International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

# Improved DCT based Digital Image Watermarking Technique using Particle Swarm Optimization Algorithm

**Nkwachukwu Chukwuchekwa[1], Bukola Akinwola[2], James Onojo[3]**

[1,2,3]*Electrical and Electronic Engineering Department, Federal University of Technology, Owerri, Nigeria*

---

**Abstract -** *The copyright laws are not sufficient to protect the multimedia data against illegal recording and transmission. Discrete Cosine Transform (DCT) image watermarking technique is used for copyright protection of digital images because of its robustness against some attacks and geometrical transformations and also its compatibility with Joint Photograph Expert Group (JPEG) standard. In this study, DCT based digital image watermarking technique was improved using Particle Swarm Optimization (PSO) algorithm. The study involves watermarking of a still image for copyright protection. The watermark information used is a pseudo-random pattern. The original still image of size 300 x 500 imported into the MATLAB directory was converted into an 8-bit RGB image of size 300 x 500. The PSO algorithm was applied on the image to find the suitable scaling factor and the coefficient for embedding the watermark. The DCT coefficient of the original image and watermark image was modified using an additive embedding formula. The extracted image was achieved by inverting the DCT of the original image. The performances of the original DCT algorithm and the PSO counterpart against some attacks which include rotation, Gaussian noise and salt and pepper noise were evaluated using error metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Results obtained show that the MSE using the PSO algorithm reduced by 42%, 36% and 65% for the rotation, Gaussian noise and salt and pepper noise respectively while the PSNR increased by 2% for each of the attacks. This shows the robustness of the POS algorithm hence better noise immunity and imperceptibility against common attacks over the conventional DCT algorithm. It is believed that the PSO algorithm will also improve the performance of other digital image watermarking techniques.*

***Key Words***: **Digital Watermarking, Discrete Cosine Transform (DCT), Particle Swarm Optimization (PSO), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).**

## 1. INTRODUCTION

The field of Information Technology has witnessed an exponential growth over the past few decades, most specifically the internet. Digital information in the form of texts, audio, images and video can be easily copied, processed and distributed among unauthorized users within seconds over the internet without the consent of the author. In addition, unlimited copies of the same original document can be perfectly reproduced bit by bit, thus allowing for pirating. It has been recognized that due to the nature of digital information, conventional copyright law is inadequate for protecting digital data, as it often causes permanent damage to the content of the host media which is generally unacceptable in some applications. The issues of piracy and copy right violation are increasing due to the advancement in growth of computer networking and technology. Therefore, it has become necessary to take into consideration the exchange of secured and protected data over the network and between individuals. Attentions of researchers and practitioners from different fields have been drawn and different methods have been presented toward developing secure protection mechanisms. One of them is watermarking, which is typically a technique for overcoming the shortcomings of conventional copy right law for protecting digital information.

Digital watermarking technology is an effective method for copy right protection of digital images [1], image /content authentication [2], broadcast monitoring and medical application [3]. It is an act of irreversibly embedding digital data or pattern (water mark) into another digital multimedia (audio, video and images) to protect owner's right [4]. In order to prove ownership or copy right data, the water mark is extracted and tested by the owner.

In embedding module, watermark algorithm combines the watermark information into the host data and produces a watermarked image. Then, the watermarked digital image is transmitted or stored. If an unauthorised user decides to make a modification, then it is called an attack. At times, the modification may not be malicious. An algorithm is applied to decode the watermark information by the owner. It will be very difficult for counterfeiter to remove or modify water mark.

The process of digital watermarking begins with the insertion of secret information such as a text or logo in an imperceptible manner into the host signal such as digital image or digital sound, digital video or 3D virtual object by an encoder to produce watermarked image. The secret information is called watermark, while the host signal can be termed original, cover image or host image. A scaling factor is used to modify the DCT coefficient of the original image and the embedding watermark in order to adjust the required amplitude of the pixel value. It is carefully assigned to preserve the quality of the watermarked image and to improve the robustness of the embedded watermark against attacks. The decoder processes and extracts the information

from the watermarked image. The decoder may not be needed if the watermark is visible. The watermarking system is referred to as a restricted key system if the input or the watermarked systems are used. The decoder correlates the extracted watermark with the original image and compares the result with a predefined threshold. The existence of the watermark is detected if the correlation matches the threshold [5].

There are different watermarking algorithms for embedding and extracting watermark. The embedding algorithms are designed based on spatial or frequency domain to insert the watermark along with a chosen key within the original image. Once the insertion is achieved, the embedded watermark can be identified based on human perception as visible or invisible watermark. The inverse operation of an embedding algorithm is performed by the extraction algorithm. It decodes the watermarking information and authenticates the embedded data against any illegal alteration applied on original digital image. Some extraction algorithms may require the use of higher watermarking technology for detection and extraction of watermark from the embedded watermark without the needs for original digital images. These algorithms are referred to as blind digital watermarking algorithm. Some of these algorithms use auxiliary means such as secret keys, position table or instinct features of digital image for positioning the watermark in such a way that they can be precisely and easily be extracted. Although, using special algorithms to create positions may be a good choice but once the algorithms are realized by unauthorised users, the watermarking may be considered unsecure. The watermarking algorithm can be grouped into spatial domain and transform domain watermarking algorithms. In spatial-domain watermarking algorithm, the watermark is directly embedded into a pre-defined set of image pixels. An example of a spatial-domain algorithm is the Least Significant Bit (LSB). The techniques have low bit capacity, require more perceptual quality, less computational cost but, are less robust against attack, as any simple noise may damage the watermark data embedded in the watermarked image. In transform-domain image watermarking, the original image is first transformed into frequency domain coefficients and then, embedded with the watermark. The algorithms have large bit capacity, more robust to attacks like sharpening, noising, filtering and compression. It is suitable for copy right application while spatial-domain type is used for user authentication. The commonly used transform –domain scheme are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

The DCT is an essential tool in signal processing for transforming signal from spatial domain to frequency domain. It has a very good energy concentration. DCT divides the carrier signal of the host image into three frequency band coefficients namely Low Frequency (LF), Middle Frequency (MF) and High frequency (HF) band coefficients and embeds watermark into any one of these band coefficients. The DCT watermarking technique can be used for data compression, pattern recognition and image processing. The following equation defined a Two Dimensional (2D) DCT formula [6].

$$G(u,v)=\sigma(u)\sigma(v)\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}g(i,j)\cos\left[\frac{(2i+1)u\pi}{2m}\right]\cos\left[\frac{(2j+1)v\pi}{2n}\right] \quad (1)$$

The inverse of DCT transform is given by,

$$G(m,n)=\sigma(u)\sigma(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}G(u,v)\cos\left[\frac{(2i+1)u\pi}{2m}\right]\cos\left[\frac{(2j+1)v\pi}{2n}\right] \quad (2)$$

$$\text{where } \sigma(u)=\begin{cases}1/\sqrt{2} & \text{for } u=0\\ 1 & \text{for } u=1,2,3,\ldots,m-1\end{cases} \quad (3)$$

$$\sigma(v)=\begin{cases}1/\sqrt{2} & \text{for } v=0\\ 1 & \text{for } v=1,2,3,\ldots,n-2\end{cases} \quad (4)$$

m and n are the size of row and column for the input image g(i,j), g(i, j) is the intensity of the image pixel, the output image G(i,j) is the DCT coefficient of the DCT matrix. DCT transform have both Alternate Current (AC) and Direct Current (DC) coefficient. The middle-band frequency coefficient (FM) and the higher frequency coefficient (FH) are selected generally for embedding of watermark bit [2]. In this research paper, the watermark was embedded in the middle frequency band coefficient of the original image. The DCT based digital image watermarking technique was improved using Particle Swarm Optimization (PSO) Algorithm. The PSO algorithm was used for determining the best position for embedding watermark on the host image and for adjusting the strength of the watermark. The DCT coefficient of the original image and watermark image was modified using an additive embedding formula. The extracted image was achieved by inverting the DCT of the original image. The performance of the proposed scheme against attacks was compared with the performance of conventional DCT scheme.

## 2. Literature Review

The authors in [7] presented the analysis of different types of attacks on the digital image watermarks in order to classify them into different categories. Six distinct removal watermark attacks were analysed based on the theoretical background of each attack and the impact of the attack on the watermarking signal. The attacks considered include Pepper noise, additive Gaussian, Gaussian smoothing, Histogram Equalization, and sharpening attacks. Two different watermarking techniques were presented in order to determine the effect of the attacks on the watermark image.

A novel algorithm based on a two –dimensional Discrete Wavelet Transform (2D-DWT) for watermarking positioning was proposed in [8]. The algorithm used local spatial features of DWT to limit the positions for watermarking embedding and formed wavelet coefficient tree to index the positions to medium frequency space for watermarking. Determination of the embedding positions involved multi-resolution decomposition and the algorithm for determining the root node of the wavelet tree. The proposed watermarking embedding system composed of wavelet transform, secret key creation, watermarking positioning, watermarking embedding and inverse wavelet transform. The positions for embedding watermarking were provided by the watermarking positioning functions which were provided by the secret key creation functions. A new watermarking series was created by using a repeated coding method that repeated severally every bit in the random watermarking series to improve the property against any kind of interferences. In order to improve the security of the embedded watermark information, two secret keys were used in the algorithm to control the direction of the wavelet tree and the nodes in the wavelet tree. Watermarking detection and correlation was carried out to determine the existence of watermarking. From the experiment, the watermarking image was almost the same as the original image and therefore, the balance between transparency and robustness was realized.

The authors in [9] proposed a multi watermarking scheme based on DWT domain. In this approach, three independent binary watermarks were embedded in the original image. A multi-watermarking were embedded simultaneously to improve the quality of watermarked image and the robustness of the extracted watermarks by first recombining a three 2D watermarks into 3D watermarking sequence. The original image was decomposed by using DWT into L-level approximation sub band and then split the approximation sub band into multiple over lapping blocks and the block with the largest block texture information were selected according to the size of binary watermark. The multi watermarks are simultaneously embedded by modifying the value of the fractional part of the pixel value from the selected blocks based on discrete algorithm. A multi watermarking extraction scheme was also developed from the distorted image. PSNR and MSE were used to evaluate the quality of the watermarked image. Several image processing attacks such as noise attack, median filtering, JPEG compression and geometric rotation were used to evaluate the robustness of the proposed watermarking scheme. The simulation result showed that one of multi-watermarks was robust against noise addition, filtering and JPEG compression while the other two watermarks were immune to any attacks.

A new watermarking algorithm based on the texture block and edge detection in the discrete wavelet domain was introduced in [10]. In the algorithm, the texture blocks were extracted after the edge detection for the original image with the canny operator by setting a threshold. By using the masking property of human visual system, the digital watermark was adaptively embedded into the high frequency and low frequency sub bands in the discrete wavelet domain of the texture block. The performance of the algorithm was tested using a Lena image as the original image and the binary text image as the original watermark. The effect of the embedding watermark was depicted and watermarked image was so similar with the original image. The ability of the algorithm to resist JPEG compression, noise, clipping, rotation and median filter were tested. The results had a good performance against the clipping attack. The robustness of the algorithm was the best under the JPEG compression attack. The algorithm showed better performance under the condition of adding salt and pepper noise than Gaussian noise of the same coefficient. A worst performance was experienced under the condition of median filter which should be improved for further study. The simulated results showed that the proposed algorithm has the ability of resisting geometric attacks and have good balance between the invisibility and robustness of the digital image watermark.

Researchers in [11] proposed a hybrid watermarking algorithm based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). In this process, watermarking was done by changing the wavelets coefficients of the host image after required DWT decomposition into four non-over lapping coefficient sets: LL (High scale low frequency), HL(Horizontal low-scale, high frequency component), LH (vertical low scale, high-frequency components), HH (Diagonal low-scale, high-frequency components). The host image was decomposed four times. Then a new embedding algorithm (NEA) was embedded in the HL and LH sub band of the host image data. DCT was performed on the two coefficient sets of HL14 and HL24 using 4 x 4 blocks. The watermarked of 32 x 32 was converted to DCT domain. The embedding of the watermark was performed by modifying the coefficient values in the DCT domain. The results of the NEA with and without attack were compared with Cox's additive embedding algorithm. The algorithms were tested with 512 x 512 host image and 32 x 32 watermark image and evaluated using imperceptibility and robustness of the mark image. The PSNR and MSE were used as the metric for testing the imperceptibility while the robustness of the algorithm was evaluated using Additive White Gaussian Noise attack (AWGN). The NEA algorithm gave a PSNR and MSE of 36.52dB and 14.49 respectively while Cox's additive algorithm gave PNSR and MSE of 27.19dB and 124.10, with AWGN, the NEA had PNSR of 30.21 dB and MSE of 61.90 and the Cox's additive algorithm had PNSR of 27.17 and MSE of 124.27. The correlation between the recovered water mark image of the NEA and the original image gave 0.80, 0.94 and 0.95 according to DWT level 4, 3, 2 respectively. This indicated an acceptable image when attack is done compared to the image quality of the Cox's additive algorithm. The NEA algorithm is a promising technique against attack compared to other embedding algorithm like Gaussian sequence algorithm, image fusion algorithm, and non-linear quantization, but applying only AWGN attack is not enough to determine the robustness of the algorithm.

An efficient DCT based image watermarking scheme that depended on the concept of spreading the watermark bits sequence for protecting distribution rights of digital images was proposed in [12]. The watermark bits are pseudo random numbers generated by Linear Feedback Shift Register (LFSR) and embedded in the DCT coefficient of the

host image. The DC components of every block was selected and modified. After modification the **inverse** DCT (IDCT) was **calculated to obtain the watermarked image.** The PSNR and MSE were calculated between the host image and the watermarked image to determine the distortion introduced into the host image. In the experiment, DCT was performed on 4 x 4, 8 x 8 and 16 x 16 embedding size of the watermarked image. The payload capacity, the robustness and quality of watermarked image were used to determine the performance of the proposed algorithm. The robustness of the proposed algorithm was tested with Tamper Assessment Function (TAF) and Normalized Correlation (NC). A comparative analysis of NC, TAF and PSNR for 4 x 4, 8 x 8 and 16 x 16 DCT based proposed watermarking algorithm was carried under different form of attacks such as JPEG compression, Median Filtering, Gaussian noise, salt and pepper noise, blurring, rotation and resizing. The performance was evaluated using dual attacks such as salt and pepper noise plus Median filtering, salt and pepper noise plus JPEG compression and Image resizing plus JPEG compression. The 8 x 8 performed better than the other methods while the 4 x 4 DCT based method had limited performance in term of PSNR, NC and the TAF values. The improvement in the performance of the proposed algorithm and the existing algorithm was determined in terms of TAF and NC. The proposed algorithm outperformed the existing algorithm against JPEG compression, Median Filtering, Gaussian noise attack, and dual attack of salt and pepper noise plus Median filtering.

**The** study in [13] proposed a new algorithm by combining both digital watermarking and tampering detection method. In the proposed methodology, in order to enhance security and robustness of the image, a 2-level DWT was performed on the RBG components of the output image watermark to decompose it into four non-overlapping multi-resolution coefficient sets. This divided the image into low frequency and high frequency components. The same process was done for the watermark which was embedded into the original image using 2 level DWT coefficients. A new watermarked image was obtained by multiplying the scaling factor with the watermark and components of the input original image. In tampering process, the original image and the watermarked image were used as a reference image for detecting tampering and a 2DWT was applied on both images. The performance of the experiments was validated using PSNR. The experiment showed good result up to 55%.

The authors in [14] carried out a comparative analysis of digital watermarking using LSB technique, DCT and DWT. In LSB technique, the pixel value of the original image and the watermarked image were converted into binary. The 8th bit of every pixel of the original image was replaced by every bit of watermark image. In the DWT technique, the DWT decomposed the original digital image into four different sub band level which are lower resolution (LL), horizontal (LH), vertical (HL) and diagonal (HH). The extraction process was carried out by subtracting the original DWT coefficients form the watermarked marked image ones. Watermarking using DCT function converted original image data into the summation of a series of cosine wave oscillating at different frequencies. The performance of the three techniques was compared on the basis of PSNR and Normalised Correlation (NC) using Gaussian noise, Poisson noise, salt and pepper noise and Speckle noise. The paper concluded that the DCT transform was best technique for digital watermarking among the above said techniques. The parameters of the techniques were also evaluated and compared using Gaussian noise, Poisson noise, salt and pepper noise and Speckle noise. The DCT gave PSNR 66.2582 and 42.2690 for Gaussian noise and salt and pepper noise respectively.

The authors in [15] presented an improved digital image watermarking scheme using the Discrete Fourier Transform (DFT) and Singular Value Decomposition (SVD). The proposed DFT-SVD based watermarking algorithm incorporated the watermark image in the DFT and SVD domains into the embedding and extracting watermark processes. In the embedding process, the forward Onion Peel Decomposition (OPD) algorithm decomposed origin shifted Fourier transformed carrier image into four different frequency sub bands so that multiple copies of watermark can be attached by the watermarking algorithm. The algorithm was applied to the origin shifted Fourier transformed image and decomposed the two –directional image into one-directional array which commenced from the higher frequency and ended at the lower frequency components of the transformed image. In the extraction process, the embedded watermark was extracted by performing the reverse process of watermarking using extraction algorithm. In order to determine the effectiveness of the proposed algorithm, its performance was compared with a set of existing algorithms proposed by [16], [17] and [18]. Twenty sets of different images with varying characteristics were used for the experimental analysis. The PSNR and Mean Absolute Error (MAE) metrics were used to analyse the objective quality of the watermarked images while the subjective visual quality of the watermarked images was analysed by Structural Similarity Index Measure (SSIM). The values of PSNR, MAE and mean SSIM produced by the proposed algorithm outperformed other algorithms. The robustness of the proposed algorithm was tested against various potential attacks such as Gaussian noise, Gaussian filtering, histogram equalization, JPEG compression, rescaling, image un-sharpening, gamma correction, salt and pepper impulse noise, pixelate, rotation and crop operations. Pearson's Correlation Coefficient (PCC) was used as objective metric numerically analyzing the robustness of the extracted watermark. Uniformity was ensured among all the algorithms used by setting PSNR watermarked image to around 31dB. The proposed algorithm outperformed other competing algorithms due to the collective benefits of the DFT, SVD and OPD algorithms. The advantages of DFT in resisting geometrical attack enhanced the performance of the proposed algorithm against rescaling, rotation and cropping. The proposed algorithm worked equally well as the algorithm proposed by [17] against potential attacks such as Gaussian noise, Gaussian filtering, salt and pepper and pixelate. In comparison with the Ganic and Eskicioglu algorithm, the proposed algorithm performed reasonably well against histogram equalization, image unsharpening and gamma correction based potential attacks. The extracted

watermarked image extracted images produced by the proposed algorithm outperformed the extracted images produced by [17] and [18]. The experimental analysis conducted on different images showed that the proposed algorithm produced high quality watermarked images.

It was found from the reviewed literatures that some algorithm proposed by researchers use auxiliary means such as secret keys, position table or instinct features of digital images for positioning the watermark. However, precise positioning of the watermarking into the host image is perceptually significant and critically challenging as alteration in the pixels or coefficient blocks can cause distortion to the original image and makes the watermark unsecure and prone to attack by malicious users. This paper provides a secured and optimized approach based on Particle Swarm Optimization (PSO) algorithm in the frequency domain of DCT for finding a suitable scale factor and best position for embedding watermark in the original image block.

### 2.1 Metrics for Evaluating Image Quality

Some watermarking metric is required to determine the quality of watermarking techniques. An ideal watermarking algorithm produces low values of Mean Square Error (MSE) and Mean Absolute Error (MAE) with high value of Peak Square Noise Ratio (PSNR). These metrics compare the watermarked image with the original image. The commonly used metrics for evaluating image quality include:

Mean Absolute Error (MAE)

$$MAE=\frac{\sum_{m,n}[I_{o(m,n)}-I_{w(m,n)}]}{M*N} \quad (5)$$

Where M and N represent the number of rows and columns in the input image patterns respectively. The $I_{o(m,n)}$ is the intensity level of the pixel of the original image and $I_{w(m,n)}$ is the intensity level of the pixel located at m and n position in the watermarked image.

(A) Mean Square Error (MSE)

The MSE depends on the image intensity scaling. The mean square **error between watermarked image and the original image** can be expressed as,

$$MSE = \frac{\sum_{m,n}[I_{o(m,n)}-I_{w(m,n)}]^2}{M*N} \quad (6)$$

where M and N represent the number of rows and columns in the input image patterns respectively. The $I_{o(m,n)}$ is the intensity level of the pixel of the original image and $I_{w(m,n)}$ is the intensity level of the pixel located at m and n position in the watermarked image.

(B) Peak Signal Noise Ratio (PSNR)

The PSNR is used to eliminate the problem of image intensity by scaling the MSE according to the image range and expressed as,

$$PSNR= 10\, log_{10}\left(\frac{R^2}{MSE}\right) \quad (7)$$

where R represents the maximum possible pixel value of the image and its value is 255 for 8-bits grey images [5]. The value is measured in decibels (dB).

(C) Signal to Noise Ratio (SNR):

SNR determines the signal strength (S) with respect to the background noise (N). It is expressed as,

$$SNR = 10 log_{10}(S/N) \quad (8)$$

(D) Bit Error Rate (BER)

BER is the number of bits modified after applying watermarked image to the total number of bits in the original cover image. It is expressed as [19],

$$BER = \frac{C}{H*W} \quad (9)$$

where C is the number of error bits, H is the height of the watermarked image and W is the width of the watermarked image.

(E) Normalized Correlation (NC)

The similarity between the original watermark image and the extracted watermarked image from the attack image is measured using Normalized Correlation. NC is calculated as in [6],

$$NC= \frac{\sum_{x=1}^{N}\sum_{y=1}^{N} W(x,y) * W'(x,y)}{\sum_{x=1}^{N}\sum_{y=1}^{N} W^2(x,y)} \quad (10)$$

where N*N, W(x,y) and W1(x,y) are the size of watermark, the pixel values at location (x,y) of the watermark and the pixel values at location (x,y) of the extracted watermark respectively.

## 3. Methodology: Particle Swarm Optimization (PSO)

Particle Swarm Optimization is a meta-heuristic optimization algorithm inspired by social and cooperative behaviors of some species to fill their need in the search space. It is developed by James Kennedy and Russell Eberhart in 1995 [20]. Each particle flies through the search space and searches for its best positions. The algorithm is initiated with particle at random positions, and then tries to search for the minimum or maximum of objective function by exploring the search area. Each particle changes its position by knowing its velocity and the position where good solutions have been found by itself or its neighboring particles. The previous best particle for the $i^{th}$ particle is ($P_{best}$) while the global best particle found by all particle is the global best particle ($G_{best}$). For a search problem in an n –

dimensional space, the next velocity of each particle is updated by,

$$V_{ij}(t+1) = w* V_{ij}(t) + C_1*r_1(t)[P_{besti} - X_{ij}(t)] + C_2*r_1(t)[G_{besti} - X_{ij}(t)] \quad (11)$$

The position of each particle is updated by

$$X_{ij}(t+1) = X_{ij}(t) + V_{ij}(t+1) \quad (12)$$

The experience of each particle is updated by using two cognitive coefficients $C_1$ and $C_2$, $r_1$ and $r_2$ are random values ranges having from 0 and 1. The inertia weight w is of value 0.9, the initial velocity is set at 0.5, the number of particle is 50 and maximum iteration is 100.
The fitness function used in the research paper to estimate the performance of each generation is given as,

$$f(x) = corr2(I, I_m) + corr2(W,W^1)/2 \quad (13)$$

where I and $I_m$ are original and watermarked images respectively while W and $W^1$ are original and extracted watermark respectively. A visible DCT image watermarking scheme where the watermark was intentionally embedded to spread in important area on the host image in order to be perceptible to observers was used. The embedding factor, 100 was used for visible watermarking. The embedding process for the method used is given below:

1. The original image (I) of size NxN and the watermark image (W) of size M x M are read from the MATLAB folder into the workspace using 'imread function'. The original image and the watermark image should be equal in size.
2. The N x N original colour image is split into three (RGB) channels and used for embedding watermark.
3. Each of RGB components is subdivided into non-overlapping blocks of size 8 x 8. Each block of the RGB is transformed into frequency domain by applying DCT.
4. The watermark image is embedded in the middle frequencies (FM) coefficients of each RGB component in order to reduce distortion. The embedding factor, α, is intentionally chosen to maximize imperceptibility and detect the watermark.
5. Apply PSO on the 2D DCT to find the suitable scaling factor and the coefficient for embedding the watermark.
6. The DCT coefficient of the original image ($I_{ij}$) and watermark image ($W_{ij}$) is modified using an additive embedding formula [21],

$$I_{w\,i,j} = I_{i,j} + \alpha W_{i\,j}, \quad i,j = 1, \ldots\ldots,n \quad (14)$$

7. The extracted image is achieved by inverting the DCT transform of the original image. In the extraction process, the original image is required to extract the watermarking information. The extraction equation is given as [21],

$$W_{i,j} = \left(I_{w\,i,j} - I_{i,j}\right)/\alpha \quad (15)$$

The above mentioned steps are depicted in the flow chart of Fig. 1

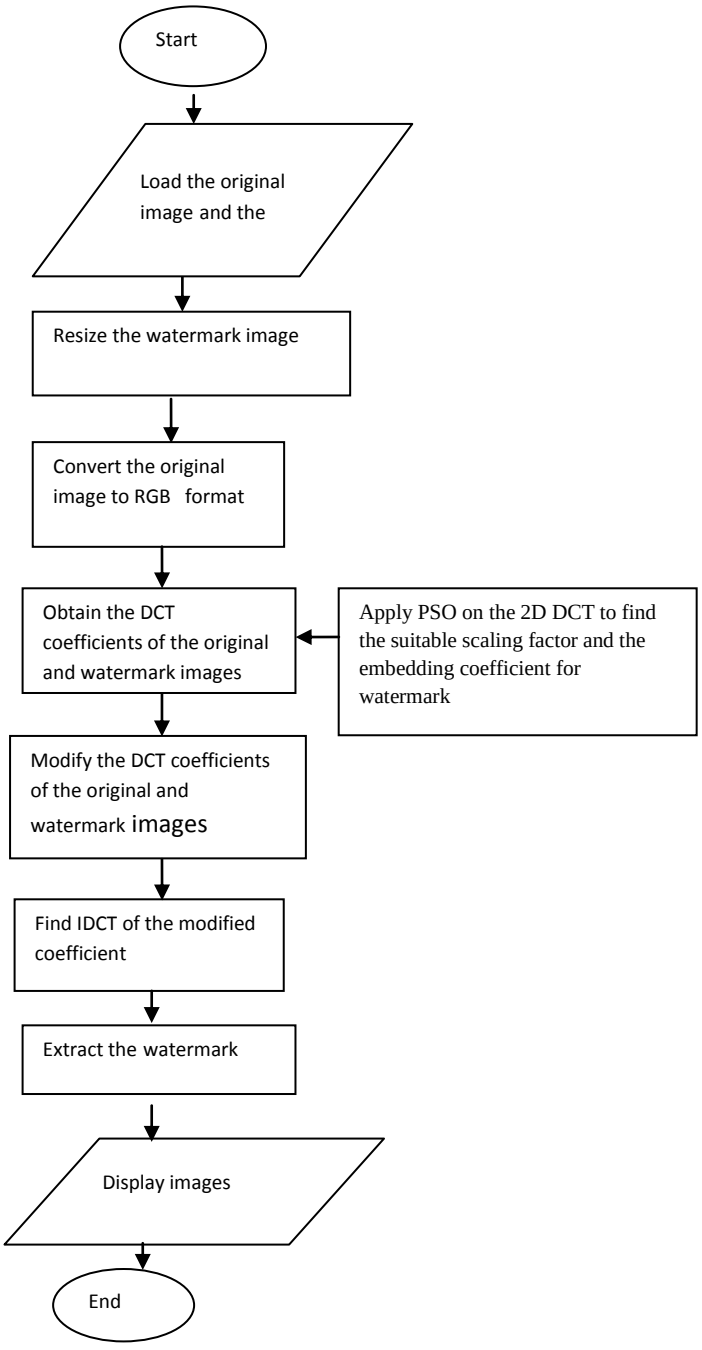


Fig (1): Methodology for coding watermarks

## 4. Simulation Results and Discussion

The study involves watermarking of a still image for copyright protection. The watermark information used is a pseudo-random pattern. The original still image of size 300 x 500 as shown in Figure 2 imported into the MATLAB directory was converted into an 8-bit RGB image of size 300 x 500. Figure 3 depicts the pseudo random pattern of the watermark. After running the Matlab code, desired results

were achieved. Figure 4 shows the output image of the watermark image process, that is the watermarked image. For the extraction of the watermarked image, the inverse discrete cosine transform technique is used (IDCT). Figure 5 was obtained from the extraction process of the watermarked image using inverse DCT. The inverse DCT reconstructs a sequence from its discrete cosine transform (DCT) coefficient. The IDCT function is the inverse of the DCT function. Figure 6 depicts the inverse DCT image extracted from the watermarked image. The Figure 7 shows the pixel intensities difference between extracted image and the original image. The three attacks applied to the watermarked **image to test the robustness of the algorithm are rotation**, Gaussian noise and salt and pepper noise. The attacked images are presented in figures 8, 9 and 10 together with the parameters used for the attacks. The perceived quality of the watermarked image was estimated using PSNR and MSE. The results are given in Table 1.

**Table 1: Comparison analysis of the three attacks**

| Attack | **MSE** | **PSNR** | **MSE (PSO)** | **PSNR( PSO)** |
|---|---|---|---|---|
| Rotation ($45^0$) | 0.556 | 43.48dB | 0.323 | 44.340dB |
| Gaussian noise (0.025) | 0.039 | 65.02dB | 0.025 | 66.302dB |
| Salt and pepper (0.02) | 2.52 | 44.147dB | 0.875 | 45.221 |

The results show that the MSE using the PSO algorithm reduced by 42%, 36% and 65% for the rotation, Gaussian noise and salt and pepper noise respectively while the PSNR increased by 2% for each of the attacks. This shows the robustness of the POS algorithm especially in the reduction of the MSE hence better noise immunity and imperceptibility against common attacks over the original DCT algorithm.

Fig (2): Original image

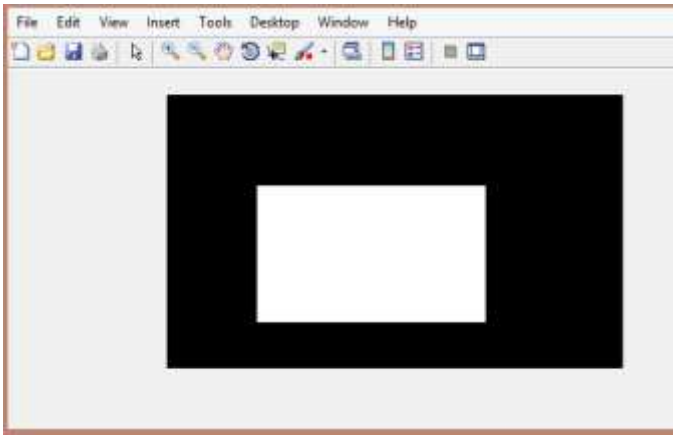

Fig (3): watermark image

Fig (4): watermarked image

Fig (5) : Extracted watermark image

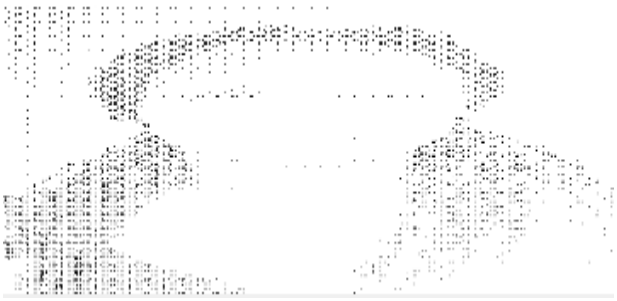

Fig (6) Inverse DCT

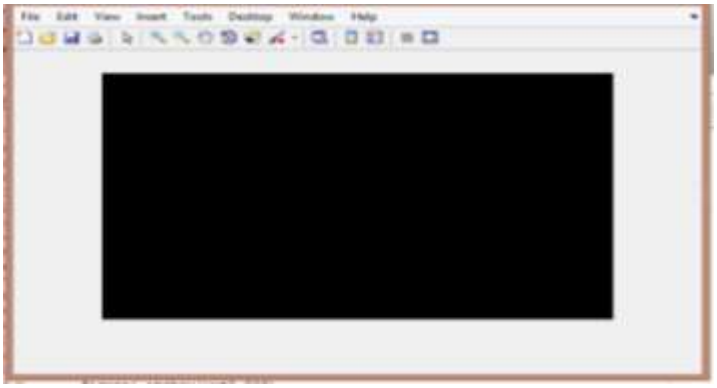

Fig (7): Difference ima

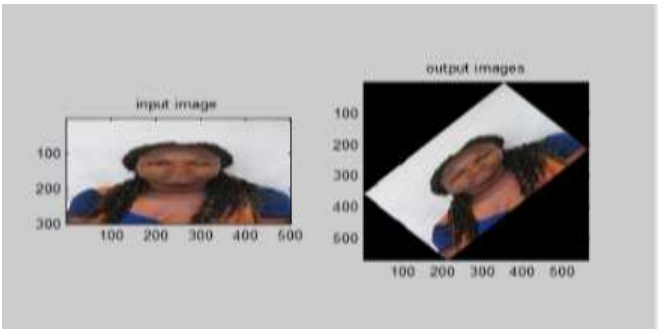


Fig (8): Rotate image ($45^0$)

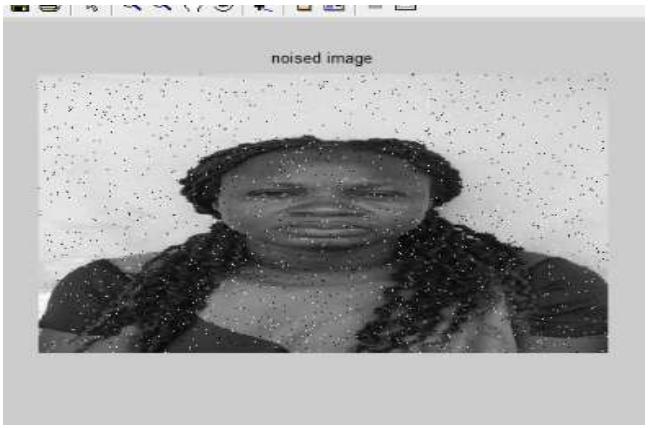


Fig (9): salt and pepper noise (0.02)


Fig (10): Gaussian noise (0.025)

## 5. Conclusion

Digital watermarking technology is an emerging field that ensures security and provides data authentication and copyright protection to digital media. The PSO algorithm was used for determining the best position for embedding watermark on the host image and for adjusting the strength of the watermark. The performance of the proposed scheme against attacks was compared with the performance of conventional DCT scheme. The experimental results show that proposed PSO-DCT image watermarking was effective in improving the imperceptibility of the watermark against some attacks. The watermarking algorithm was implemented on MATLAB software. The proposed watermarking gives less MSE with high PSNR when compared to the original DCT watermarking techniques. It is believed that the PSO algorithm will also improve the performance of other digital image watermarking techniques.

## REFERENCES

[1]. Chirag Sharma and Deepak Prashar, "DWT Based Robust Technique of Watermarking Applied on Digital Images", International Journal of Soft Computing and Applied Engineering (IJSCE), Vol. 2, No 2, pp 2319-6378, 2012.

[2]. Yanxia Z and Zenghui Z, "Multipurpose Blind Watermarking Algorithm for Color Image based on DWT and DCT", Proceedings of the 8th IEEE International and Conference on Wireless Communications, Networking and Mobile Computing (WICOM), Shangai, China pp 1-4, 2012.

[3]. Dong Chunhua, Jingbing Li, Yen-wei Chen and Yong Bai,"Zero Watermarking for Medical Images based on DFT and LFSR", Proceedings of IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, pp 22-26, 2012.

[4]. Namita T. and Sharmila, "Digital Watermarking Applications, Parameter Measurements and Techniques", International Journal of Computer Science and Network Security, Vol.17, No 3, pp 184- 194, 2017.

[5]. Puneet K S and Rajni, "Analysis of Image Watermarking using Least Significant Bit Algorithm", International Journal of Information Sciences and Techniques (IJIST), Vol.2, No.4, pp 95-101, 2012.

[6]. Bhaskar T and Vasumathi,"DCT Based Watermark Embedding into mid frequency of DCT coefficients using Luminance Component", International Research Journal of Engineering and Technology (IRJET), Vol 2, No 3, pp 738-741, 2015.

[7]. Chunlin S, Sud S, Majeb M and David L., "Analysis of digital image watermarks attacks", IEEE Consumer

Communications and Network Conference (CCNC) pp 941-945 , Las Vegas, NV, USA, 2010.

[8]. Zhang Yongping, ''Digital Watermarking Technique for Images based on DWT'', Proceedings of 7th IEEE International Conference on Digital Object, Wuhan, China, pp. 1-4, 2011.

[9]. Yaxun Z and Wei J, ''A Robust Digital Image Multi-Watermarking Scheme in the DWT Domain'', International Conference on Systems an Informatics (ICSAI), Yantai, China, pp 1851-1854, 2012.

[10]. Yingli W, Xue B and Shuang Y '' Digital Image Watermarking based on Textsure Block and Edge Detection in the Discrete Wavelet Domain'', IEEE International Conference on Sensor Network, Security Technology and Privacy Communication System (SNS & PCS), Nangang, China, pp 170-174, 2013.

[11]. Afroja Akter, Nur-E-Tajnina, and Muhammad Ahsan Ullah (2014). ''Digital Image Watermarking Based on DWT-DCT: Evaluate for a New Embedding Algorithm'', 3rd IEEE International Conference on Informatics, Electronics and Vision, Dhaka Bangladesh, pp 1-6, 2014.

[12]. Gupta G, Amit M. J. and Kanika S ''An Efficient DCT Based Image Watermarking Scheme for Protecting Distribution Rights'', Proceedings of 8th IEEE International Conference in Contemporary Computing, Noida, India, pp 70-75, 2015.

[13]. Madhuri R and Tomar D.S., ''A Secure Watermarking and Tampering Detection Technique on RGB Image using 2 Level DWT'', 5th IEEE International Conference on Communication Systems and Network Technologies, Gwalior, India, pp 638-642, 2015.

[14]. Neha B, AtulB, Vinay K D and Pooja P..''Comparative Analysis of LSB, DCT, and DWT for Digital Watermarking'', Second IEEE International Conference on Computing for Sustainable Global Development (INDIACom),New Dehli, India. pp 40 -45, 2015.

[15]. Justin V, Omer B H, Krishnan N, Mohammed R. S.,''An Improved Digital Image Watermarking Scheme using the Discrete Fourier Transform and Singular Value Decomposition'', Turkish Journal of Electrical Engineering and Computer Sciences, Vol.24, pp 3432-3447, 2016

[16]. Run R S. Horng S J, Lai J L, Kao T W and Chen R J. ''An improved SVD based Watermarking technique for copyright protection '', Vol.39, pp 673-689, 2012.

[17]. Sverdlov A, Dexter S, Eskicioglu A,''Secure DCT-SVD Domain Image Watermarking: Embedding Data in all Frequencies'', Image Processing Seminar, pp 23-26, 2006.

[18]. Gani E and Eskicioglu A, ''Robust Embedding of Visual Watermarks using Discrete Wavelet Transform and Singular Value Decomposition'', Journal of Electron Imaging, Vol.14, pp, 1-13, 2005.

[19]. Amrinder S., ''Image Watermarking: A Review of Literature'', International Journal of Engineering Trends and Technology, Vol. 40, No. 1, pp 15-22, 2016.

[20] Kennedy J, Eberhart C. R, "Particle Swarm Optimization'', Proceeding of IEEE International Conference on Neural Networks, Piscataway, NJ Vol. 4, pp 1942-1948, 1995.

[21]. Hanjalic A, Langlaar G. C, Van Roosmalen PMB, Biemond J and Langendijk R. L. ''Image and video databases: restoration, watermarking and retrieval'', IEEE Circuits and Devices Magazine, Vol.17, No. 4, pp 37-38, 2001.