

Watermarking of Frequency and Steganography for Protection of Medical Images Based on Bacterial Foraging Optimization and Genetic Algorithm

Abdul Joseph Fofanah

Mathematics and Computer Science, Milton Margai
Technical University, Freetown, Western Area, Sierra Leone

Ibrahim Kalokoh

Computer Science, University of Makeni,
Makeni, Sierra Leone

ABSTRACT

The art of watermarking and steganography are techniques to hide a secret message in an image or other media. They can be used to protect the privacy and security of medical images and patient data in the healthcare industry. We propose two algorithms for watermarking and steganography based on discrete wavelet transform (DWT), discrete cosine transform (DCT), parallel bacterial foraging optimization (PBFO), and genetic algorithm (GA). These algorithms can embed a secret message in a grayscale medical image of size 512x512 pixels, with high imperceptibility and capacity. Imperceptibility means that the stego image does not have noticeable distortions from the cover image. Capacity means that the stego image can carry as much information as possible without compromising imperceptibility. Algorithm I uses DWT to decompose the cover image into four sub-bands, and DCT to transform each sub-band into a matrix of coefficients. It uses PBFO to select the best coefficients for embedding the message, and GA to embed the message using a binary encoding scheme. Algorithm II is similar to Algorithm I, but it does not use PBFO. It uses GA to select and embed the coefficients directly. We compare the performance of Algorithm I and Algorithm II using peak signal-to-noise ratio (PSNR) and payload. PSNR measures the similarity between two images, where higher values indicate better quality. Payload measures how many bits of information can be embedded per pixel in an image, where higher values indicate more capacity. We use grayscale medical images from a public database as cover images, and random binary strings as secret messages. We vary the length of the secret message from 0.1 to 0.7 bits per pixel. The results show that Algorithm I has better performance than Algorithm II in terms of PSNR and payload. Algorithm I produces less distortion and can embed more information than Algorithm II. Therefore, Algorithm I is more suitable for watermarking and steganography in medical images than Algorithm II. We also discuss some possible applications and challenges of watermarking and steganography in the healthcare domain.

Keywords: watermarking, steganography, medical images, discrete wavelet transform, discrete cosine transform, parallel bacterial foraging optimization, genetic algorithm.

INTRODUCTION

Digital medical images can now be shared globally for services such as telemedicine, teleradiology, teleradiology, teleradiology, and teleconsultation as a result of the extensive proliferation of computer networks and the prevalence of electronic medical record management. Immediate diagnosis and understanding of a disease, as well as a reduction in the number of misdiagnoses, have had significant social and economic effects, highlighting the need for efficient patient information sharing between hospital specialists. Priority number one in the management of medical images is protecting the patient's records from tampering by unauthorized individuals. Thus, the primary concern of the current electronic medical system is the development of a standard solution to preserve the authenticity and integrity of medical image content [1, 2].

As a result, one solution to the aforementioned problem is the use of digital watermarking. In other words, watermarking can improve the security of medical photographs by injecting specific information, known as a watermark or concealed data, in a non-obtrusive manner. Watermark data is often added in binary format to the pixel value of the host image. This information can then be recovered and used to determine if the medical image was disseminated by the correct source (authenticity) or whether it belongs to the correct patient (integrity) [3].

Data hiding techniques have been widely employed in a variety of applications, including copyright protection, data integrity, covert communication, non-repudiation, and authentication. Data concealing technologies, such as digital watermarking and steganography, are becoming increasingly important in ensuring multimedia security in the context of increased dissemination and distribution of multimedia material (text, music, video, etc.) over the internet. Many data-concealing approaches seek to achieve optimal performance due to the complimentary nature of these methods' general needs, including imperceptibility, resilience, security, and capacity. In addition to the aforementioned classical applications of data hiding, new application scenarios have emerged in recent years [4]. Among these new applications of data hiding are transaction tracking that protects privacy, digital watermarking for data provenance, digital watermarking for forensics, network flow watermarking, network steganography, VoIP steganography, steganography for criminals and terrorists, and steganography for malware injection.

Watermarking methods are categorised depending on their perspectives. This paper covers many types of watermarking procedures. Watermarking algorithms can be classed as spatial or transform domain based on the embedding information notion [4]. The watermark information is directly included in the pixel value of the host or cover image in the spatial domain. These methods are quick and easy to use, and they have a large capacity for embedding watermarks. Spatial domain approaches have certain advantages and can defeat cropping assaults, but their main disadvantage is their vulnerability to noise or lossy compression attacks. Furthermore, once the mechanism is discovered, implanted watermarks can be simply updated by a third party [5, 6]. The watermarked image is obtained in the transform domain by inserting the watermark onto the modified version of the source image [7]. In the following sections, we will look at several of these transformations and analyze their advantages and disadvantages.

The two key features, robustness and imperceptibility, are critical in protecting photographs from unlawful use. Robustness refers to the ability to recognize the watermark picture after

applying common signal processing aberrations. The embedded watermarks are unnoticeable both perceptually and statistically, and they have no effect on the aesthetics of the watermarked multimedia content. The strength of the watermark is maintained when embedding it into the host image without taking into account the host image's local distribution. As a result, some unnecessary visible things arise in the smooth zones. As the watermark strength or amplification factor is reduced, these deformations decrease. However, robustness cannot be attained throughout this process. As a result, the watermark must be perceptually formed, with appropriate amplification values for DWT sub-bands. The selection of amplification factors can be thought of as an optimization problem that can be solved using the Genetic Algorithm.

Watermarking methods are classified into visible and invisible watermarks based on human perception. Logos are a prominent example of visible approaches, as they are placed in the corners of photos or videos to protect the content or copyright. Invisible watermarks can be used for authentication, integrity verification, and copyright protection. Watermarking that is both visible and invisible can be utilized at the same time. The invisible watermark can serve as a backup for the visible one in this situation. This is referred to as the dual watermarking technique [8, 9].

Wu et al. [10] have proposed an innovative DWT watermarking scheme for audio signals based on Genetic Algorithms. Using genetic algorithms, the optimal localization and intensity were determined, and the method was found to be resistant to cropping, low-pass filtering, and additive noise. Wu J.Y. et al. [11] described an imperceptible and secure digital image watermarking scheme based on DWT and DCT. Similarly, Krishnasamy et al. [12] developed a DWT-based technique for fidelity and robustness evaluation. These algorithms were able to extract the watermark, but they suffered from the problems of unsatisfactory values of fidelity and robustness against various assaults. Zhicheng Wei et al. [13] proposed an algorithm that produced an invisible-to-human-eyes and robust-to-various-image-manipulation watermark, and the results demonstrated that only a few specific positions were optimal for embedding the watermark. The authors used GA to train the frequency set for embedding the watermark and compared their approach to Cox's method [14] to demonstrate its robustness. In this procedure, the analysis of GA was limited to JPEG compression attacks. Jin Cong et al. proposed a scheme in [15] that does not require the original image because the neural network memorized the information from the shape-specific elements of the original image. This scheme resists geometric attacks using the shape-specific points technique and the point matching method based on the genetic algorithm. To evaluate the robustness of digital image watermarking techniques, Hamdia et al. [16] proposed a new flexible and efficient evaluation tool based on genetic algorithms. Given a set of potential assaults, the method identifies the unwatermarked image with the highest Weighted Peak Signal-to-Noise Ratio (WPSNR). Wu Q. [17] proposed a novel watermarking scheme based on genetic algorithms (GA) in the transform domain, taking into account the image quality of the watermarked data.

In this paper, we combined DWT+ DCT+PBFO+GA algorithms called Algorithm I and combined DWT+DCT+GA called Algorithm II, by optimizing the watermark amplification factor at each selected DWT sub-band will enhance the watermark's imperceptibility and resistance to attacks. As a basis for evaluating the fitness function, the proposed method employs the normalized correlation between the cover image and the watermarked images. The fitness

function serves as the objective function to be optimized and examines the population for suitable embedding locations for the watermark within the cover image.

EXTRACTION PROCESS OF THE WATERMARK USING ALGORITHM I AND II METHOD WITH THE BEST CHROMOSOME PARAMETERS

The extraction process of the watermark using the Algorithm I and II method is a technique for protecting digital data by embedding a watermark image within a host image using the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT), and Parallel Bacterial Foraging Optimization (PBFO). The PBFO is a meta-heuristic algorithm that imitates the foraging behavior of bacteria and employs the Genetic Algorithm (GA) to enhance the population's diversity and convergence [18].

The watermarked image is the input for this procedure. The DWT-DCT-SVD combination is used to derive the watermark with the scaling factors of the singular value modification having their values optimized [19]. The optimal chromosome parameters for PBFO+GA are problem and fitness function dependent. There is no single optimal value for such parameters. The extraction process for the PBFO and GA algorithm is illustrated in Figure 1b. However, the following are some ways to locate them:

Parameter Tuning

This is an offline parameter search that attempts various parameter combinations prior to executing the GA. Simple parameter sweep, meta-GA on top of a GA, racing strategy, or meta-GA and racing together are some techniques for parameter tuning [20].

Parameter Control

This is an online parameter adjustment that modifies the GA run's parameters. Adaptive probabilities for mutation and crossover, self-adaptive population size, and deterministic genetic operators are some techniques for parameter control [20].

Advantages of PBFO Over Other Optimization Algorithms

BBFO is a nature-inspired optimization algorithm that minimizes the foraging behavior of bacteria and employs GA to increase the population's diversity and convergence. It is a gradient-free and local optima avoidance method that can handle complex and nonlinear problems, it has a high scalability across different problem domains and can handle multiple objectives, it is suitable for parallel and distributed computing due to its collective robustness and individual simplicity, and it can incorporate prior knowledge and constraints into the search process by utilizing heuristics [21].

EMBEDDING PROCESS OF THE WATERMARK USING ALGORITHM I AND II METHOD WITH THE BEST CHROMOSOME PARAMETERS

The embedding procedure of the watermark using the Algorithm I and II method is a technique for protecting digital data by embedding a watermark image within a host image using the Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Parallel Bacterial Foraging Optimization (PBFO). The PBFO is a meta-heuristic algorithm that imitates the foraging behavior of bacteria and optimizes the scaling factors of the singular value modification using the Genetic Algorithm (GA).

This process accepts as input the host image and the watermark image. Both images are subjected to DWT to separate them into four sub-bands: LL, LH, HL, and HH. DWT further decomposes the LL sub-band of the host image into four sub-bands. The DCT is then applied to the LL sub-band of the watermark image and the LL sub-band of the host image's second level decomposition. To acquire the singular values, the singular value decomposition (SVD) is applied to both DCT coefficients. Using a scaling factor, the singular values of the watermark image are incorporated into the singular values of the host image. To acquire the watermarked image, the inverse SVD, inverse DCT, and inverse DWT are used. The embedding process for the PBFO and GA watermarking scheme is represented by Figure 1a.

The optimal chromosome parameters for PBFO+GA are derived by optimizing an objective function measuring the trade-off between imperceptibility and robustness of the watermarking scheme using genetic algorithms. The objective function is described as follows:

$$f(x) = \alpha PSNR(x) + \beta NC(x)$$

where α and β are weighting coefficients and x is a vector of scaling factors. The genetic algorithm makes use of a binary encoding scheme, a roulette wheel selection method, a single-point crossover operator, and a bit-flip mutation operator.

Advantage of using GA over PBFO optimization process

GA is a population-based optimization algorithm that generates novel solutions from existing ones using biological operators such as selection, crossover, and mutation. By refining the scaling factors of the singular value modification, the efficacy of PBFO can be enhanced using GA. The following are some of the advantages of using GA over PBFO for optimization: GA can investigate a more expansive and diverse search space than PBFO, which may be constrained by the initial population size and chemotaxis steps, using crossover and mutation operators that introduce new genetic material and diversity to the population, genetic adaptation can avoid premature convergence and stagnation, the GA is more adept at handling discrete and continuous variables than PBFO, which may necessitate specialized encoding schemes or operators for discrete variables, using adaptive probabilities for mutation and crossover, self-adaptive population size, or deterministic genetic operators, genetic algorithms can adapt to dynamic and chaotic environments.

Advantage of using PBFO over GA optimization process and how GA improves the performance of PBFO

The PBFO is a nature-inspired optimization algorithm that imitates the behavior of bacteria during foraging and uses GA to optimize the scaling factors of the singular value modification. PBFO has the following advantages over the GA optimization process: the PBFO can exploit the local information and gradient of the objective function by using chemotaxis and swarming operators, which can increase the convergence speed and accuracy. The PBFO can maintain a good balance between exploration and exploitation by using elimination-dispersal and reproduction operators, which can prevent premature convergence and stagnation.

GA is a population-based optimization algorithm that generates novel solutions from existing ones using biological operators such as selection, crossover, and mutation. By optimizing the

scaling factors of singular value modification, GA can enhance the efficacy of PBFO. Among the methods in which GA can enhance the efficacy of PBFO are the following:

- By fine-tuning the scaling factors, GA can achieve a more optimal balance between imperceptibility and robustness of the watermarking scheme.
- GA can investigate a larger and more diverse space for optimal scaling factors than PBFO, which may be constrained by the initial population size and chemotaxis steps [22].
- Using crossover and mutation operators, genetic adaptation can introduce new genetic material and diversity into a population, which can aid in escaping local optimums and stagnation.
- Using adaptive probabilities for mutation and crossover, self-adaptive population size, or deterministic genetic operator, GA can adapt to dynamic and noisy environments.

Some of the gains of PBFO and GA watermarking technique algorithm are: PBFO and GA are stochastic optimization techniques that can discover the optimal solution for watermark embedding and extraction by exploring the search space and employing evolutionary operators; by selecting the optimal coefficients and quantization stages for watermark embedding and the optimal secret key and threshold for watermark extraction, PBFO and GA can enhance the watermark's imperceptibility and robustness; the PBFO and GA can adapt to the dynamic changes of the image and prevent becoming caught in local optima by increasing the population's diversity and convergence.

Nevertheless, the combined PBFO and GA techniques have some limitations: both PBFO and GA are computationally intensive and time-consuming methods that require a large number of iterations and evaluations to find the optimal solution; Both PBFO and GA are sensitive to the selection of performance-influencing parameters such as population size, mutation rate, crossover rate, chemotaxis step size, etc.; If the parameters are not correctly calibrated, PBFO and GA may not guarantee the global optimality of the solution and may suffer from premature convergence or stagnation.

MEDICAL IMAGE WATERMARKING REQUIREMENTS

In addition to the fundamental criteria of a standard watermarking system, as previously mentioned, the medical watermarking system requires several additional capabilities. These are discussed more below:

Imperceptibility

The level of invisibility of a watermarked picture in comparison to a non-watermarked image may be quantified using statistical standard metrics such as SSIM or PSNR.

Reversibility:

Due to picture quality, the used method for medical watermarking should be reversible, which means that the original image should be recoverable after removing the watermark [23].

Integrity Control

The ability to ensure that the picture has not been altered without permission.

Authentication

Authentication entails identifying the picture source and confirming that the image belongs to the proper patient [23]. Finding and developing novel watermarking techniques that meet these needs is clearly a vital important research subject.

BLOCK-DIAGRAM FOR COMBINED DCT, DWT, PFO, PBFO AND GA WATERMARKING TECHNIQUE

The DCT (Discrete Cosine Transform) is a mathematical technique that converts an image into a set of coefficients representing its frequency components. DCT is frequently used for image compression and watermarking because it can reduce the amount of data without sacrificing a significant quantity of information. The DWT (Discrete Wavelet Transform) is an additional mathematical technique that transforms an image into a set of coefficients representing its various scales and orientations. DWT is also utilized for image compression and watermarking due to its ability to capture an image's local characteristics and boundaries. The PFO (Particle Filter Optimization) is a stochastic optimization method that employs a population of particles to explore the search space and identify the optimal solution. PFO is frequently used for image watermarking because it can adapt to the dynamic changes of the image and increase the watermark's robustness. The PBFO (Parallel Bacterial forage Optimization) is a variation of PFO that imitates the behavior of bacteria during forage. PBFO is also utilized for image watermarking due to its ability to increase the diversity and convergence of the particles and prevent them from becoming confined in local optima. The GA (Genetic Algorithm) is a stochastic optimization technique that imitates the process of natural evolution. GA is also used for image watermarking because genetic operators such as selection, crossover, and mutation can generate diverse and high-quality solutions.

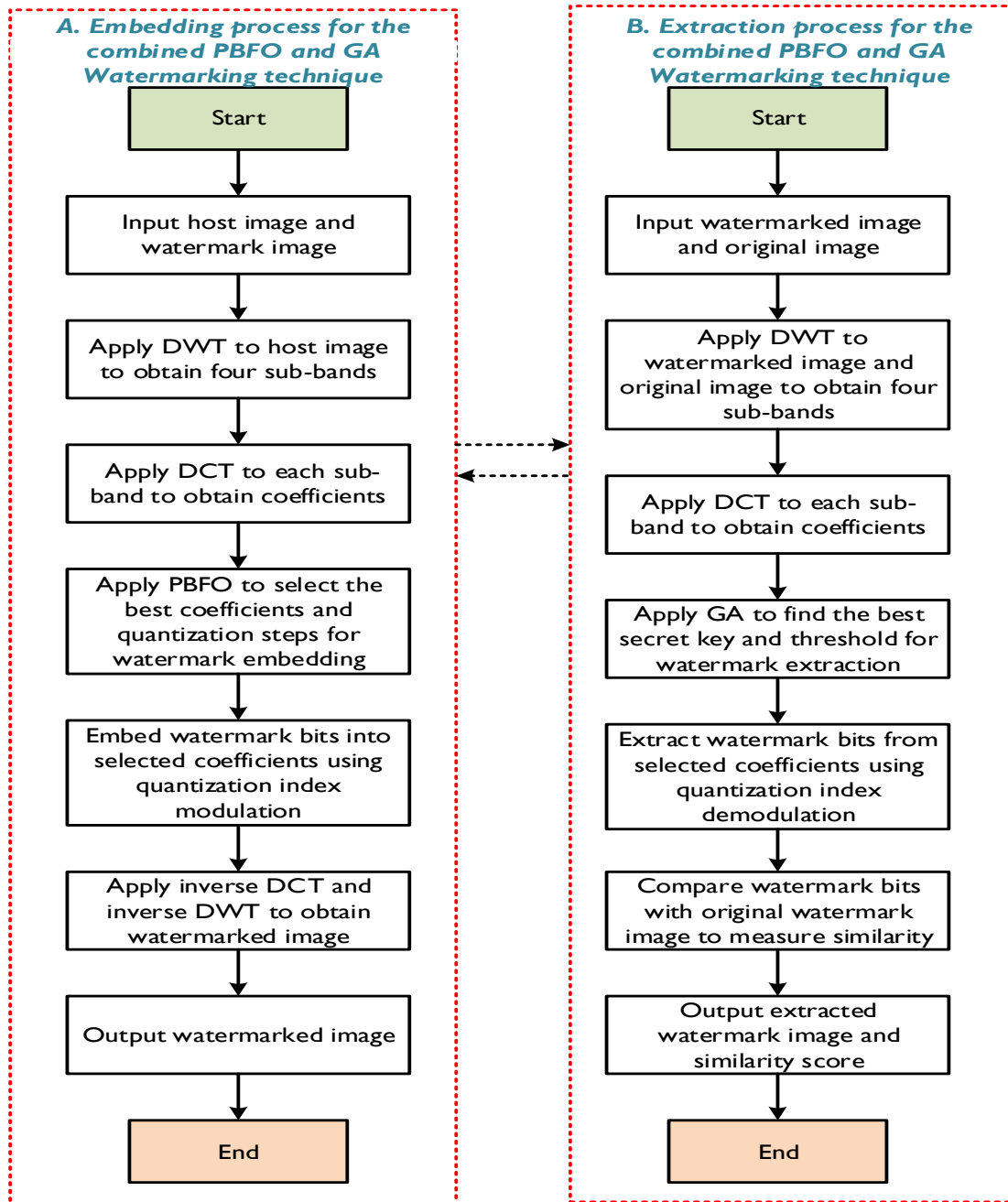


Figure 1: The embedding and extraction process of PBFO and GA watermarking scheme

These techniques can be combined in a variety of ways to produce a watermarking scheme that embeds a hidden message or logo within an image. One scheme [18] uses DWT to decompose the source image into four sub-bands, then applies DCT to each sub-band and embeds the watermark using PBFO into the selected DCT coefficients. Another method [24] uses DWT to decompose the host image into three levels, then applies DCT to the low-frequency sub-band and embeds the watermark using BFO or PSO/PBFO in the selected DCT coefficients represented by a block-diagram in Figure 2.

The block diagram for the combined DCT, DWT, PFO, PBFO, and GA watermarking technique is a method for embedding secret data within an image or video using various transformation and

optimization techniques. The Discrete Cosine Transform transforms an image into a frequency domain representation. DWT is the abbreviation for Discrete Wavelet Transform, which disassembles an image into sub-bands with varying resolutions. PFO stands for Particle Filter Optimization, which is a stochastic algorithm that approximates the optimal solution to a problem using a set of particles. Parallel Bacterial Foraging Optimization is a variant of PFO that imitates the behavior of bacteria in their search for sustenance sources. GA is an evolutionary algorithm that employs a population of individuals to evolve towards the optimal solution to a problem.

The combined technique's block diagram can be described as follows:

- The original image is divided into non-overlapping blocks, and each block is transformed using discrete cosine transform (DCT).
- The DWT is used to divide the DCT coefficients into four sub-bands: LL, LH, HL, and HH.
- Each non-overlapping block of the watermark image is encoded with GA.
- Using PFO or PBFO, the GA-encoded watermark blocks are embedded in the HH sub-band of the DCT coefficients.
- The watermarked HH sub-band is then combined with the other sub-bands, followed by the application of inverse DWT to obtain the watermarked DCT coefficients.
- The watermarked DCT coefficients are inverted to produce the watermarked image.

APPLICATION OF THE WATERMARKING AND STEGANOGRAPHY ALGORITHMS IN HEALTHCARE DOMAIN

Watermarking has several practical uses in the medical profession, including teleradiology, teleconferences among physicians, and medical personnel distance learning. The exchange of medical pictures between clinicians, specialists, and radiologists offers a forum for clinicians, specialists, and radiologists to debate and consult on diagnostic and therapeutic measures. In this instance, the electronic patient report (EPR) and medical photographs are delivered to the destination independently. Using watermarking techniques and including the EPR into medical photographs ensures not only the secrecy and security of the supplied data, but also the integrity of the medical images. Furthermore, watermark authentication and tampering detection methods may be utilized to identify the source of medical photos and locate the altered area [25].

In the healthcare domain, these algorithms (I and II) have various applications which we have discussed below. The watermarking algorithms depend on the application. Different algorithms have varying conditions and restrictions. The following are a few watermarking applications [26, 27]:

Copyright Security

In this application, the owner's copyright information is inserted invisibly into the digital image, and ownership can be proven by extracting this information in the event of a dispute. For this reason, the watermark should be resistant to both legal and illegal attacks. This type of watermark is not suitable for preventing users from duplicating digital images.

Fingerprinting

In this application, the proprietor must embed unique watermarks based on the identity of each consumer. It indicates that the data used as a watermark will be selected based on the customer's information. This method allows the owner to readily identify the source of illegal duplicates and the customer who violates the license agreement. This watermark should also be durable and undetectable.

Authentication and Integrity Verification

The purpose of this application is to determine if the digital image has been altered and then to pinpoint the location of the alteration. This application should employ fragile or semi-fragile watermarking algorithms, which are susceptible to content modification. Digital image watermarking is also utilized for broadcast monitoring, content description, and covert communication.

Biometric Image Security

These algorithms can be used to embed biometric features such as iris, palm print, fingerprint, etc. into other biometric images in order to create a dual authentication system that improves the security of the user's media [28].

Medical Image Protection

These algorithms can be used to embed a watermark such as a logo, signature, patient ID, etc. into medical images such as X-Ray, MRI, CT scan, etc. to protect their ownership, authenticity, and integrity [9].

Medical Image Transmission

These algorithms can be used to embed a watermark, such as a secret key or a hash value, into medical images to ensure the images' confidentiality and integrity during transmission over insecure channels [29].

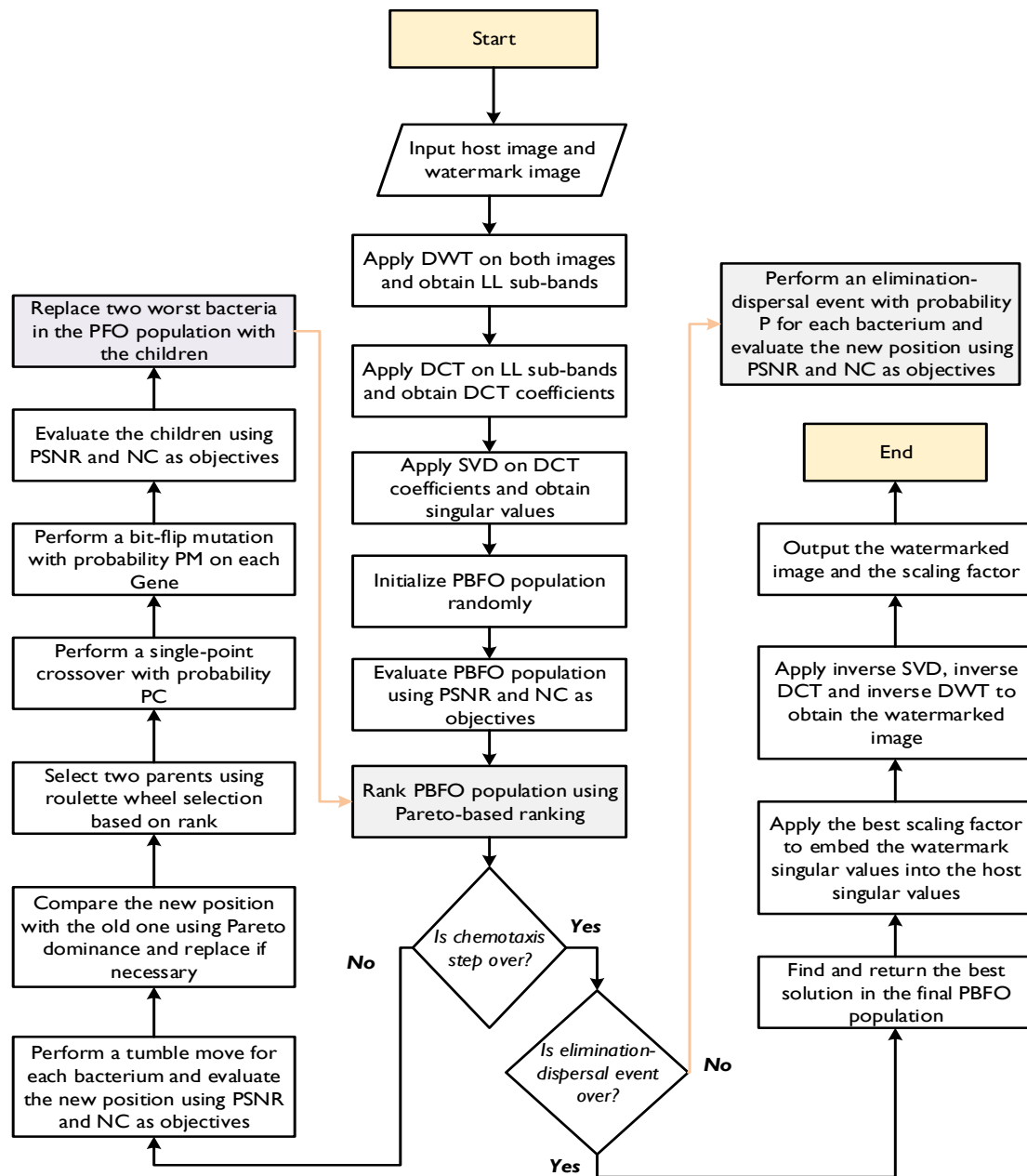


Figure 2: Block-diagram for the proposed Algorithm I and II watermarking and steganography

Watermarking Benchmarks and Performance Analysis

After removing the watermark from a medical image, the image's quality and patient information must be preserved. As a result, two groups of benchmarking are required for assessing a watermarked picture; the first is to evaluate the quality of the watermarked image, and the second is to test the accuracy of the extracted watermark.

Imperceptivity Evaluation:

When a watermark is included in a cover picture, various distortions occur. Several major distortion measures of watermarked pictures used in various literatures are discussed in by these authors [9, 30, 31]. In these equations, $I(i, j)$ represents the original picture, I_w represents the watermarked image, and $N * M$ indicates the image dimensions.

Mean Square Error:

The mean square error (MSE) is the measure between the original image and the watermarked given by the equation [1]:

$$MSE = \frac{1}{MN} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - I_w(i,j))^2 \quad [1]$$

Peak-Signal-To-Noise-Ratio:

The peak-signal-to-noise-ratio (PSNR) is the measure between the original and watermarked image, and it is obtained by the equation [2]:

$$PSNR(I, I_w) = 10 * \log_{10} \frac{(MAX_I^2)}{MSE} \quad [2]$$

Where MAX_I is the maximum possible pixel value of the original image I . The larger the PNSR means the original and watermarked image are more similar to each other. To obtain acceptable perceptual value, the PNSR should be greater than 30dB.

Structural Similarity Index:

The structural similarity index (SSIM) approach calculates the degree of similarity between two pictures [32]. SSIM can take a value between 1 and 1, with 1 indicating that the two photos are perfectly comparable to each other given by the equation [3].

$$SSIM(I, I_w) = \frac{(2\mu_I\mu_{I_w} + C_1)(2Cov + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \quad [3]$$

$$\begin{cases} C_1 = (k_1 L)^2 & k_1 = 0.01 \\ C_2 = (k_2 L)^2 & k_2 = 0.03 \end{cases}$$

Where μ_I and μ_{I_w} are average of I and I_w , respectively. μ_I^2 and $\mu_{I_w}^2$ are the variance of I and I_w , respectively. Cov is the covariance of I_w , C_1 , and C_2 are variance to stabilize the division with weak denominators, and L is the dynamic range of pixel values ($L = 2^{\text{number of bits per pixel}} - 1$).

Image Fidelity:

This metric (IF) evaluates how comparable the watermarked and unwatermarked images are. In other terms, fidelity is the extent of imperceptibility of a watermarked image's watermark. The higher the IF, the less visible the encoded data in the watermarked image is [33]. The percentage normalized root mean square error (NRMSE) is the percentage NRMSE between the original image and the embedded image value is computed by the equation representing below (equations [4] and [5]).

$$IF = 1 - \frac{\sum_{i,j} (I(i,j) - I_w(i,j))^2}{\sum_{i,j} (I(i,j))^2} \quad [4]$$

$$\%NRMSE(I, I_w) = \sqrt{\frac{\sum_{y=0}^{N-1} \sum_{x=0}^M [I(x, y) - I_w(x, y)]^2}{\sum_{y=0}^{N-1} \sum_{x=0}^{M-1} [I(x, y)]^2}} \quad [5]$$

Robustness Evaluation:

The following quantitative criteria can be used to assess the reliability of an extracted watermark for binary sequence information. $W(i, j)$ represents the original watermark in these equations, whereas $W'(i, j)$ represents the extracted watermark.

Correlation Coefficient:

The CRC may be used to determine the compatibility of the original and extracted watermarks. This matrix's minimum and maximum values are 0 and 1, respectively [32].

$$CRC = \frac{\sum_i \sum_j W(i, j) W'(i, j)}{\sqrt{\sum_i \sum_j W(i, j)^2 * \sum_i \sum_j W'(i, j)^2}}$$

Similarity Measure:

The SIM is used to quantify the similarity between an original and extracted watermark, and it is given by the equation:

$$SSIM = \frac{\sum_i \sum_j W(i, j) W'(i, j)}{\sum_i \sum_j W'(i, j)^2}$$

Bit Error Rate:

When the watermark is a binary sequence, bit error rate (BER) is a useful evaluator. BER indicates the likelihood of erroneously decoded binary patterns. As a result, the smaller the BER, the better the performance of the watermarking system.

$$BER = \frac{DB}{NB}$$

where DB is the number of bits that is decoded incorrectly and NB is the total number of original watermark bits.

Genetic Algorithm

Genetic Algorithm (GA) is a heuristic search technique for identifying global maximum/minimum solutions to problems in evolutionary computation [34, 35]. By defining the chromosomal representation, fitness function, and implementation of the GA operators, any optimization problem can be modeled in GA. The process of genetic adaptation begins with a few randomly selected genes in the first generation, known as the population. Each member of the population corresponding to a solution to the problem is referred to as a chromosome, which consists of sequences of finite length. The objective of the problem, known as the fitness function, is used to assess the quality of each chromosome within a population. Fit chromosomes are those that are of high quality, and which survive to populate the following generation. Over successive generations, the three GA operators, selection, crossover, and mutation, are routinely applied to the chromosomes to determine the optimal solution [34]. The value of the watermark amplification factor in digital image watermarking using the DWT

domain strikes a balance between imperceptibility and robustness. This equilibrium is obtained through the Genetic Algorithm-driven optimization procedure.

In digital image watermarking, the population is initialized by selecting a set of random coordinates in the cover image and inserting the watermark image in those spots. The optimal solutions for digital watermarking using DWT are determined by two crucial factors: the DWT sub-band and the watermark amplification factor value [36]. The GA algorithm searches its population for the optimal DWT sub-band and watermark amplification factor combination. The genetic algorithm procedure will seek to identify the specific sub-band that provides perceptual transparency and robustness simultaneously. To increase the algorithm's resistance to assaults, the watermark strength or amplification factor must be optimized, but this factor varies across sub-bands.

Initially, the input image is encoded using a binary string encoding scheme. The ones in the string designate where the watermarks are located. After encoding all chromosomes, the objective function is evaluated. The objective function, also referred to as the fitness function, consists of the Peak Signal-to-Noise Ratio (PSNR) and the correlation factor $\rho(\alpha * NRC)$ and is given by the function:

$$\text{Fitness function} = \text{PSNR} + 100 * \rho$$

Where PSNR is computed and illustrated in equation [2] above.

PROPOSED BENCHMARKED

There are various ways to tune the parameters of PBFO and GA, dependent on whether you want to do it offline (prior to executing the algorithm) or online (while the algorithm is running). The proposed algorithms I and II are illustrated by pseudocodes.

Among offline techniques are *simple parameter sweep*: evaluate the performance of various parameter combinations on a set of benchmark problems; *meta-GA*: use an additional GA on top of the initial GA to optimize the parameters as a second optimization problem; *racing strategy*: compare various parameter settings on a subset of problems and eradicate the worst ones until the best one is discovered.

These are some online methods include *adaptive probabilities*: modify mutation and crossover probabilities according to fitness values or population diversity; *self-adaptive population size*: alter the population size based on certain criteria, including convergence speed, diversity, fitness development, etc.; deterministic genetic operators employ fixed or periodic patterns for mutation and recombination rather than arbitrary probability.

Algorithm I pseudocode: DWT+DCT+PBFO+GA

Input: cover image C , secret message M

Output: stego image S

- 1 Convert C to grayscale and resize it to 512x512 pixels
- 2 Convert M to a binary string B
- 3 Apply DWT to C and obtain four sub-bands: LL, LH, HL, HH
- 4 Apply DCT to each sub-band and obtain four matrices of coefficients: CLL, CLH, CHL, CHH
- 5 Initialize a population of bacteria P with random positions and health values
- 6 Repeat until a termination criterion is met:
 - **For each bacterium b in P :**
 - Select a random number of coefficients from CHH as the embedding locations L
 - Embed B in L using GA and obtain a stego sub-band SHH
 - Apply inverse DCT to SHH and obtain a stego sub-band SHH'
 - Apply inverse DWT to SHH', CLH, CHL, and CLL and obtain a stego image S
 - Calculate the fitness value F of b as a function of PSNR and payload of S
 - **Update the health value H of b as $H + F$**
 - Perform chemotaxis, reproduction, and elimination-dispersal operations on P
 - Select the best bacterium b^* from P with the highest health value H^*
 - Use the embedding locations L^* and the secret message B^* of b^* to embed B^* in CHH using GA and obtain a stego sub-band SHH*
 - Apply inverse DCT to SHH* and obtain a stego sub-band SHH*'
 - Apply inverse DWT to SHH*', CLH, CHL, and CLL and obtain a stego image S^*
 - Return S^* as the output

Algorithm II pseudocode: DWT+DCT+GA

Input: cover image C , secret message M

Output: stego image S

- 1 Convert C to grayscale and resize it to 512x512 pixels
- 2 Convert M to a binary string B
- 3 Apply DWT to C and obtain four sub-bands: LL, LH, HL, HH
- 4 Apply DCT to each sub-band and obtain four matrices of coefficients: CLL, CLH, CHL, CHH
- 5 Initialize a population of chromosomes P with random binary strings of the same length as B
- 6 Repeat until a termination criterion is met:
 - **For each chromosome c in P :**
 - Embed c in CHH using a binary encoding scheme and obtain a stego sub-band SHH
 - Apply inverse DCT to SHH and obtain a stego sub-band SHH'
 - Apply inverse DWT to SHH', CLH, CHL, and CLL and obtain a stego image S
 - Calculate the fitness value F of b as a function of PSNR and payload of S
 - **Perform selection, crossover, and mutation operations on P**
 - Select the best chromosome c^* from P with the highest fitness value F^*
 - Use c^* as the secret message B^* and embed B^* in CHH using a binary encoding scheme and obtain a stego sub-band SHH*
 - Apply inverse DCT to SHH* and obtain a stego sub-band SHH*'
 - Apply inverse DWT to SHH*', CLH, CHL, and CLL and obtain a stego image S^*
 - Return S^* as the output

EXPERIMENTAL RESULTS AND ANALYSIS

Analysis

As samples for evaluating the algorithm, we used images with low, high, and medium levels of contrast. Various simulation exercises conducted on both medical images and other standard images, such as Lena, Mandrill, Brain, Barbara, Abdominal etc., have been used to evaluate the algorithm for use in the experimentation of our schemes. Several of the images tested have the standard dimensions of 512x512 and 256x256 for both colour and grayscale images. According to the literature on computer graphics, images with a higher pixel density are more effective. The number of histogram bins is always positioned to the left when images are presented in low key, to the right when they are presented in high key, and in the center when images are presented in medium key.

In order to determine the effectiveness of the algorithm and its performance matrix, we experimented the combined algorithm; Algorithm I: DWT+DCT+PBFO+GA and Algorithm II: DWT+DCT+GA for different images with a payload of 0.7bpp as shown in Table.

In order to maximize payload, our algorithm employs three out of four sub-bands for watermark embedding and frequency sub-band of 8x8 DCT. By inverting the 0.6bpp payload, the outcomes of Algorithm I and II testing for both medical images and other standard images have been achieved (tabulated in Table 5). These results were obtained using MATLAB 2020b on a 2.30GHz Intel R Core™ i7-33770 processor with 16GB of RAM.

The PSNR, NCC, SSIM, and BER matrices are utilized to evaluate the performance of watermarking or steganography algorithms. These metrics are used to evaluate an image's integrity after processing, such as compression, watermarking, or steganography. The values of these metrics depend on a number of variables, including the size and content of the image, the type and quantity of processing, and the statistical model used to compute them. Consequently, it is impossible to provide a definitive response to your query without more information about the image and its processing (Figure 3-6).

On the other hand, it seems implausible that an image could have such high PSNR and SSIM values with such low NCC and BER values, based on some general observations. PSNR and SSIM are measures of the similarity between two images, with greater values indicating superior image quality. Lower NCC and BER values indicate higher image quality. If an image has high PSNR and SSIM values, it indicates that it is very similar to the original image; consequently, it should also have high NCC and low BER values. In contrast, if an image has a low NCC and a high BER value, it indicates that it differs significantly from the original image and should therefore have a low PSNR and SSIM value (Table 1-4).

Exceptions or special circumstances may exist in which these metrics deviate from the expected trends. Some research papers have reported, for instance, that PSNR and SSIM are not always consistent with the human perception of image quality, and that NCC and BER are not always resistant to particular assaults. Therefore, it is essential to utilize multiple metrics and compare them with subjective evaluations to obtain a more precise image quality assessment.

Table 1: cover image PSNR, NCC, IF, SSIM, and BER comparison brain image using 1x35bmp

No.	Cover image of PSNR, NCC, IF Comparing brain image combination algorithms (1x35 bmp)					
	DWT	DWT+DCT	DWT+DCT +BFO	DWT+DCT +PBFO	DWT+DCT+GA	DWT+DCT+ PBFO+GA
PSNR	27.3046	48.5088	53.3750	58.6142	63.5034	88.4601
NCC	0.0019	0.0038	0.0038	0.0038	0.0038	0.0038
IF	-0.0384	-2.4368e-04	-1.0236e-04	-2.2202e-05	-3.5234e-05	-3.3034e-05
SSIM	1	1	1	1	1	1
BER	0	0	0	0	0	0

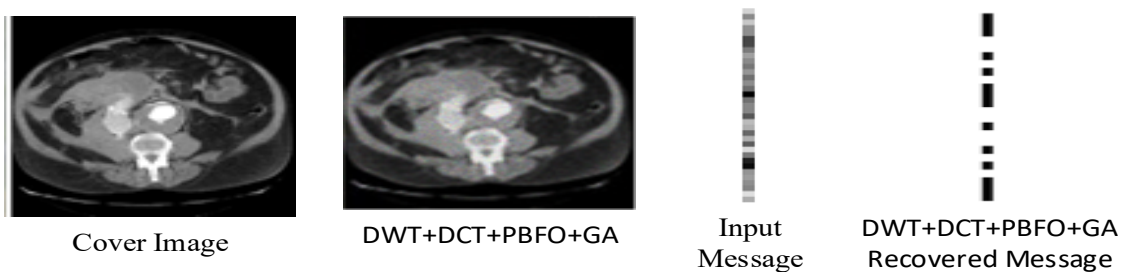


Figure 3: Cover brain image, watermark, key, and recovery message using 1x35bmp

Table 2: Cover image PSNR, NCC, IF, SSIM, and BER comparison Brain image using 12x9bmp

No	Cover image of PSNR, NCC, IF Comparing brain image combination algorithms (12x9 bmp)					
	DWT	DWT+DCT	DWT+DCT +BFO	DWT+DCT +PBFO	DWT+DCT+GA	DWT+DCT+ PBFO+GA
PSNR	28.3046	45.5088	49.2759	55.9132	60.5902	87.3211
NCC	0.0036	0.0049	0.0049	0.0049	0.0038	0.0038
IF	-0.0384	-2.4368e-04	-1.0236e-04	-2.2202e-05	-3.5234e-05	-3.3034e-05
SSIM	1	1	1	1	1	1
BER	0	0	0	0	0	0

(Brain with key)

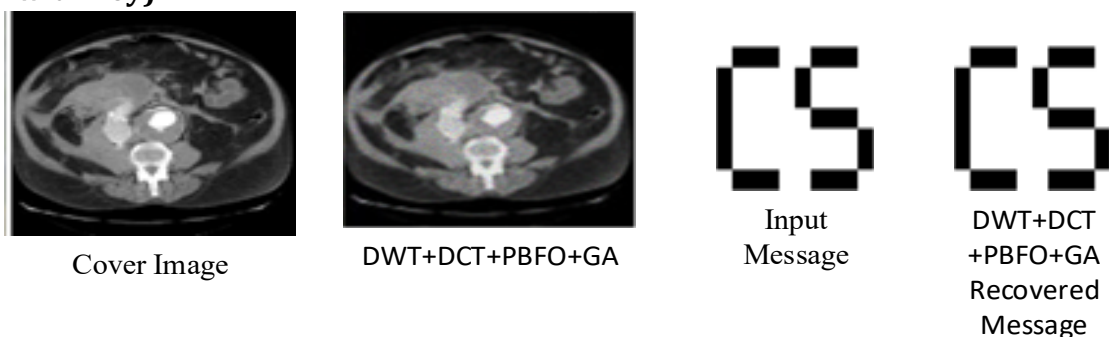


Figure 4: Cover Brain image, watermark, key, and recovery message using 12x9bmp

Table 3: The cover image PSNR, NCC, IF, SSIM, and BER comparison Lena image using 1x35bmp

No	Cover image of PSNR, NCC, IF Comparing Lena image combination algorithms (1x35 bmp)					
	<i>DWT</i>	<i>DWT+DCT</i>	<i>DWT+DCT+ +BFO</i>	<i>DWT+DCT+ +PBFO</i>	<i>DWT+DCT+GA</i>	<i>DWT+DCT+ +PBFO+GA</i>
PSNR	27.6777	44.9180	48.8679	55.2328	58.9067	85.4578
NCC	0.0035	0.0049	0.0049	0.0049	0.0034	0.0035
IF	-0.0217	-6.0065e-05	-2.4190e-05	-5.5863e-06	-6.5095e-05	-6.5863e-05
SSIM	1	1	1	1	1	1
BER	0	0	0	0	0	0



Figure 5: The cover Lena image, watermark, key, and recovery message using 1x35bmp

Table 3: The cover image PSNR, NCC, IF, SSIM, and BER comparison Lena image using 12x9bmp

No	Cover image of PSNR, NCC, IF Comparing Lena image combination algorithms (12x9bmp)					
	<i>DWT</i>	<i>DWT+DCT</i>	<i>DWT+DCT+ +BFO</i>	<i>DWT+DCT+ +PBFO</i>	<i>DWT+DCT+GA</i>	<i>DWT+DCT+ +PBFO+GA</i>
PSNR	25.4835	44.8913	48.6671	54.4986	58.8067	85.1532
NCC	0.0017	0.0039	0.0039	0.0039	0.0035	0.0035
IF	-0.0366	-6.0436e-05	-2.5334e-05	-6.6152e-06	-6.4903e-05	-6.4502e-05
SSIM	1	1	1	1	1	1
BER	0	0	0	0	0	0



Figure 6: The cover Lena image, watermark, key, and recovery message using 12x9bmp

The results we obtained from the experimental analysis shows that for both images we tested our algorithm performs better against the parameters: PSNR, NCC, IF, SSIM and BER. However, when we embedded the low and high key imputed messages into the covered images, we obtained slightly higher values performance in terms of quality matrix for the low key

(recovered messages) as compared to the higher (input messages). Additionally, when we tested Mandrill cover image (512x512) pixels, the recovered message was slightly detorted with 0.97778 SSIM value (Table 4 and Figure 7).

Table 4: The cover image PSNR, NCC, IF, SSIM, and BER comparison Mandrill image using 12x9bmp

No	Cover image of PSNR, NCC, IF Comparing Lena image combination algorithms (12x9bmp)					
	<i>DWT</i>	<i>DWT+DCT</i>	<i>DWT+DCT+ +BFO</i>	<i>DWT+DCT+ +PBFO</i>	<i>DWT+DCT+GA</i>	<i>DWT+DCT+ PBFO+GA</i>
PSNR	25.3300	44.8913	48.6660	54.6031	59.6032	86.3561
NCC	0.0021	0.0034	0.0032	0.0028	0.0025	0.0024
IF	-0.0306	-9.6025e-05	-4.0264-05	-1.0261e-05	-2.5503e-05	-2.0234e-05
SSIM	1	1	1	0.9856	0.9847	0.9778
BER	0	0	0	0	0	0

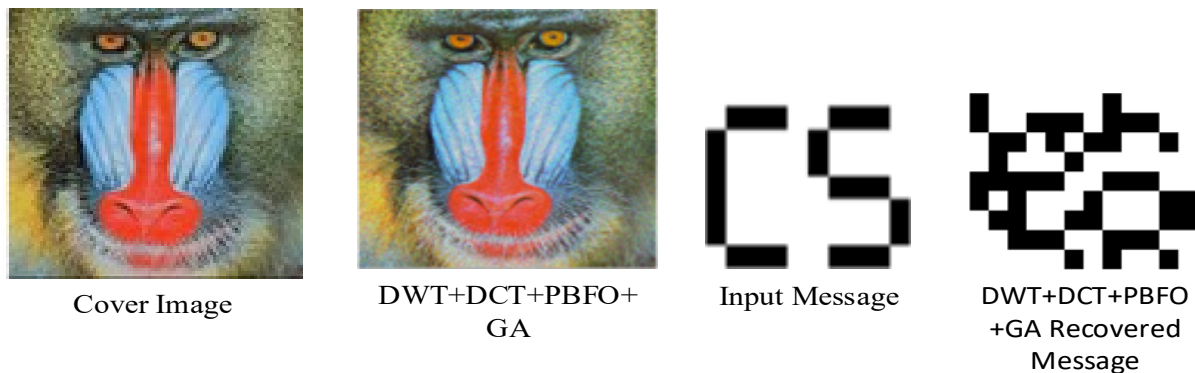


Figure 7: The cover Mandrill image, watermark, key, and recovery message using 12x9bmp

Algorithm I and II Explained

Steganography is the practice of concealing a secret message within an image or other medium in such a way that it cannot be detected by an observer. Two criteria can be used to evaluate the efficacy of a steganography algorithm: imperceptibility and capacity. Imperceptibility denotes that the stego image (the image containing the embedded message) should not have discernible distortions relative to the cover image (the original image). Capacity refers to the ability of the stego image to transport as much information as possible without compromising its undetectability.

Two metrics that can be used to evaluate imperceptibility and capacity, respectively, are PSNR and payload. PSNR is a measure of the similarity between two images, with greater values indicating a higher quality. Payload is a measurement of how many bits of data can be embedded per pixel in an image, with higher values indicating greater capacity. A steganography algorithm should ideally have a high PSNR and a large payload.

Algorithms I and II are based on discrete wavelet transform (DWT) and discrete cosine transform (DCT), which decompose an image into various frequency components. The discrete wavelet transform (DWT) divides an image into four sub-bands: low-low (LL), low-high (LH), high-low (HL), and high-high (HH). DCT transforms each sub-band into a matrix of coefficients representing the sub-band's spatial frequency content. Afterwards, the secret message is

embedded in some of the coefficients using genetic algorithm (GA), a technique that mimics natural evolution to discover optimal solutions.

Algorithm I employs parallel bacterial foraging optimization (PBFO) prior to GA, whereas Algorithm II does not. PBFO is a technique that imitates the behavior of microorganisms when searching for optimal solutions. PBFO can assist in selecting the optimal coefficients for message encoding so that distortion is minimized, and robustness is maximized.

On the basis of the PSNR and payload values shown in Table 4, Algorithm I performs better than Algorithm II (see Table 4). Algorithm I has a higher PSNR value than Algorithm II (for all medical images and other standard images tested), indicating that Algorithm I produces less image distortion than Algorithm II. Algorithm I also has a higher payload value than Algorithm II, meaning that Algorithm I can embed more information into the stego image. Algorithm I is therefore more imperceptible and has greater capacity than Algorithm II.

One possible explanation for this distinction is that PBFO improves the efficacy of GA by providing superior initial solutions and reducing the search space. PBFO can also help to strike a balance between imperceptibility and capacity by selecting coefficients that have a smaller impact on visual quality and a greater impact on robustness. Therefore, PBFO can increase the effectiveness and efficacy of GA in discovering optimal steganography solutions.

Table 5: PSNR (dB) Vs Payload (bpp) based comparison of Algorithm I and II

Image	Payload (bpp)	0.1	0.2	0.3	0.4	0.5	0.6	0.7
Lena	Effective payload	0.58						
	Algorithm I: DWT+DCT+PBFO+GA	59.81	54.54	53.23	52.33	51.63	50.32	49.31
	Algorithm II: DWT+DCT+GA	58.21	53.32	51.91	50.45	49.01	47.02	48.56
Barbara	Effective payload	0.48						
	Algorithm I: DWT+DCT+PBFO+GA	89.24	87.32	45.68	44.81	44.11	43.10	42.43
	Algorithm II: DWT+DCT+GA	85.15	84.21	85.71	84.82	84.12	83.21	83.11
X-ray	Effective payload	>0.6						
	Algorithm I: DWT+DCT+PBFO+GA	87.44	86.23	83.45	80.40	75.82	73.24	70.89
	Algorithm II: DWT+DCT+GA	85.23	82.34	80.35	78.32	74.23	70.45	65.45
Brain	Effective payload	>0.6						
	Algorithm I: DWT+DCT+PBFO+GA	87.64	85.82	81.35	78.23	75.35	73.45	70.23
	Algorithm II: DWT+DCT+GA	84.30	83.03	80.41	81.26	79.25	76.45	67.32
Mandrill	Effective payload	>0.6						
	Algorithm I: DWT+DCT+PBFO+GA	84.23	81.31	79.23	77.89	75.88	74.06	72.23
	Algorithm II: DWT+DCT+GA	82.34	79.89	77.26	75.09	73.25	72.56	70.43

CONCLUSION

In telemedicine applications, watermarking frequency and steganography are two methods for securing medical images. To safeguard the ownership and integrity of an image, watermarking frequency embeds a watermark in the frequency domain of the image, such as the discrete cosine transform (DCT) coefficients. Steganography conceals a secret message within an image by manipulating pixels or coefficients in an imperceptible manner.

Algorithm I and Algorithm II are examples of frequency watermarking and steganography, respectively. Algorithm I uses a public key and a private key to generate a binary sequence of

pseudorandom numbers that indicates where the secret message's components will be inserted. The insertion occurs at the first seven AC coefficients in the DCT domain after transformation. Algorithm II makes use of an adaptive frequency-domain channel attention network (AFcaNet) to assign weights to each frequency channel and improve the capability of feature extraction. In addition, the network employs a low-frequency loss function to reduce image distortion in low-frequency regions.

Both Algorithm I and Algorithm II for watermarking and steganography of medical images are based on frequency domain techniques. In terms of capacity and security, they are superior to spatial domain approaches. However, they face some constraints and obstacles. For instance, Algorithm I may be vulnerable to assaults that target the DCT coefficients, such as compression and cropping. Optimal performance of Algorithm II may require additional computational resources and training data. Future research can therefore concentrate on enhancing the robustness and efficacy of these algorithms and investigating other frequency domain transformations, such as the discrete wavelet transform and discrete Fourier transform.

Reference

- [1] Aruna, M., Arulkumar, V., Deepa, M. and Latha, G.C.P., 2022, March. Medical Healthcare System with Hybrid Block based Predictive models for Quality preserving in Medical Images using Machine Learning Techniques. In 2022 International Conference on Advanced Computing Technologies and Applications (ICACTA) (pp. 1-10). IEEE.
- [2] Liu, X., Lou, J., Fang, H., Chen, Y., Ouyang, P., Wang, Y., Zou, B. and Wang, L., 2019. A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. *Ieee Access*, 7, pp.76580-76598.
- [3] Aparna, P. and Kishore, P.V.V., 2019. A blind medical image watermarking for secure E-healthcare application using crypto-watermarking system. *Journal of Intelligent Systems*, 29(1), pp.1558-1575.
- [4] Megías, D. Data hiding: new opportunities for security and privacy? In *Proceedings of the European Interdisciplinary Cybersecurity Conference (EICC 2020)*, Rennes, France, 18 November 2020; Article No.: 15. pp. 1–6. [CrossRef]
- [5] Abraham, J. and Paul, V., 2019. An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University-Computer and Information Sciences*, 31(1), pp.125-133.
- [6] Jayashree, N. and Bhuvaneswaran, R.S., 2019. A robust image watermarking scheme using z-transform, discrete wavelet transforms and bidiagonal singular value decomposition. *Comput. Mater. Continua*, 58(1), pp.263-285.
- [7] Anand, A. and Singh, A.K., 2021. Watermarking techniques for medical data authentication: a survey. *Multimedia Tools and Applications*, 80, pp.30165-30197.
- [8] Anand, A. and Singh, A.K., 2022. Dual watermarking for security of COVID-19 patient record. *IEEE Transactions on Dependable and Secure Computing*.
- [9] Fofanah, A.J. and Gao, T., 2020, May. Dual Watermarking for Protection of Medical Images based on Watermarking of Frequency Domain and Genetic Programming. In *Proceedings of the 2020 the 4th International Conference on Innovation in Artificial Intelligence* (pp. 106-115).
- [10] Wu, Q., Qu, A., Huang, D. and Ma, L., 2021. Robust and Blind Audio Watermarking Scheme Based on Genetic Algorithm in Dual Transform Domain. *Mathematical Problems in Engineering*, 2021, pp.1-14.

-
- [11] Wu, J.Y., Huang, W.L., Xia-Hou, W.M., Zou, W.P. and Gong, L.H., 2020. Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition. *Multimedia Tools and Applications*, 79, pp.22727-22747.
- [12] Krishnasamy, Balasamy, M. Balakrishnan, and Arockia Christopher. "A genetic algorithm based medical image watermarking for improving robustness and fidelity in wavelet domain." In *Intelligent Data Engineering and Analytics: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020)*, Volume 2, pp. 289-299. Springer Singapore, 2021.
- [13] Zhicheng Wei, Hao Li and Jufeng Dai, "Image Watermarking Based on Genetic Algorithm", *Proceedings of International Conference on Multimedia and Expo*, pp.1117-1120, 2006.
- [14] Zahidova, G.A., 2021, November. DIGITAL WATERMARKING AND STEGANOGRAPHY. In *nd 2 INTERNATIONAL SCIENCE AND ENGINEERING CONFERENCE*.
- [15] Cong Jin, "Affine invariant watermarking algorithm using feature matching", *Digital Signal Processing*, Vol. 16, No.3, pp. 247-254, 2006.
- [16] Hamdia, K.M., Zhuang, X. and Rabczuk, T., 2021. An efficient optimization approach for designing machine learning models based on genetic algorithm. *Neural Computing and Applications*, 33, pp.1923-1933.
- [17] Wu, Q., Qu, A., Huang, D. and Ma, L., 2021. Robust and Blind Audio Watermarking Scheme Based on Genetic Algorithm in Dual Transform Domain. *Mathematical Problems in Engineering*, 2021, pp.1-14.
- [18] A. Singh, A. Kumar and M. K. Dutta, "DWT, DCT and PBFO based Approach for Biometric Image Security," 2020 International Conference on Contemporary Computing and Applications (IC3A), Lucknow, India, 2020, pp. 298-303, doi: 10.1109/IC3A48958.2020.233317.
- [19] Hiba Abdel-Nabi, Ali Al-Haj, Chapter 2 - Frequency domain-based data hiding for encrypted medical images, Editor(s): Amit Kumar Singh, Mohamed Elhoseny, In *Intelligent Data-Centric Systems, Intelligent Data Security Solutions for e-Health Applications*, Academic Press, 2020, Pages 21-56, ISBN 9780128195116, <https://doi.org/10.1016/B978-0-12-819511-6.00002-9>.
- [20] Nikola Jovanovic (2023). Digital Watermarking – Comparison of DCT and DWT methods (<https://github.com/etfovac/watermark/releases/tag/v1.2.3>), GitHub. Retrieved May 23, 2023.
- [21] Sharifi, M.R., Akbarifard, S., Qaderi, K. et al. A new optimization algorithm to solve multi-objective problems. *Sci Rep* 11, 20326 (2021). <https://doi.org/10.1038/s41598-021-99617-x>
- [22] Yassami, M. and Ashtari, P., 2023. A novel hybrid optimization algorithm: Dynamic hybrid optimization algorithm. *Multimedia Tools and Applications*, pp.1-33.
- [23] Memon, N.A. and Alzahrani, A., 2020. Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection. *Ieee Access*, 8, pp.75448-75462.
- [24] K. Suniti Singh, P. Singh and H. Vikram Singh, "Design and Analysis of BFO-PBFO based Optimized Watermarking Algorithm for Medical Images," 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE), MANGALORE, India, 2022, pp. 166-171, doi: 10.1109/ICRAIE56454.2022.10054270.
- [25] Singh, A.K., Kumar, B., Singh, G. and Mohan, A., 2017. Medical image watermarking. Springer Science+ Business Media.
- [26] Jabade VS, Gengaje SR: Literature review of wavelet based digital image watermarking techniques. *Int J Comp Appl* 31(1):28–35, 2011
-

- [27] Adnan WAW, Hitarn S, Abdul-Karim S, Tamjis MR: A review of image watermarking, in *Research and Development*, 2003. SCORED 2003. Proceedings. Student Conference. pp 381–384, 2003.
- [28] Mousavi, S.M., Naghsh, A. and Abu-Bakar, S.A.R., 2014. Watermarking techniques used in medical images: a survey. *Journal of digital imaging*, 27, pp.714-729.
- [29] Malayil, M.V. and Vedhanayagam, M., 2021. A novel image scaling based reversible watermarking scheme for secure medical image transmission. *ISA transactions*, 108, pp.269-281.
- [30] Hui, Z. and Zhou, Q., 2020. A novel high payload steganography scheme based on absolute moment block truncation coding. *Multimedia Tools and Applications*, 79(33-34), pp.24241-24264.
- [31] Ahmad, B., Kamili, A., Gull, S. and Parah, S.A., 2021. Data Embedding in Color Images: A Secure Data Communication Framework Based on Modular Arithmetic. *Multimedia Security: Algorithm Development, Analysis and Applications*, pp.157-176.
- [32] Sivananthamaitrey, P. and Kumar, P.R., 2022. Optimal dual watermarking of color images with SWT and SVD through genetic algorithm. *Circuits, Systems, and Signal Processing*, 41, pp.224-248.
- [33] Krishnasamy, Balasamy, M. Balakrishnan, and Arockia Christopher. "A genetic algorithm based medical image watermarking for improving robustness and fidelity in wavelet domain." In *Intelligent Data Engineering and Analytics: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020)*, Volume 2, pp. 289-299. Springer Singapore, 2021.
- [34] Shukla, A.K., Pippal, S.K. and Chauhan, S.S., 2023. An empirical evaluation of teaching–learning-based optimization, genetic algorithm and particle swarm optimization. *International Journal of Computers and Applications*, 45(1), pp.36-50.
- [35] Fofanah, A.J., Koroma, S. and Bangura, H.I., 2023. Experimental Exploration of Evolutionary Algorithms and their Applications in Complex Problems: Genetic Algorithm and Particle Swarm Optimization Algorithm. *British Journal of Healthcare and Medical Research-Vol*, 10(2).
- [36] Shanmugam, K. and Nagarajan, K., 2022. Security-based teleradiology in DICOM used two-level DWT based optimization watermarking. *Concurrency and Computation: Practice and Experience*, 34(15), p.e6963.