermarking technique through lightweight encryption for medical images,’’ Concurrency Comput., Pract. Exper., vol. 31, p. e5108, Dec. 2018.
28. G. Nagaraju, Dr. P.V. Ramaraju, P. Udaya Bhanu, Y.S.V. Satyavathi, T.Srinadh, K.Ganesh, K.Hari Subrahmanyam, (2020), “Optimized Image Watermarking Scheme Based on IWT and DCT”. International Journal of Advanced Science and Technology, 29(4), pp:132-147.
29. S. Thakur, A. Singh, and S. Ghrera, ‘‘NSCT domain–based secure multiple-watermarking technique through lightweight encryption for medical images,’’ Concurrency Comput., Pract. Exper., vol. 31, p. e5108, Dec. 2018.
30. R. Mehta, N. Rajpal, and V. P. Vishwakarma, ‘‘LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR,’’ Multimedia Tools Appl., vol. 75, no. 7, pp. 4129–4150, 2016.
31. G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, Sateeshkumar Deevi, (2020), “An Intelligent Watermarking Technique for Secured Medical Images with Patient Health Document”, The J.of Research on the Lepidoptera, 51(3), pp:1-17.
32. A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, ‘‘Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm,’’ Expert Syst. Appl., vol. 41, no. 17, pp. 7858–7867, 2014.
33. Z. Xiao, J. Sun, Y. Wang, and Z. Jiang, ‘‘Wavelet domain digital watermarking method based on fruit fly optimization algorithm,’’ J. Comput. Appl., vol. 35, no. 9, pp. 2527–2530, 2015.
34. Nagaraju G, Ramaraju PV, Chaitanya RK, (2015), “Image encryption and decryption using Advanced Encryption Standard Algorithm”, Discovery, 29(107), pp:22-28.
35. Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, ‘‘A blind double color image watermarking algorithm based on QR decomposition,’’ Multimedia Tools Appl., vol. 72, no. 1, pp. 987–1009, 2014.
36. G. Naga Raju, Dr. P V Rama Raju, P. Udaya Bhanu, P V V Abhilash, M S S S L Prasad, N Keerthi, P Satish, (2020), “A Hybrid Encryption Technique for Data Embedding in Medical Images”. International Journal of Advanced Science and Technology, 29(4), pp:116-131.

ABOUT AUTHOURS:

Dr. G. NAGA RAJU

Presently working as assistant professor in Dept. of ECE, S.R.K.R. Engineering College, Bhimavaram, AP, India. He received B.E. degree from S.R.K.R Engineering College, Bhimavaram in 2002, M.E. degree in Computer electronics specialization from Govt. College of Engg., Pune University in 2004 and Doctorate from Department of ECE, KL University, Vaddeswaram in 2021. His current research interests include Image processing, digital security systems, Signal processing, Biomedical Signal processing, and VLSI Design.

P. UDAYA BHANU

Presently working as assistant professor in Dept. of EEE, S.R.K.R. Engineering College, Bhimavaram, AP, India. She received B.Tech degree from DNR College of Engineering and Technology, Bhimavaram in 2016, and M.Tech degree in Power Systems and Automation specialization from S.R.K.R Engineering College, Bhimavaram in 2018. Her current research interests include Signal processing, Image processing, power systems and automation.

T. VIDYA PRAVALLIKA

Presently pursuing Bachelor of Engineering degree in Electronics &Communication engineering S.R.K.R. Engineering College, AP, India.

P. DURGA RAO

Presently pursuing Bachelor of Engineering degree in Electronics &Communication engineering S.R.K.R. Engineering College, AP, India.

V. KUMARA SANKARA

Presently pursuing Bachelor of Engineering degree in Electronics &Communication engineering S.R.K.R. Engineering College, AP, India.

S. TEJA NAGA KRISHNA VARMA

Presently pursuing Bachelor of Engineering degree in Electronics &Communication engineering S.R.K.R. Engineering College, AP, India.