

DWT & SVD Based Digital Image Watermarking Using an Optimization with ANN Approach

Shivani

M. tech Scholar , Computer science and engineering, Krishna Institute Of Engineering and Technology,Uttar Pradesh, India.
shoisingh@gmail.com

Abstract— You can use a watermarking system to encrypt and safeguard any kind of data, from text to photos to audio and video. We decided to concentrate on image-based watermarking for security reasons. Any user with access to the source data can alter information shared on social media. Several watermarking techniques have been developed in response to this demand for secrecy. In the first, the watermark is visible to all users regardless of file type, whereas in the second, only the administrator can see it. Proposed research employs scalar value decomposition (SVD), a type of wavelet transform, and discrete wavelet transforms (DWTs) for decomposition and extraction (Singular Vector Decomposition). Consequently, our proposed approach heavily employs DWT and SVD, two decomposition methods having advantages over their competitors but also their own limits. Once the image data is collected, it can be optimised using a method like a Genetic Algorithm to produce the best results. In this study, we introduce a novel hybrid Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) digital watermarking technique (SVD). An embedding key and watermark are added to the host image for added security and viewer verification in multimedia files. The host image and the watermark image are disassembled using a 2-level DWT strategy as part of the embedding procedure. A further subdivision of the pixel depths is achieved by the SVD technique. To further improve the stealthiness of the watermarked image, we apply a novel fitness function of genetic algorithm (GA) to the pixels generated by the SVD. Images, both unaltered and with watermarks, can now be used to teach a computer vision system (ANN). So that the watermark would be most difficult to remove, the trained network was utilised to choose the optimal area in the original image on which to place it. With this method, data loss is reduced to a minimum. Experimental results showed that the proposed method improved PSNR above that of the preceding work by Sangeetha et al (2018).

Keywords— DWT, SVD, WATERMARKING, DIGITAL IMAGE WATERMARKING.

I. Introduction

Since the Internet is so pervasive, data security is a primary motivation for watermarking. When duplicating a document and delivering it to a big number of people requires minimal work. Once the articles have been downloaded and shared, they can be revised. Therefore, it is essential to refine and improve the watermarking technique for safeguarding sensitive information. After the watermark is placed, the original data is altered such that it no longer takes up as much room as before. In the context of media, "watermarking" refers to the practise of adding a digital signature, logo, or script to an image, audio file, or video. These kind of procedures have been in use for some time. It was in Italy, around the year 1282, that the first watermarked paper appeared. Starting with a

tiny wire attached to the paper mould, an external label is created. The initial purpose of these watermarks has not been determined. A watermark is a hidden message embedded into the source material or host signal to prevent tampering or duplicating. Even while audio, video, text, and photos can all benefit from watermarking, we will be concentrating on still shots here.



Figure 1.1 Watermarked Image

The image watermark used to encrypt the shown image is shown in Figure 1.1. Image watermarking is useful in many contexts, including copyright protection, medical security, fingerprinting, copy protection, broadcast surveillance, data encryption, encoding, information concealing, and many more besides. Images can be "watermarked" with text, other images, audio, or video without detracting from the quality of the original. Figure 1.2 illustrates how watermarks can be sorted according to their host signal, perceptivity, robustness, and watermark type.

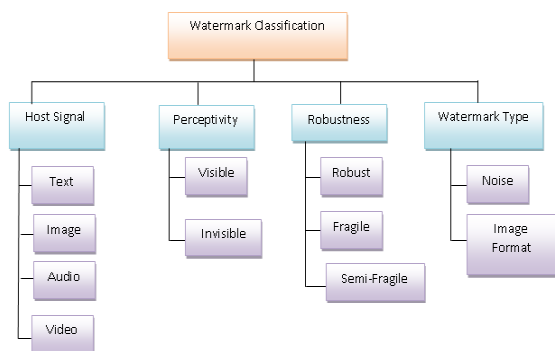


Figure 1.2 Watermark Classification [5]

Process Of Watermarking

Generally speaking, the watermark, the cover object, and the secret key are the inputs to the embedding approach, which is represented in Figure 1.3. With the help of the key, the watermark is secured and fortified.

Only the data's owner has the key necessary to remove the watermark. Lossy compression, geometric distortions, signal processing methods, and the conversion from digital to analogue and back again are all potential risks to the watermarked image as it travels through the transmission channel.

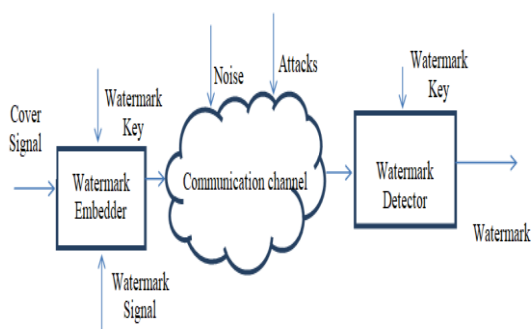


Figure 1.3 Process of Watermarking [12]

Watermarked data might potentially be transmitted through a channel with significant loss, interference, and unreliability. This allows the received data to be distinguished from the watermarked original. Information is watermarked and must be removed using the same key that was used to embed it. Watermarked data is what comes out of watermarking processes [12].

II. Literature Review

Sangeetha, N., & Anita, X. (9, 2018), have proposed a new watermarking image model using host entropy and watermark image texture. The method evaluates the entropy of the host image by calculating the coefficients of the discrete wavelet transform. The sub-band with the most entropy serves as a background for the watermark's textured imprint. The watermark is created by transforming a procedurally generated texture using the Arnold transform. Instead of using a watermark, a texture could be used for added security. It has been shown experimentally that the proposed entropy-based sub-band range, linear weight assessment, watermark embedding, and watermark host extraction all work as intended. Experiments show that by employing this technique to separate the watermark from the host item, watermark concealment can be greatly enhanced.

Thakkar, F. N., & Srivastava, V. K. (24, 2017), have proposed a blind object watermarking scheme is based on discrete wavelet transformation (DWT) and singular value decomposition (SVD). In this case, we use DWT to analyse a local region of a biological image and separate it into its component colours (ROI). A logo and an identification were used to confirm the medical image's authenticity. The watermark and accompanying text ensure the integrity of electronic health records (EPR). A comparison mechanism similar to that employed during embedding is utilised to carry out blind recovery of both watermarks at the receiving end. The proposed method is compatible with many different kinds of diagnostic imaging techniques. Combining the discrete wavelet transform and the singular value decomposition, this method enhances the readability of the watermarked image and the chances of its recovery.

Ansari, I. A., & Pant, M. (25, 2017), have proposed, a multi-purpose image watermarking scheme to provide host image verification of tamper location, self-recovery and ownership. To make the proposed method more flexible and widely applicable, we employ a grey watermark for genuine watermarking. First, the host must be transformed into the DWT (Discrete Wavelet Transform) domain, and then its values must be adjusted so that they are consistent with the watermark's theoretical underpinnings. By include them, we can reduce the number of false positives and increase our productivity. When implementing a robust watermark, the final two LSBs (Least Significant Bits) of the host are altered in such a way that the SVD decodes a muddled but computationally tractable average representation of the host (Singular Value Decomposition).

Qin et al. (26, 2017), have presented a novel fragile watermarking strategy focused on simultaneous embedding scheme including high-quality recovery capabilities. The proposed method incorporates both the frameworks for material recovery and pixel-by-pixel localisation. This is accomplished by first calculating the average value of the overlapping blocks through the interleaving process, and then randomly inserting the reference bits into either the LSB layer of the horizontal-vertical mode picture, or the USB layer of the diagonal mode picture, respectively. Each block's authentication bits are concealed by a sequence of adaptive core LSB layers whose depth grows in proportion to the complexity of the block, ensuring their safety at all times. After manipulative blocks are identified and mean-value bits are rebuilt, three pixel-wise restoration techniques are utilised to return the pixels with the aid of certain overlapping, conflicting frames, which may result in greater visual quality of restored results.

Shehab et al. (27, 2018), have proposed a modern fragile watermarking method for authentication of image and clinical self-recovery and also retrieves the original image and locates manipulation of image. Singular value decomposition (SVD) is used to evaluate a transformation in a host image by inserting block-wise SVD traces into the least significant bit of image pixels. The proposed method will be put through its paces in a number of different contexts,

such as those involving text erasure, text intrusion, and copy/paste attacks. The proposed method outperforms the state-of-the-art in two critical areas: localization accuracy and the peak signal-to-noise ratio of the independently reconstructed image.

Al-Haj et al. (28, 2017), have presented a blind, imperceptible, and stable 3D DIBR digital watermarking algorithm based on two computational transformations, Combining DWT and SVD, or the Discrete Wavelet Transform and Singular Value Decomposition. There are two different but complementing robustness rates that the two transformations have against watermarking assaults. Using a sample set of monocular objects and their corresponding per-pixel map pictures, the undetectability and dependability of the proposed technique are demonstrated. Analysis results showed the approach to be detectable and robust against generic signal processing assaults and DIBR-specific attacks such as depth picture pre-processing and baseline distance ratio alteration.

Zear et al. (29, 2018), A multi-watermarking approach based on discrete wavelet transform, discrete cosine transform, and singular value decomposition has been developed for usage in medical settings (SVD). In order to verify the identity of the sender and the recipient, this technique uses a Lump watermark on medical photographs, a doctor's signature or identifying key, and text watermarked diagnostic information about the patient. The created picture watermark is then fortified against noise using a back propagation neural network (BPNN).

Singh, A. K. (30, 2017), have presented a state-of-the-art, resilient multi-watermarking hybrid technique by fusing DWT, DCT, and SVD rather than implementing DWT, DCT, and SVD independently or integrating DWT-SVD or, by merging DCT-SVD. As a result, many watermarks, including text and images, are incorporated in a single interactive object to increase security while remaining largely undetectable. To speed up the embedding and extracting procedures, this system employs a straightforward encryption mechanism. Overall, this method outperforms the other recorded methods in terms of robustness and embedding

efficiency, suggesting its potential utility in medical applications concerned with preventing patient identity theft.

Zhou et al. (31, 2018), have advocated for a hybrid watermarking system that is both secure and efficient. Watermarking techniques like singular value decomposition (SVD) and discrete wavelet transformation (DWT) have emerged and found widespread application in recent years. The direct current (DC) coefficients of the high-frequency sub-bands (LH and HL) generated by block-based APDCBT are modulated with watermarking, making the watermark more difficult to detect. This method yields lower-quality watermarked photos compared to the more popular SVD-based watermarking approach and other methods.

Bajracharya, S., & Koju, R. (32, 2017), have presented YCbCr Color Space Hidden Robust Digital Watermarking using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). When it comes to resistance to different kinds of geometric attacks, the proposed solution excels over previous work. Non-blind digital watermarking is used because the watermark cannot be erased without the cover image. The authors claim to have found striking parallels between the cover and watermarked images, indicating that imperceptibility can be detected with a sufficiently high signal-to-noise ratio (PSNR). Even after being exposed to repeated geometric attacks, a watermark with a high normalised cross correlation (NC) value demonstrates that the original watermark and the derived watermark are substantially similar. Based on these evaluations, it would appear that the proposed method is far more stable than the present state of the art.

Singh, D., & Singh, S. K. (33, 2017), a new robust and blind watermarking technique based on DWT-SVD and DCT encrypted with the Arnold Cat Map have been proposed for copyright protection. This solution solves two problems that have plagued SVD-based watermarking methods: unauthorised decryption and false-positive detection. This eliminates the requirement to find a suitable scaling factor, making the proposed method much more convenient. The proposed method eliminates the risk of erroneous positive detection. Both

intentional and unintentional attacks against the watermarking method were undertaken. System reliability and durability were top priorities during development. Every grey watermark pixel's most significant bit (MSB) and least significant bit (LSB) are used to make a checkerboard design (LSBs). At the one-level, the DWT sub-bands of the host frame hold the Discrete Cosine Transform (DCT) coefficients for the midsingular value of each block of size 4×4 .

Liu et al. (34, 2017), created a fresh digital image watermarking system proposed using fractal encoding and discrete cosine transform. Watermarking methods using fractal encoding and the discrete cosine transform (DCT) for double encryption are similar to this. A novel method has been proposed that significantly improves the privacy of individual photographs. Second, a fractal encoded watermark could modernise the look of an older logo while also making the watermark thinner. The watermark is embedded in the carrier via DCT, which is permanent. You can now choose between three distinct possibilities rather than just two (scale and offset) as before. The system was put through its paces with three separate attacks. Our experimental results indicate the usefulness and usability of our suggested approach by comparing it to the gold standard methods of principal component analysis and two-dimensional principal component analysis.

Ojha et al. (35, 2018), developers have recommended adopting a reliable and effective watermarking method to reclaim ownership and fix the security flaw. With more and more people turning to the internet for their news, entertainment, and other information and communication needs, protecting creators' rights to their multimedia works like films, albums, and songs is more important than ever. For the purpose of protecting the essential part of the cover image that was taken off during cropping, this solution makes use of a cutting-edge watermarking technique based on Discrete Wavelength Transform (DWT) and Decomposition of Singular Value (SVD). Cover image watermarking is done with SVD and ROI processing is done with DWT. The proposed method is unaffected by common geometric and filtering attacks including cropping, rotation, Poisson noise, Gaussian noise, etc.

Assini et al. (36, 2017), have suggested a hybrid multiple watermarking technique, DWT- FWHT-SVD, to secure medical photos by embedding two watermark images, "Barbara" and "Fingerprint," inside a single cover medical image in DWT's high-frequency sub-band HH. Protecting sensitive patient information and preventing fraud of any type can be accomplished by incorporating multiple watermarks onto the cover image. With the benefits of DWT, FWHT, and SVD combined, this watermarking method produces high-quality outcomes in terms of stealth, durability, and efficiency.

Panda et al. (37, 2017), have introduced a new variant of the DWT-SVD watermarking technique using the Genetic Algorithm. A watermark image's single value component can be adjusted by scaling the image up or down by the right amount. GA optimises this scaling function to obtain high values and resilience without sacrificing the watermark's transparency using the PSNR values as the fitness criterion. Applied researchers are increasingly putting the Noise Correlation to use as a fitness technique for robustness testing.

III. Problem Formulation

Despite extensive research, much of it fails to recognize the strong security provided by watermark images. Digital watermarking, the process of discovering and devaluing hidden signals in the form of text, audio, image, and many others, is one way that security workers can fight back against data hiding techniques. We are still far from having a digital watermarking technique that is completely secure.

Within the scope of the proposed research, we employ a decomposition strategy (discrete-wavelet transform with singular-value decomposition), an artificial neural network (ANN), and an optimization technique to develop a practical and accessible digital image-based watermarking system. Pixels in the cover image are selected using artificial neural networks (ANNs), but finding the smallest and best-fitting region to insert the image inside is a separate challenge. Optimization is the problem; without it, we'd be trapped in a chaotic, noisy market. Since this optimization requires a lot of trial and error, we turn to a genetic algorithm (GA). To embed the secret/watermark image, they first categorise a region suitable for doing so, and

then use the SVD technique to generate a sample of pixels from the classified region to train the ANN. The main contributions of our work come from employing a Genetic Algorithm in tandem with DWT and SVD. Results metrics for digital watermarking photos with an Artificial Neural Network and a Genetic algorithm have been generated so that the proposed work can be compared to previous work.

IV. Methodology

Digital watermarking with DWT and SVD is explained, as is optimization using an AI-based method. The digital watermarking technology discussed here is adaptable and can be utilised in a wide range of secure settings. Digital watermarking entails the transmission of information together with a covert watermark image, which is subsequently decoded at the receiving end using an encryption key. This method could be used to establish data reliability or to validate the identity of a digital asset's owner. We have optimised an ANN method based on the DWT and SVD principles for security purposes. To select the best pixel group for hiding the watermark, the watermark image is split into the LL, LH, HL, and HH planes via the discrete wavelet transform (DWT) decomposition technique.

The main components and steps of digital watermarking are outlined in the image below. That images can be embedded and then extracted from a watermark is a necessary feature of any watermarking system. There are two critical components to successful embedding: the integrity of the watermarking image used on the test image and the precision with which the watermarked image is reconstructed.

A watermarking image is inserted into the original test image using some predetermined keys, and then the image and the embedded data are transmitted to the receiving end over some communication means. The watermarked version can be recreated from the original with the correct decryption key. Without the correct key, the watermark will remain on the image. The basic block diagram of the proposed work is given in figure 4.1.

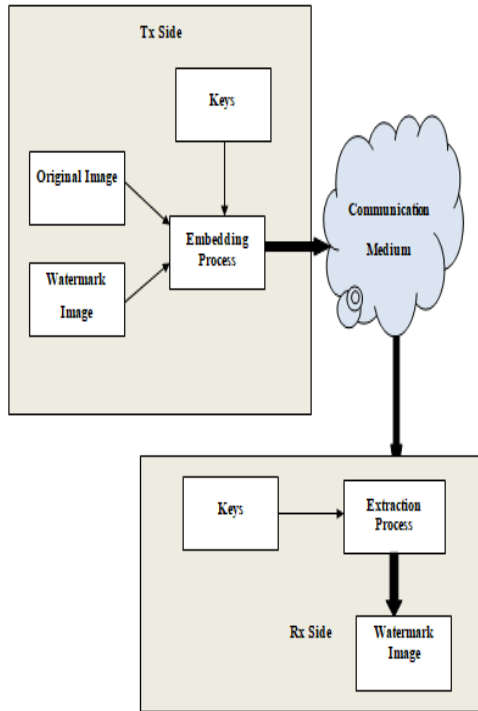


Figure 4.1 General Block diagram of digital watermarking system

To prove the efficacy of our watermarking system, we subject it to rigorous testing, including a battery of trials on several images and the use of an Artificial Neural Network optimised with a Genetic Algorithm. In the suggested study, several methods have been applied to ascertain which region of pixels should be used to insert the watermark and enhance the quality of extraction. The methodology of proposed work is given below with flow chart:

Step 1: “Design a proper GUI of proposed digital watermarking module”.

Step 2: “Develop a code to upload original image and watermark image from database for training and testing”.

Step 3: Apply pre-processing on uploaded original as well as watermark image. Pre-processing has followed few steps like as resizing, color conversion, image decomposition and many more. The entire process has been performed to obtained image with better quality and can be easily compatible for the present work. The histogram representation, which is a function of H_i has also been determined. The H_i count denotes the number of observations and known as bin. The histogram of an image can be represented mathematically as;

$$H_i = \sum_{i=1}^m \frac{1}{n_i} \quad (4.1)$$

Here,

H_i Histogram of an image

m Total number of bins

n Total number of observations

Step 4: Develop a code for the histogram construction of original image and then apply DWT & SVD on the pre-processed image. After pre-processing, optimization of obtained pixels has been done using metaheuristic inspired Genetic algorithm process of natural selection inspired algorithm. The GA helps to find best pixels from the SVD image of both original as well as watermark image.

Step 5: After that set the fitness function of Genetic Algorithm according to the requirement so we can find out the appropriate and optimal pixel group.

$$Fitness = \begin{cases} F_s(True) & \text{if } F_s \geq F_t \\ F_t(False) & \text{otherwise} \end{cases} \quad (4.2)$$

Where F_s is the selected value of feature and F_t is the threshold value of feature which is calculated by the given expression where n is the total number of feature and G is the feature value.

$$G_t = \frac{1}{n} \sum_{i=1}^n G_i \quad G_i = \frac{1}{n} (G_1 + G_2 + G_3 + \dots + G_i) \quad (4.3)$$

Step 6: Now, train ANN based on obtained optimized pixel of original as well as watermark image. Based on the trained network, the best region among the original image has been determined on which the watermark image has been embedded. This process helps to minimize the information loss.

$$Structure \ of \ ANN = B + W * \tanh(B + W * x) \quad (4.4)$$

Where W is the weights that are obtained from the input of ANN, x is the number of W and B is the bias. In the ANN a transfer function is needed to transfer the input data one layer to the other layer of network, so “tansig” is transfer function which is known as the tan sigmoid. The error during the learning is called the Mean Squared Error (MSE) and is defined as:

$$MSE_{ANN} = \frac{\sum_{i=1}^n (O_i - T_i)^2}{n} \quad (4.5)$$

in which, O_i is the desired output for the training data or cross-validation data i , T_i is the network output for the training data or cross-validation data i , and n is the number of data in the training data set or the cross-validation data set.

Step 7: After that generate an embedded key to embedding process.

Step 8: Embed the watermark image in the original image using their suitable region with the private key and apply image compression to reduce the size of embedded image for communication purpose.

Step 9: After the embedding phase extraction part enable and we extract the watermark image from the original image using authenticated key and if key is correct then we got the watermark image otherwise we cannot extract the watermark image.

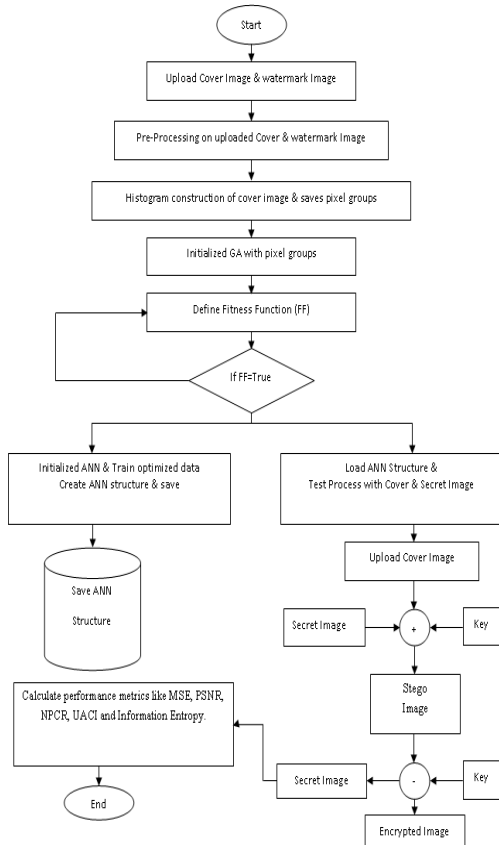


Figure 4.2 Flow chart of proposed work

Step 10: At the last we compute the performance metrics like MSE, PSNR, NPCR, UACI and Information Entropy.

Figure 4.2 shows the flow chart of proposed work for the DWT based method for digital watermarking image using Artificial Neural Network with Genetic Algorithm as an optimization technique. By using above procedure we achieve better results which are well described in the next section.

Techniques Used

In this work, DWT & SVD with GA has been used as an optimization algorithm in addition to ANN as a classification algorithm. The algorithms along with their uses in the research are provided below:

GENETIC ALGORITHM (GA)

Genetic algorithm is an optimization algorithm that is used to determine the appropriate and best pixel group. The used for GA is written as follows.

Algorithm 1: Genetic Algorithm

Input: Decomposed pixels by hybridization of DWT & SVD

Output: Best Pixel Sets

1 Define: Fitness Function:

$$Fit_{fun} = \begin{cases} Ture(T); & \text{if } P_{Val} < Th_{Val} \\ False(F); & \text{Otherwise} \end{cases}$$

Where, P_{Val} is pre-processed pixel value and Th_{Val} is the pixel's threshold value (mean of all pixel values)

2 Estimate, row (R) and columns (C) of pre-processed Image pixel

3 Initialize GA parameters

- Iterations (T)
- Population Size (P)
- Crossover function
- Mutation function
- Selection function (P_{Val} and $Threshold_{Val}$)

4 Best Pixel = []

5 for $i = 1 \rightarrow R$

6 for $j = 1 \rightarrow C$

$$7 \quad Pixel_{Val} = \sum_{i=1}^P Image(i)$$

$$9 \quad Th_{Val} = \frac{\sum_{i=1}^P Image(i)}{Length\ of\ Image}$$

$$10 \quad Fit\ Fun = Fit\ Fun(P_{Val}, Th_{Val})$$

11 Best Pixel =

GA (Fit Fun, Initialize Parameters)

12 end

13 "end"

14 "Returns: Best Pixel Sets"

15 "end"

ARTIFICIAL NEURAL NETWORK (ANN)

ANN, a categorization system inspired by the human brain, is composed of three distinct layers: input, intermediate, and output. To train an ANN network, the best possible set of pixels is used as input. The intermediate layer's pixels are modified using the sigmoid function. The training error is measured based on MSE parameters. The algorithm of ANN is written below;

ANN algorithm

Input: Initialize Embedded

Output: Range of pixels for embedding

Load optimized pixel as a training data

Training:

1 Initialize the basic parameters of ANN such as: –

Number of

– Number of Neurons (N)

Techniques: Levenberg Marquardt

Data Division: Random

1 for i = 1 \square **T**

2 if T = embeddable group of pixel

3 Group (1) = embeddable Pixels of the lower bit

4 else

5 Group (2) = Extra pixels or higher bit

6 end

7 end

8 Call and setup the ANN using Training pixel data and their Group

9 Net-DWM = Newff (T, G, N)

10 Net-DWM = Train (Net, T, G)

Testing or Embedding Phase:

11 Data-Test = Pixels of Cover Image

12 Pixel Sets Range = simulate (Net-DWM, Data-Test)

13 Return: Range of pixels for embedding

14 end

V. Results

This chapter explains the screenshots of design GUI in MATLAB simulator.



Figure 5.1 Main GUI of the Proposed Work

The main GUI of the proposed work is shown in Figure 5.1. The above figure represents the GUI mainly consists of two panels (i) embedded panel and (ii) Extraction Panel.

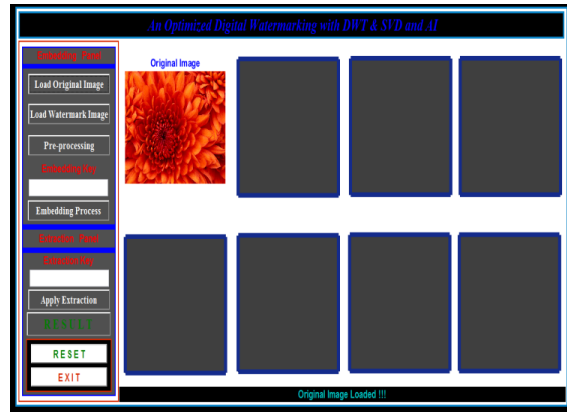


Figure 5.2 Uploading Original Image

After clicking on upload original image, the uploaded test image is shown in Figure 5.2. After uploading the original image, watermark image has been inserted as shown in Figure 5.3. This is done to protect image from the content theft. Once, the watermark image has been inserted in the test image no one can use it without your permission.

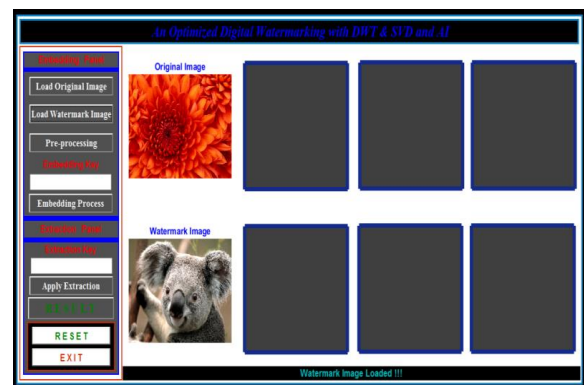


Figure 5.3 Upload Watermark Image

As can be seen in figure 5.4, pre-processing has now been conducted, which includes procedures like image scaling, color-to-grayscale conversion, and image deconstruction. The original and watermarked images' histograms have also been created. Both the original and watermarked images have had DWT and SVD applied to them.

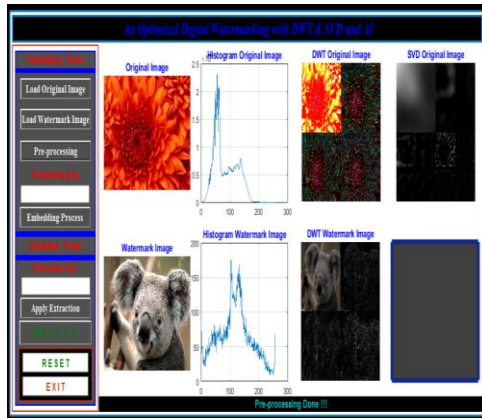


Figure 5.4 Pr-processed image

DWT is utilized in digital image watermarking because of its outstanding spatial localization along with multi resolution features. These features are identical to the theoretical model of the human visual system. Also, the performance of the digital watermarking system has been improved by increasing its level. In this case, the DWT upto 2 levels have been used. The four levels of the DWT image are depicted in Figure 5.4. Each comprises of LL, LH, HL and HH image. After applying DWT, SVD has been applied to break pixels into smaller one. This helps to reduce the information loss while extracting the embedded watermarking image.

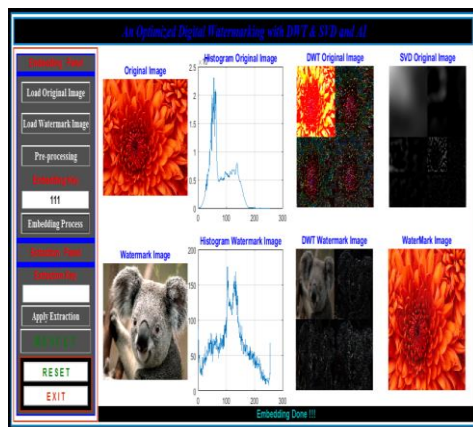


Figure 5.5 embedding

Now, genetic algorithm with an appropriate fitness function has been applied to obtain optimized histogram pixels.

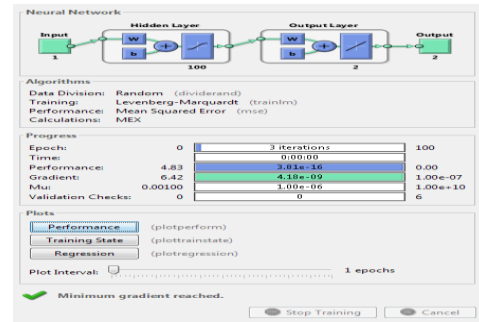


Figure 5.6 Training structure of ANN

The training structure of ANN after the training process of digital watermarking system is shown in Figure 5.6. The above figure comprises of four numbers of panels named as (i) Neural Network, (ii) Algorithm, (iii) progress and (iv) Plots. The neural network comprises of three number of layers input followed by hidden layer. The last one is the output layer. The algorithm that has been followed by ANN is listed under algorithm section: trained data is divided randomly and trained using levenberg- Marquardt principle. The performance has been measured in terms of mean Square Error and calculated as MEX.

The training progress is shown under progress panel and measured in terms of epoch, time, performance, gradient, mutation and validation checks. Among all the stated training progress if one of them is completed, the system is trained. The performance measured is described in the following section.

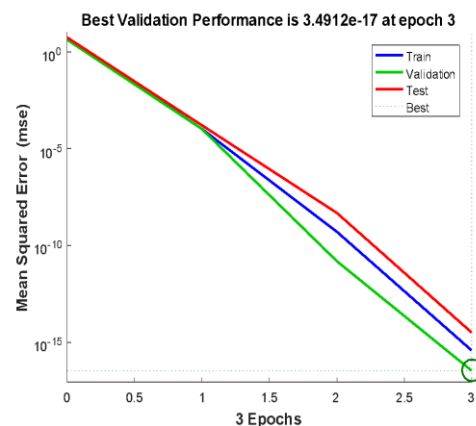


Figure 5.7 Performance

The performance measured in terms of Mean Square Error (MSR) is depicted in Figure 5.7. From the graph, the minimum MSE of about 3.491×10^{-17} has been obtained as denoted by green circle. The MSE obtained for training, validation and test data

are represented by the green, the blue and the red line.

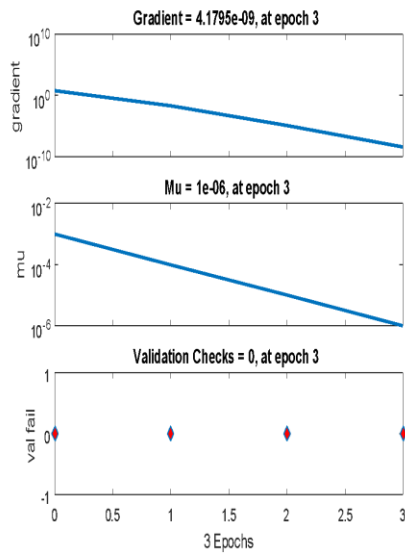


Figure 5.8 Training State

Figure 5.8 illustrated the training state of ANN classifier in the form of graph. The above graph is obtained after the completion of training process and contains waveform named as gradient, mutation and validation checks of with maximum values of 4.1795×10^{-9} , 1×10^{-6} and 0 respectively for maximum 3 epochs.

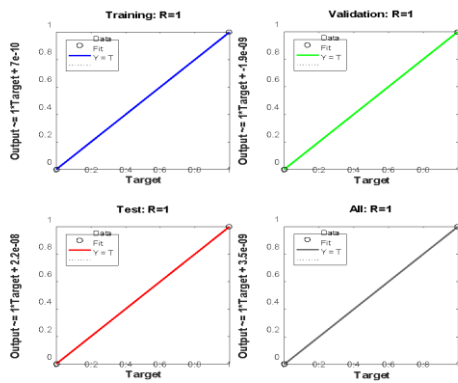


Figure 5.9 Regression

Regression parameter is used to validate the performance of the proposed digital watermarking system. The graph in Figure 5.9 represents the network output along with targets analyzed for training, validation and test data. The best training, the data must lie along the straight line marked at 45 degree at which the output of the system is equal to the target. For best fit, the R value must be higher than 0.93.

After training, the validation of the system has been performed by uploading test image along with watermark image. The test results analyzed by entering wrong embedding key and with accurate embedding key are shown in Figure 5.10 and 5.11 respectively.

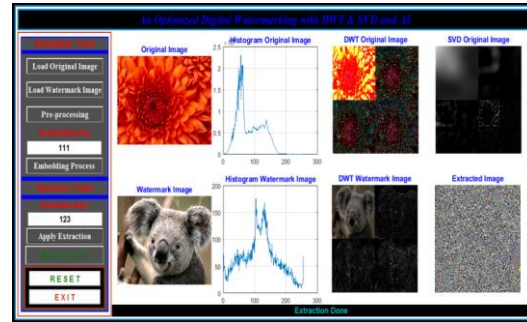


Figure 5.10 Result with wrong key

When wrong embedding key is entered, the watermark image has not been appeared under the extracted image as shown in above Figure 5.10.

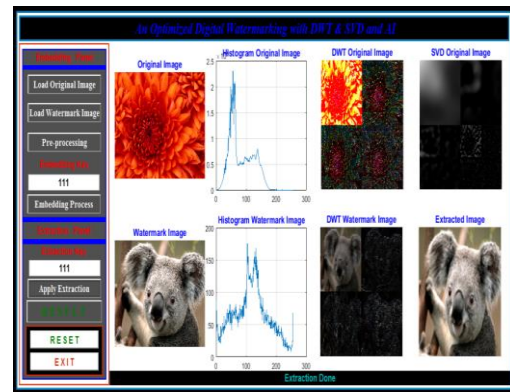


Figure 5.11 Result with correct key

After entering the correct key, an accurate watermark image, which is embedded during the transmission process is extracted and appear under the extracted image as shown in Figure 5.11. the results examined after extracting an accurate water mark image is shown in the screenshot provided in Figure 5.12.

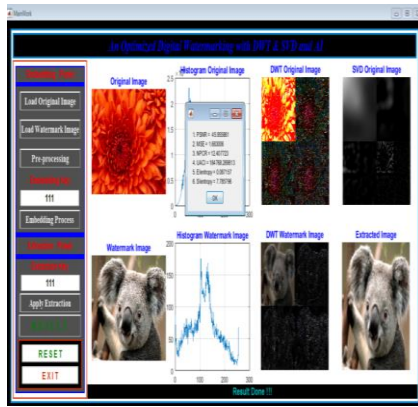


Figure 5.12 Results

The similar process is followed by embedding different watermark images to the test images and the parameter such as PSNR, MSE, NPCR, UACI, Elentropy and Slentropy have been measured.

PARAMETERS USED

To measure the efficiency of the designed digital watermarking system following parameters are evaluated:

i. "peak signal to noise ratio (PSNR)"

This shows the quality of the hidden watermark image belonging to the original image. This can be stated as:

$$PSNR = 20 \frac{Max_f}{\sqrt{MSE}}$$

Max_f Signify the amount of pixels in the watermark image.

ii. "Mean Square Error (MSE)"

This indicates the error rate measured while decoding the original watermark image and mathematically can be represented as:

$$MSE = \frac{1}{y \times z} \sum_0^{b-1} \sum_0^{a-1} |f(i,j) - g(i,j)|^2$$

Here, f(i,j) defined the original watermark image, g(i,j) denotes the extracted watermark image, y and z represents the width and height of the watermark image.

i. Number of pixels change rate (NPCR)

It is used to measure the different pixel percentage of two images (original image and watermark decoded image). The formula can be written as:

$$NPCR = \frac{1}{y \times z} \sum P(i,j)$$

Let, p1 (I,j) signify the original watermark image, p2 (i,j) defines the decoded image, therefore,

$$p(i,j) = \begin{cases} 1 & \text{if } p1(i,j) \neq p2(i,j) \\ 0 & \text{else} \end{cases}$$

i. Unified Average Changing Intensity (UACI)

It evaluates the average intensity of dissimilarity between the two images like original watermark image and decoded image. It is represented as:

$$UACI = \frac{1}{y \times z} \sum_0^{b-1} |p1(i,j) - p2(i,j)|$$

Table 5.1 Parametric analysis against correct key

Number of Test samples	PSNR	MSE	NPCR	UACI	EI Entropy	SI Entropy
1	64.42	3.54	67.89	17.72	7.528	6.796
2	69.51	5.89	68.59	16.35	6.297	5.758
3	64.28	8.56	96.51	14.32	5.897	4.587
4	59.51	7.62	98.36	15.98	7.258	3.297
5	61.79	7.98	97.18	16.14	7.348	4.587
6	63.57	6.35	96.38	18.84	7.359	4.364
7	60.05	5.89	95.28	16.32	5.367	4.584
8	66.74	8.68	99.67	17.35	6.258	5.687
9	67.98	9.78	98.64	16.43	6.357	5.687
10	69.08	9.54	99.04	15.59	6.984	5.575

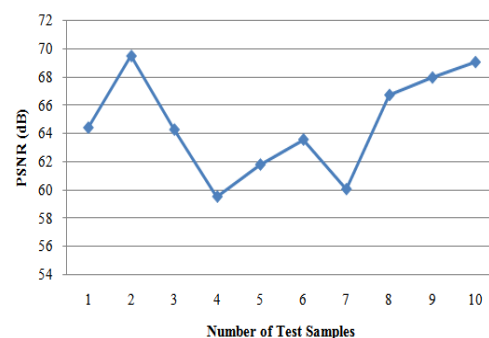


Figure 5.13 PSNR

The PSNR measured with respect to the number of test samples uploaded during the testing process of

the proposed digital watermarking system is depicted in Figure 5.13. the graph has shown that PSNR is changes irregularly that is for some test samples the PSNR is high whereas at some it is low. For 2nd, 9th and 10th test sample, the PSNR is maximum, this is due the effect that the noise level present in the test image is small and hence the PSNR is high. The average PSNR value detected for the proposed work is about 64.69 dB.



Figure 5.14 MSE

The MSE value measured after the complete extraction process of watermark image for 10 different test samples is shown in Figure 5.14. The above figure represents that for 9th test sample highest MSE has been observed this is because of unsuccessful decoding process of the original watermark image. Less MSE means better decoding of watermark image. The average of MSE observed for watermarking image is about 7.383.

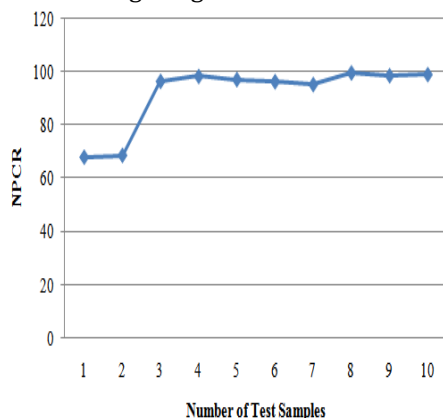


Figure 5.15 NPCR

The NPCR rate observed for the proposed work is shown in Figure 5.15. It is mainly utilized to determine the difference between the pixels of two images named as original test image and watermark as a cover image. The average value of NPCR computed for the 10 different test images is 91.75.

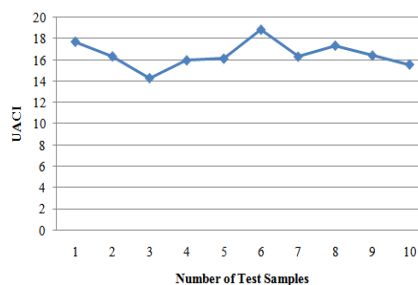


Figure 5.16 UACI

This parameter has been evaluated to know the average intensity of dissimilarity between the two watermark images such as original watermark image and decoded image. Less is the difference better is the quality of the image. The average value of UACI detected for the proposed model is about 16.504.

Comparison of Entropy

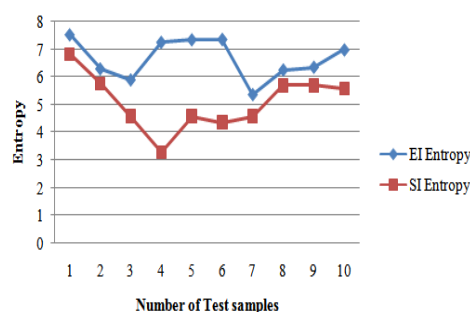


Figure 5.17 Entropy

Another parameter that has been computed to measure the efficiency of the proposed work is entropy that is EI Entropy and SI entropy. The extracted image (EI) and secret watermark image (SI) entropy are shown by the blue and the red color line.

To show the effectiveness of the proposed work compared to existing work, the comparative analysis has been performed and shown in Figure 5.18. The work has been compared with the existing work performed by **Sangeetha et al. (47, 2018)** in the field of watermarking system by utilizing the concept of texture of watermark image with the host entropy. Also, the DWT scheme has been applied to determine the DWT coefficient of the test image. The results indicated that average PSNR of about 28.62 dB was obtained. The comparison of the existing PSNR (28.62 dB) with the proposed PSNR of about 64.69 dB has been obtained. Thus, in proposed work the watermark image has been extracted with better PSNR with an enhanced rate of about 55.76 %.

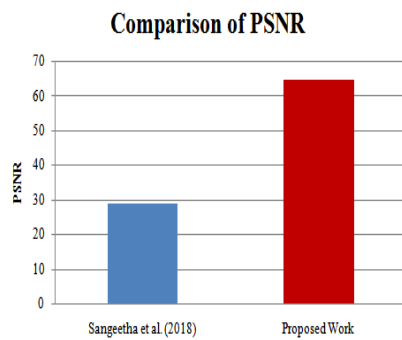


Figure 5.18 Comparison of PSNR

VI. Conclusion And Future Scope

The versatile nature of watermarking has led to a strong research community. The algorithms developed for secretly conveying digital signals are significant, especially given the young age of the field in which they were developed (text, image and video). They can be described using a wide variety of models. In the best-case scenario of this research, the digital image was watermarked utilizing discrete wavelet transform, SVD, and artificial intelligence. At first, the required pixel attributes were extracted using a DWT plus SVD approach. An ANN method was used to embed the watermark image, and the acquired post-SVD image's pixels were optimized with the proper fitness function. To further tighten the system's security, an embedding key has been entered on both the transmitting and receiving ends. The proposed layout has been proven to be more effective than competing approaches, notably in terms of embedding capacity and robustness. This method might therefore be used to secure many media types. Analyses of PSNR, pixel-to-pixel variation rate, unified average variable intensity, EI, and SI entropy, among others, have been performed on various samples of test data. The PSNR of the watermark image was determined to be approximately 64.69 dB, which is an improvement over previous efforts. The outcome was a 55.76 percent increase over the state of the art.

VII. References

1. Mane, G. V., & Chiddarwar, G. G. (2013). Review paper on video watermarking techniques. *International Journal of Scientific and Research Publications*, 3(4), 1-5.
2. Durvey, M., & Satyarthi, D. (2014). A review paper on digital watermarking. *International Journal of Emerging Trends & Technology in Computer Science*, 3(4), 99-105.

3. Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005*. (pp. 709-716). IEEE.
4. Nikolaidis, N., & Pitas, I. (1999, June). Digital image watermarking: an overview. In *Proceedings IEEE International Conference on Multimedia Computing and Systems* (Vol. 1, pp. 1-6). IEEE.
5. Patel, R., & Bhatt, P. (2015). A review paper on digital watermarking and its techniques. *International Journal of Computer Applications*, 110(1), 10-13.
6. Jiao, S., Zhou, C., Shi, Y., Zou, W., & Li, X. (2019). Review on optical image hiding and watermarking techniques. *Optics & Laser Technology*, 109, 370-380.
7. Liu, J., & He, X. (2005, August). A review study on digital watermarking. In *2005 International Conference on Information and Communication Technologies* (pp. 337-341). IEEE
8. Chawla, G., Saini, R., & Yadav, R. (2012). Classification of watermarking based upon various parameters. *International Journal of Computer Applications & Information Technology*, 1(II).
9. Sangeetha, N., & Anita, X. (2018). Entropy based texture watermarking using discrete wavelet transform. *Optik*, 160, 380-388.
10. Jabade, V. S., & Gengaje, S. R. (2011). Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications*, 31(1), 28-35.
11. Chang, C. C., Tsai, P., & Lin, C. C. (2005). SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577-1586.
12. Surekha, P., & Sumathi, S. (2011). Implementation of genetic algorithm for a dwt based image watermarking scheme. *IJSC*, 2(1), 244-252.
13. Lai, C. C. (2011). A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing*, 21(4), 522-527.
14. Ziabari, S. S. M., Atani, R. E., Keyghobad, K., & Riazi, A. (2013). The optimized image watermarking using genetic algorithm. *Current trends in technology and science*, 2(6), 359-363.
15. Malonia, M., & Agarwal, S. K. (2016, March). Digital image watermarking using discrete wavelet transform and arithmetic progression technique. In *2016 IEEE Students' Conference on Electrical*,

Electronics and Computer Science (SCEECS) (pp. 1-6). IEEE.

16.Sadeghzadeh, M., & Taherbaghal, M. (2014). A new method for watermarking using genetic algorithms. In *International Conference on Machine Learning, Electrical and Mechanical Engineering (ICMLEM'2014), January* (pp. 8-9).

17.Hussein, E., & Belal, M. A. (2012). Digital watermarking techniques, applications and attacks applied to digital media: a survey. *International Journal of Engineering Research & Technology*, 1(7), 1-8.

18.Gupta, N. (2013). Artificial neural network. *Network and Complex Systems*, 3(1), 24-28.

19.Mamatha, P., & Venkatram, N. (2016). Watermarking using Lifting Wavelet Transform (LWT) and Artificial Neural Networks (ANN). *Indian Journal of Science and Technology*, 9(17), 1-7.

20.Karimi, M., Mohrekesh, M., Azizi, S., & Samavi, S. (2013, September). Transparent watermarking based on psychovisual properties using neural networks. In *2013 8th Iranian Conference on Machine Vision and Image Processing (MVIP)* (pp. 33-37). IEEE.

21.Movaghar, R. K., & Bizaki, H. K. (2017). A new approach for digital image watermarking to predict optimal blocks using artificial neural networks. *Turkish Journal of Electrical Engineering & Computer Sciences*, 25(1), 644-654.

22.Sarangi, P. P., Sahu, A., & Panda, M. (2013). A hybrid differential evolution and back-propagation algorithm for feedforward neural network training. *International Journal of Computer Applications*, 84(14).

23.Zhang, L., & Suganthan, P. N. (2016). A survey of randomized algorithms for training neural networks. *Information Sciences*, 364, 146-155.

24.Thakkar, F. N., & Srivastava, V. K. (2017). A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, 76(3), 3669-3697.

25.Ansari, I. A., & Pant, M. (2017). Multipurpose image watermarking in the domain of DWT based on SVD and ABC. *Pattern Recognition Letters*, 94, 228-236.

26.Qin, C., Ji, P., Zhang, X., Dong, J., & Wang, J. (2017). Fragile image watermarking with pixel-wise

recovery based on overlapping embedding strategy. *Signal Processing*, 138, 280-293.

27.Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., & Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, 6, 10269-10278.

28.Al-Haj, A., Farfoura, M. E., & Mohammad, A. (2017). Transform-based watermarking of 3D depth-image-based-rendering images. *Measurement*, 95, 405-417.

29.Zear, A., Singh, A. K., & Kumar, P. (2018). A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia tools and applications*, 77(4), 4863-4882.

30.Singh, A. K. (2017). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications*, 76(6), 8881-8900.