International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimization of Multiple Scaling Factors for ECG Steganography Using Dynamic Thresholding GA

Hasanain F. Hashim *[1], Meriam Jemel [2], Nadia Ben Azzouna [2]

Submitted: 04/05/2023 **Revised:** 10/07/2023 **Accepted:** 02/08/2023

Abstract*:* Protecting patient data has become a top priority for healthcare providers in the digital age. ECG steganography is a technique for concealing electrocardiogram (ECG) signals during Internet transmission along with other medical data. This strategy aims to recover all embedded patient data while minimizing degradation of the cover signal caused by embedding. Quantization techniques make it possible to include patient information in the ECG signal, and it has been discovered that multiple scaling factors (MSFs) provide a superior trade-off than uniform single scaling factors. In this paper, we present a novel contribution to the field: a discrete wavelet transforms and singular value decomposition-based dynamic Thresholding GA (DTGA)-based ECG steganography scheme. Using the MITIH database, we demonstrate the efficacy of this method, and our findings corroborate that DTGA significantly improves data security.

Keywords: *Steganography, ECG, Genetic Algorithm, Privacy, Security*

1. Introduction.

Because medical technology has gotten better recently, it is now possible to keep an eye on everyone. To do this, the collected medical information and patient data are sent to the doctor over the Internet. During these kinds of moves, it is very important to keep patient information safe [1] [2]. In this situation, data-hiding methods like steganography can be used to hide the identity of the medical information. The goal of privacy through data hiding is paramount in today's digital age. With the ever-increasing amount of personal information being shared and stored online, it is essential to protect sensitive data from malicious actors. Data hiding techniques such as encryption and steganography provide a means to safeguard information by making it difficult or impossible for unauthorized individuals to access or decipher. By implementing strong privacy measures, individuals and organizations can ensure that their personal and confidential data remains secure and protected from potential breaches or cyber-attacks.

The steganography is the data that needs to be kept safe, and the information that carries the steganography is called the cover signal. The success of steganography rests on keeping the signal degradation caused by embedding to a minimum and being able to withstand attacks from the outside [3-6]. In the medical field, steganography techniques secure patient information by concealing it within their medical records [7]. Multiple scaling factors (MSFs) refer to a technique used in steganography to embed data into a cover signal, such as an ECG signal. MSFs are used to adjust the magnitude of the data being embedded, allowing for a better trade-off between data capacity and signal degradation. Using MSFs can improve the quality of the stego-signal and reduce the chance of detection, as compared to using uniform single scaling factors. MSFs have been found to be particularly useful in ECG steganography, where the signal is highly sensitive and any degradation can impact diagnosis and treatment. In related works [7], researchers have explored various optimization techniques for MSFs, including genetic algorithms [7] and particle swarm optimization [7]. These approaches aim to find the optimal set of MSFs that maximize data capacity while minimizing signal degradation.

In this research, the purpose of using a Dynamic Thresholding Genetic Algorithm (DTGA) in optimization problems is to enhance the optimization process's efficiency and effectiveness by adjusting the threshold value used in the selection process. This strategy enables the algorithm to concentrate on promising solutions while avoiding early convergence, resulting in a more adaptive and flexible search approach. By integrating dynamic thresholding into the genetic algorithm, it is possible to obtain superior outcomes in a shorter time frame, making it an excellent method for complex optimization problems with extensive search spaces. Ultimately, the objective is to identify the optimal solution that satisfies all the constraints and objectives of the particular problem being addressed. The following sections of this work are organized as follows. The second section displays the current relevant works. Section 3 provides a detailed description of our suggested approach using Dynamic Thresholding GA for the optimization of MSFs for ECG Steganography. Section 4 contains the results and discussion of the experiments. In

[1] *LR11ES03 SMART Lab, Universite de Tunis, ISG, Tunis, Le Bardo, Tunis, Tunisia,*
[2] *LR11ES03 SMART Lab, Universite de Tunis, ISG, Tunis, Le Bardo, Tunis, Tunisia,*
* *Corresponding Author Email: hasaneanduh@gmail.com*

Section 5, the conclusion of the work is presented.

2. Related Work

The security of sensitive information has become a significant concern in the current digital age. Using steganography and watermarking techniques is one method to protect this information. To verify ownership, these techniques involve concealing data within another file or embedding a unique identifier within a file. Steganography is the art of concealing information within other data, such as images, audio, or text, without arousing suspicion.

In the healthcare sector, steganography has emerged as a promising technique to protect sensitive patient information from unauthorized access and potential breaches. By embedding confidential medical data into seemingly harmless cover signals, such as ECG signals or medical images, healthcare professionals can ensure that patient information remains secure and confidential. Moreover, steganography can also be used to transmit medical data over insecure networks without compromising patient privacy. However, the use of steganography in healthcare requires careful consideration of various factors, including data capacity, signal degradation, and detection probability. In this context, Multiple Scaling Factors (MSFs) have emerged as an effective technique to enhance the quality and security of stego-signals in healthcare applications.

In this section we investigate the main ECG steganography and steganography techniques that were developed, as well as their benefits, limitations, and potential applications in sectors such as healthcare, finance, and national security. In addition , we explore the use of MSFs in healthcare steganography and highlight the potential benefits and challenges associated with this approach.

2.1 ECG Steganography and steganography techniques

Steganography and watermarking are both techniques used to hide information within other data, but they differ in their purpose and application. The goal of steganography is to keep the information hidden from unauthorized access and potential breaches. Steganography is often used in the healthcare sector to protect sensitive patient information. Watermarking, on the other hand, is the practice of embedding a visible or invisible mark within digital media, such as images or videos, to indicate ownership or authenticity. The goal of watermarking is to protect intellectual property rights and prevent unauthorized use or distribution of digital media. Watermarking is commonly used in the entertainment industry to protect copyrighted material.

Given that the primary objective of steganography techniques is to minimize any noticeable changes to the original cover signal, so ensuring that the detectability of the hidden information is not compromised, it can be concluded that steganography does not pose a threat to detectability. Steganography commonly utilizes transform domain techniques [8], including Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and several other methods [8]. In the context of transform domain steganography, the original signal, known as the cover signal, undergoes a decomposition process. During this process, the watermark, which is a hidden message or data, is embedded within one or several sub bands of frequencies. The existing body of literature on ECG steganography mostly centers around the exploration of several transformation and watermarking methodologies [8-9-10]. The implementation of electrocardiogram (ECG) steganography is performed in reference [8] by the utilization of discrete wavelet transform (DWT) and least significant bit (LSB) techniques.

The evaluation of the efficacy of Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) in the context of electrocardiogram (ECG) steganography is conducted in reference [9]. The study conducted in reference [9] shown that the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) provide more favorable outcomes compared to the Discrete Fourier Transform (DFT). In their study, researchers introduce a method for ECG steganography that utilizes the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), as described in reference [10]. The SVD watermarking approach is employed to embed the patient data into a certain frequency sub-band obtained using the Discrete Wavelet Transform (DWT). This embedding process occurs subsequent to the transformation of the ECG signal into a two-dimensional matrix.

However, the a critique of the limitations and gaps in these previous works. For example, the use of DWT and LSB algorithms in ECG steganography may not provide an optimal trade-off between data capacity and signal degradation. Furthermore, the authors have not highlighted the potential benefits of using MSFs in ECG steganography, which can offer better results in terms of data capacity and signal quality. Therefore, a more detailed critique of the previous works would have helped to highlight the contributions and significance of the novel approach proposed in this paper.

Scaling factors are a key part of SVD-based quantization because they keep the cover signal from getting worse [19, 20]. In the case of a single scaling factor, a low scaling factor makes it harder to notice, while a high scaling factor makes it harder to fight from the outside. So, the scale factor determines the trade-off between being hard to notice and being strong. So, the way the information is quantized is a very important part of how good it is. The constant growth factor, on the other hand, is easier to find out in case of a hack. When working with these kinds of situations, it's best to use, but you need to use optimization methods [20–23] to find them.

2.2 Approaches for MSFs optimization

The authors present a novel approach for picture watermarking in their study referenced as [24]. This approach utilizes the Lifted Wavelet Transform (LWT) and Singular Value Decomposition (SVD) techniques. The determination of the MSFs is accomplished by the utilization of the Multi Objective Ant Colony Optimization (MOACO) technique, leading to an enhancement in the robustness of the watermark while simultaneously maintaining its perceptibility. The investigation conducted in reference 16 examines the efficacy of Singular Value Decomposition (SVD)-based watermarking techniques in conjunction with Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for the purpose of copyright protection. The believability of the image is enhanced by embedding the watermark inside its core components, while the calculation of optimum MSFs is achieved by the utilization of the Particle Swarm Optimization approach.

The authors of reference [20] propose the utilization of the Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) technique for picture watermarking. This approach incorporates the Firefly Algorithm (FA) to optimize the fitness function, which is defined as a linear combination of detectability and robustness. The results of their study demonstrate that the suggested approach for picture watermarking using singular value decomposition (SVD) is capable of identifying the most effective multi-scale features (MSFs) with significantly better performance compared to currently available methods. In this study, the authors employed self-adaptive Differential Evolution (DE) in order to improve the effectiveness of picture watermarking in the context of the DWT-SVD method [22]. The utilization of a self-adaptive differential evolution (DE) technique is employed to optimize the scaling parameters in order to achieve optimal levels of robustness and invisibility.

Despite its promising results, some disadvantages are associated with related works in ECG steganography. For instance, some methods such as Particle Swarm Optimization-based ECG Steganography require a large number of iterations to achieve optimal results, leading to high computational complexity and long processing times. Additionally, these approaches may not be suitable for real-time applications due to their high computational requirements. Therefore, there is a need for more efficient and effective methods that can address these limitations and improve the performance of ECG steganography.

3. Proposed Approach

The principle of our proposed approach using DTGA-based ECG steganography scheme is to embed secret information into the ECG signal while maintaining the quality of the original signal. This is achieved through the use of dynamic thresholding GA, which optimizes the embedding process by adjusting the threshold value based on the fitness function. The scheme also employs DWT and SVD to enhance the security and robustness of the steganography technique.

This section begins by the ECG database description including the preprocessing of ECG signal and patient data, the DWT–SVD. Also addressed are the DTGA based MSFs selection and scale factors procedures. Fig.1 depicts the steps of our proposed DTGA based ECG steganography approach.

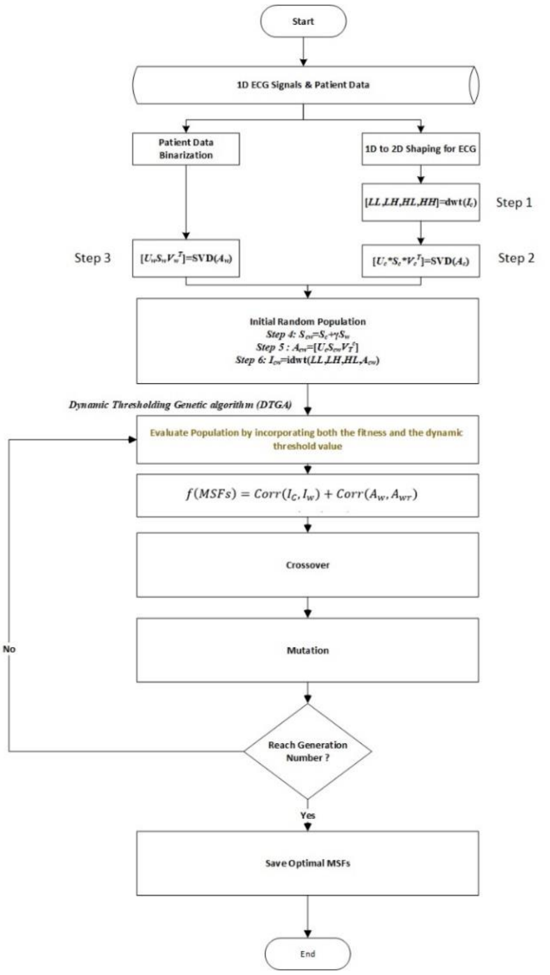
Start
1D ECG Signals & Patient Data
Patient Data Binarization
1D to 2D Shaping for ECG
$[LL,LH,HL,HH]$=dwt(I_c)
Step 1
Step 3
$[U_w S_w V_w^T]$=SVD(A_w)
$[U_c{}^*S_c{}^*V_c^T]$=SVD(A_c)
Step 2
Initial Random Population
Step 4: $S_{cw}=S_c+\gamma S_w$
Step 5 : $A_{cw}=[U_c S_{cw} V_T^c]$
Step 6: I_{cw}=idwt(LL,LH,HL,A_{cw})
Dynamic Thresholding Genetic algorithm (DTGA)
Evaluate Population by incorporating both the fitness and the dynamic threshold value
$f(MSFs) = Corr(I_C, I_w) + Corr(A_w, A_{wr})$
Crossover
Mutation
No
Reach Generation Number ?
Yes
Save Optimal MSFs
End

Fig 1. General process of the proposed approach

3.1- Steganography algorithm description

Important characteristics of an ECG signal include the QRS complex, P, T, and U waves. The QRS complex represents the rapid depolarization of the heart's right and left ventricles. P and T waves represent depolarization and repolarization of the atria and ventricle, respectively. U wave refers to the repolarization of the interventricular septum [27]. These defining markers are integral to defining an ECG signal. The proposed ECG steganography algorithm uses a 2D ECG matrix as a conceal signal. The 1D ECG data is preprocessed in order to generate the 2D ECG image using Pan Tompkin's QRS detection method [27]. Thus, the 1D ECG signal can be reconstructed utilizing these reference points.

DWT is a time-frequency analysis that can be used to analyze an image or signal in multiple frequency bands with variable resolution. This quality can be used to determine the frequency sub-band of a signal with the least significance. The distinctive regions of the ECG signal, such as the QRS complex, P and T waves, are located in the sub-bands of low frequency. Consequently, embedding the watermark in a sub-band with a high frequency is the obvious solution for preserving diagnosability data. The advantage of DWT is that the original signal can be recovered by applying the inverse DWT transform to frequency bands. SVD is a matrix factorization technique used frequently in dimension reduction applications, such as data compression. It is utilized to conceal information in the context of steganography. In 2D ECG steganography [30], singular values (SVs) of the cover image are changed to singular values (SVs) of the concealed data. However, the watermark's size is restricted in this manner. In this study, we plan to employ DWT and SVD as follows:

Step 1: Using discrete wavelet transform (DWT) with the Debauches 4 wavelet, the 128 by 128 pixel 2D ECG cover image (Ic) is broken down into four frequency sub-bands which are LL, LH, HL and HH (Eq.(1)).

$$[LL,LH,HL,HH]=\mathrm{dwt}(I_c) \tag{1}$$

Step 2: Apply SVD using the Eq. (2) to the 67 by 67 coefficient matrix Ac representing the high frequency sub-band HH

$$[U_c{*}S_c{*}V_c^T] = \mathrm{SVD}(A_c) \tag{2}$$

Where SVD function produces a diagonal matrix Sc of the same dimension as Ac, with nonnegative diagonal elements in decreasing order, and unitary matrices Uc and Vc so that Ac = $U_c{*}S_c{*}V_c^T$

Step3: Apply SVD on the watermark Aw of size 67×67 as given in Eq.(3).

$$[U_wS_wV_w^T] = \mathrm{SVD}(A_w) \tag{3}$$

Step 4: Embed the singular values of the watermark (Sw) into the singular values of the cover signal (Sc) using the additive quantization approach, as shown in Eq. (4). Here, γ is the scaling factor.

$$S_{cw}=S_c+\gamma S_w \tag{4}$$

Step 5:, Use the inverse SVD formulated in Eq (2). Reconstruct the high frequency sub-band (HH) modified coefficient matrix Acw (5).

$$A_{cw}=[U_cS_{cw}V_T{}^c] \tag{5}$$

Step 6: Use inverse discrete wavelet transform (DWT) with the HH coefficients adjusted by Acw to generate the watermarked ECG image, as shown in Eq (6)

$$I_{cw}=\mathrm{idwt}(LL,LH,HL,A_{cw}) \tag{6}$$

Step7: Apply 2D to 1D ECG signal conversion method to obtain the 1D watermarked ECG signal.

Watermark extraction algorithm

The embedded watermark can be retrieved using watermark extraction method as follows:

Step 8: Apply DWT to Icw to get [LLcw, LHcw, HLcw, HHcw], which is quite similar to step1.

Step 9: Similarly to Step 2, apply SVD to the coefficient matrix Acw of the high frequency band HHcw to produce the singular values Sc of the watermarked image.

Step 10: Use the formula given in Eq.(7) to evaluate the singular values of the watermark that was recovered from Sc (7)

$$S^*{}_w=(S^*{}_c-S_c)/\gamma \tag{7}$$

Step11: With Uw and Vw from Eq.(3), retrieve the watermark A_w^* using inverse SVD method as given in Eq.(8)

$$A^*{}_w=[U_wS^*{}_wV^T{}_w] \tag{8}$$

3.2 Dynamic Thresholding genetic algorithm (DGTA) for MSFs optimization

In this research work, we propose to use Dynamic Thresholding Genetic Algorithm (DGTA) for optimizing MSFs, which involves evaluating multiple factors at different scales to assess the system performance and select the factors that improve the performance. By dynamically adjusting the threshold values during the optimization process, DGTA can effectively explore the search space and converge towards optimal solutions for MSF optimization.

3.3.1 DTGA principle

In DTGA [36], the binary representation of populations is adopted for minimization problems. The characteristic of the representation is that the bits are utilized to embody the state operator as:

$$q_j^t = [\beta_1^t|\beta_2^t|\dots\dots\dots|\beta_m^t|] \tag{9}$$

q_j^t represents the chromosome of the t-th generation and the j-th individual, and m is the gen β index number. The employing of bit encoding allows one individual to embody the states instantaneously, forcing the DTGA be better in terms of diversity compared to the CGA algorithm. As stated in [31], convergence can also be achieved with the bit statement. β attitudes to 0 or l.

Dynamic thresholding is a technique that can be used to enhance the population diversity and exploration space of a Classical Genetic Algorithm (CGA).

This technique works by setting a threshold for each individual in the population, which is then adjusted dynamically based on the performance of the individual. If an individual performs better than the threshold, then its threshold is increased, allowing it to explore more of the search space. Conversely, if an individual performs worse than its threshold, then its threshold is decreased, limiting its exploration capabilities. By adjusting thresholds dynamically in this way, it is possible to continue allowing individuals to explore various parts of the search space while maintaining a diverse population. The following steps represents the mechanism of dynamic thresholding in genetic algorithm:

1. The dynamic thresholding technique assigns a threshold value to each individual in the population, denoted as T(i), where i represents the index of the individual.
2. The threshold value T(i) is determined by analyzing the performance of the individuals in the population by measuring the fitness value for each individual, typically based on their fitness or correlation coefficient values.
3. If the population is observed to be evolving rapidly, as determined by a correlation coefficient, the threshold value T(i) is increased by increasing the ones genes in population by one to adapt to the changing dynamics of the population.
4. Conversely, if the population is stagnating or the fitness value does not change, the threshold value T(i) is decreased by decreasing the ones genes in population by one to encourage exploration and avoid premature convergence.
5. Solutions from the population are selected for further evaluation and modification based on their fitness or correlation coefficient values relative to the threshold value T(i). Individuals whose performance exceeds or meets the threshold T(i) are considered as potential solutions for further processing.
6. The selected solutions are subject to modification through crossover and mutation genetic operators, to introduce diversity and explore different regions of the search space.
7. The algorithm terminates when the genetic algorithm completes its execution or when a termination criterion is met. The high-quality solutions obtained during the dynamic thresholding process are returned as the final output of the algorithm.

This can lead to improved performance and better solutions being found by the genetic algorithm [36-37]. Algorithm 1 represents the pseudo code of DTGA

Algorithm 1: DTGA

```
Inputs: Dataset T, Number of generations t, Number of individuals j, Initial Populations Pops, and Dynamic thresholding DT
1. While t is less than MAX_GENS, do the following:
2. Increment t by 1
3. Encode Pops using bit_Encoding
4. Evaluate the fitness values of Pops using Fitness_Evaluation
5. Select the best individuals from Pops based on their fitness values using Selection_Best
6.Update Pops using Dynamic_Thresholding_Function(pop)
7. If Termination_Condition is False, then do the following:
    a. For each i from 0 to j-1, do the following:
        i. Perform crossover on Pop to generate a new individual New_Pops(i)
        ii. Perform mutation on New_Pops(i)
    b. End for loop
    c. Set Pops to New_Pops
8. End if statement
9. If Termination_Condition is True, then do the following:
    a. Return Pops
10. End if statement
11. End while loop
12. Best individual is the one in Pops with the highest fitness value.
Dynamic_Thresholding_Function(Pop)
2.    threshold = computeThreshold(Pop)
3.    while geneticAlgorithmIsRunning():
4.        if populationIsEvolvingRapidly():
5.            threshold = increaseThreshold(threshold)
6.        else if populationIsStagnating():
7.            threshold = decreaseThreshold(threshold)
8.            selectedSolutions = selectSolutions(pop, threshold)
```

```
        evaluateSolutions(selectedSolutions)
        modifySolutions(selectedSolutions)
    return highQualitySolutions
```

3.3.2 MSFs optimization using DTGA

In this research work, DTGA is used for multi-scale factor optimization in healthcare data steganography by dynamically adjusting the thresholds of the genetic algorithm to identify the optimal combination of factors that can enhance data security. This paper explores the potential benefits of using DTGA for multi-scale factor optimization in healthcare data steganography and its significance in protecting sensitive healthcare information. The MSFs must be acknowledged in a way that achieves a balance between anonymity and tenacity. The following steps represents the MSFs optimization using DTGA

Initially, a threshold random value between 1 and 20 is assigned to each individual. After that, this threshold value is determined by measuring the fitness value for each individual. The fitness function is depicted by the objective function in Eq. (10)

$$f(MSFs) = Corr(I_C, I_w) + Corr(A_w, A_{wr}) \qquad (10)$$

Where I_C represents a cover ECG signal, and $I_w$represents a watermarked ECG signal. $A_w$is the initial watermark, while $A_{wr}$is the watermark extracted when receiving data. The correlation ($Corr$) value is unitless and fluctuates between [0, 1]. $Corr$ is estimated as shown in Eq (11).

$$Corr(d, d^*) = \frac{\sum_{i=1}^{N}(d_i - \bar{d})(d_i^* - \bar{d})}{\sqrt{\sum_{i=1}^{N}(d_i - \bar{d})}\sqrt{\sum_{i=1}^{N}(d_i^* - \bar{d})}} \qquad (11)$$

where d_i and d_i^* are the original and altered data, respectively. Where $\bar{d}$ is the average of the original data. Higher image correlation indicates greater imperceptibility. A greater correlation between the watermark and the original indicates greater resilience. Consequently, the goal of this optimization problem is to maximize the fitness value $f(MSFs)$.

4. Simulation Results and Analysis

The performance evaluation of ECG steganography is crucial to assess the effectiveness and robustness of the proposed techniques. In this work, we present an overview of various evaluation metrics used to measure the performance of ECG steganography techniques. These metrics include imperceptibility, capacity, robustness, and security. We also discuss their significance in evaluating the performance of ECG steganography techniques and provide insights into their limitations and challenges.

4.1 Evaluation metrics

The suggested ECG steganography approach's efficiency can be measured using measures such as Peak Signal-to-Noise Ratio (PSNR), Peak-to-Residual Ratio(PRD), Kullback-Leibler (KL) divergence, and Bit Error Rate (BER).

PSNR in particular [32], offers the measure of steganography imperceptibility provided in Eq (12). The distance between the cover (d_i) and watermarked (d_i^*) ECG signals is provided by PRD in Eq (13) [33]. The distance between the histograms of Original and watermarked signals is given by KL divergence D in Eq. (14).

$$PSNR = 20log_{10}\left[\frac{\max(d_i)}{\sqrt{\frac{1}{N}\sum_{n=1}^{N}(d_i - d_i^*)^2}}\right]db \qquad (12)$$

$$PRD = \sqrt{\left[\frac{\sum_{i=1}^{N}(d_i - d_i^*)^2}{\sum_{i=1}^{N}(d_i)^2}\right]} * 100 \qquad (13)$$

$$D(p_c, p_w) = \int p_c(d_i)\log\frac{p_w(d_i)}{p_c(d_i)}d_i \qquad (14)$$

N is the signal length, p_c and p_w are the Probability Density Functions (PDF) of the cover and watermarked ECG signals, respectively. Lastly, the error in extracted watermark bits caused by the steganography process can be assessed using the BER formula given in (Eq) (15) [35].

$$BER = \left[\frac{\sum w_{ret}}{\sum w_{org}}\right] * 100 \qquad (15)$$

w_{ret} represents the amount of watermark bits retrieved without mistake, whereas w_{org} represents the total number of original watermark bits

4.2 Simulation setup and Results

A set of experiments is conducted to assess the effectiveness of the proposed approach, and its performance is compared to that of Ant Colony [27] to determine the best multi scale factors. In this study, the CGA and DTGA algorithms are utilized to validate our proposition. The feasibility of the suggested approach is evaluated by utilizing MITIH database [38]. DTGA differs from most other research methodologies in that it generates model populations by evolving random starting model using a genetic algorithm.

The proposed approach is made available as a MATLAB library for use in custom applications. The experiments were conducted on a computer with an Intel(R) Zeon(R) CPU E5430@ 2.66GHz (2 processors), 16GB RAM, and Microsoft Windows 10-64 bit. The results of the simulation clearly demonstrate the effectiveness of the proposed method in identifying the most optimal MSFs. Table 1 represents the used parameters belongs to the simulation setup.

Table 1. Genetic Algorithm Parameters

Parameter	Default Values

Population size	[5,10,15,…..65]
Generation Number	[5 or 10]
Crossover Ratio	0.5
Mutation Ratio	0.5
Threshold	18

Table 2 effectively illustrates the differences between the outcomes of CGA, DTGA, and the Classical Ant Colony Optimization (CACO) approach [32], all tested on the same dataset with a watermark size of 3KB. The results indicate that both CGA and DTGA outperform CACO, with DTGA showing superior performance and numerous advantages over CGA. This investigation makes use of normal ECG signals from the MITBIH normal sinus rhythm database [28] [29]. The frequency of sampling is 128 Hz, and the gain is 200.

Table 2. Performance Comparison between DTGA, CGA & CACO based ECG steganography.

Method	Watermark size	PSNR (db)	PRD	KL distance	BER (%)
DTGA	3 Kb	60.417	0.203	0.213	0
CGA		59.741	0.199	0.194	0
CACO[32]		34.46	0.06	2.04	0

Table 2 compares the efficacy of three distinct ECG steganography techniques: DTGA, CGA, and CACO. The table contains the watermark size, PSNR, PRD, KL distance, and BER metric values for each method. In terms of PSNR and PRD, the results indicate that DTGA outperforms both CGA and CACO. CGA yielded a PSNR of 59.7417 dB and a PRD of 0.199733, whereas DTGA yielded a PSNR of 60.4017 dB and a PRD of 0.203032. CACO obtained a significantly lower PSNR of 34.46 dB and a higher PRD of 0.06. The results indicate that DTGA is a more efficient method for ECG steganography than CGA and CACO. Table 2 clearly demonstrates that the proposed DTGA and CGA algorithms outperformed the CACO algorithm. One possible explanation for these results is that DTGA and CGA are better suited for solving MSFs extraction problems. DTGA generates a diverse range of solutions with unlimited search ability based on different GA parameters such as selection, crossover, and mutation. This diversity is often associated with an objective function that can produce optimal populations (MSFs). On the other hand, CACO optimization quality is often limited by factors such as architecture complexity, generalization ability, noise-tolerant ability, and limited search-ability. [32]. Fig. 2 shows 2 samples of 1D cover and watermarked ECG signal extracted from the proposed application.

The effectiveness of watermarking is demonstrated in Figure 2, where multiple 1D cover and watermarked ECG signals are presented. Despite minimal signal deterioration, the signals are indistinguishable, except for the ECG signal that contains the watermark with the highest capacity, highlighting the effectiveness of watermarking.

Table 3 presents the experimental results of DTGA (Differential Evolutionary Algorithm) and CGA (Conventional Genetic Algorithm) based ECG (Electrocardiogram) steganography on a testing subset comprising 20% of the ECG Data Set. The experiments were conducted with a mutation ratio of 0.5, crossover ratio of 0.5, threshold of 18, and sampling frequency of 200. The table includes the performance metrics PSNR (Peak Signal-to-Noise Ratio), PRD (Percentage Residual Difference), and KL_D (Kullback-Leibler Divergence) for both DTGA and CGA. The results are organized by generation numbers (GN) and population size (PS). It can be observed that the PSNR values range from 55.83 to 60.41 for DTGA and from 31.3592 to 59.7417 for CGA. The PRD values vary from 0.203032 to 0.329907 for DTGA and from 0.199733 to 0.589471 for CGA. Additionally, the KL_D values range from 0.19456 to 0.76945 for CGA and from 0.19944 to 0.3954 for DTGA. These results provide insights into the performance of both algorithms in terms of their ability to embed and extract hidden information within ECG signals.

Table 4 presents the comparative results between the best outcomes obtained by using two different algorithms, namely CGA and DTGA. The results show that CGA outperformed DTGA in terms of population size, with a population size of 55 compared to DTGA's 10. However, both algorithms had the same number of generation numbers, with 10 generations each. CGA also had a slightly better best fitness value of 0.028 compared to DTGA's 0.022, but DTGA had a higher PSNR value of 60.417 compared to CGA's 59.7417. The total populations used in CGA and DTGA were 550 and 100 respectively. Finally, the time taken to complete the optimization process was significantly shorter for DTGA, with a time of 41.3 seconds compared to CGA's 228 seconds. Overall, the results indicate that both algorithms have their strengths and weaknesses, and the choice of algorithm depends on the specific optimization goals and constraints.

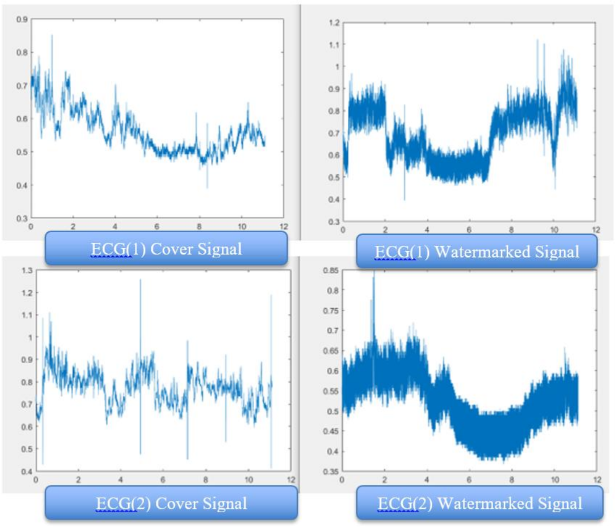

Fig. 2. Samples of 1D cover and watermarked ECG signal.

Table 3. Performance of DTGA & CGA based ECG steganography on Testing 20% from ECG Data Set when Mutation Ratio=0.5, Crossover Ratio =0.5, Threshold =18, and Sampling Frequency=200. GN stands for generation numbers and PS stands for population size

		DTGA based ECG steganography			CGA based ECG steganography		
GN	PS	PSNR	PRD	KL_D	PSNR	PRD	KL_D
5	25	55.83	0.329	0.290	52.484	0.589	0.244
5	50	59.60	0.226	0.2975	31.359	0.232	0.769
5	55	59.95	0.279	0.289	54.943	0.350	0.245
5	65	59.67	0.281	0.267	57.087	0.255	0.203
10	5	57.75	0.234	0.256	56.325	0.306	0.395
10	10	60.41	0.203	0.213	50.493	0.550	0.265
10	15	58.52	0.271	0.199	53.889	0.398	0.320
10	35	58.71	0.323	0.346	58.191	0.237	0.302
10	50	56.91	0.263	0.365	56.440	0.286	0.229
10	55	60.20	0.281	0.287	59.741	0.199	0.194

Table 4. Comparative results between best results between CGA & DTGA

	CGA	DTGA
Population size	55	10
Generation Numbers	10	10
PSNR	59.7417	60.417
Total Populations	550	100
Time Seconds	228	41.3

5 Conclusion

This research aimed to improve the security of patient data during Internet transmission by introducing new techniques based on Electrocardiogram (ECG) signals using CGA and DTGA. Unlike conventional training methods, the effectiveness of DTGA in optimizing MSFs is founded on the utilization of dynamic thresholding to capitalize on the randomness of binary chromosomes represented by bits. According to the experimental findings, the DTGA-optimized model provides a more precise optimization than the CGA-optimized model, which is optimized according to a specific specification. Because the model configuration is not predetermined in DTGA, the solution space is larger. The model configuration is instead determined by the evolutionary mechanism with probabilities derived from the bit overlay using dynamic thresholding. DTGA outperforms CGA, as the MSFs extraction procedure in DTGA required approximately 81% less time than in CGA. By combining the CGA and dynamic thresholding methods, we enhanced the ECG steganography procedure's accuracy. According to the results, our proposed methodologies outperform the CACO method. Future research could investigate the application of these methods to the transmission of ECG data in real-time and their resistance to various assaults.

References

[1] Al Ameen, M., Liu, J. and Kwak, K., 2012. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, *36*(1), pp.93-101.

[2] AbdelMouty, A.M., Abdel-Monem, A., Aal, S.I.A. and Ismail, M.M., 2023. Analysis the Role of the Internet of Things and Industry 4.0 in Healthcare Supply Chain Using Neutrosophic Sets. *Neutrosophic Systems with Applications*, *4*, pp.33-42.

[3] Podilchuk, C.I. and Delp, E.J., 2001. Digital watermarking: algorithms and applications. *IEEE signal processing Magazine*, *18*(4), pp.33-46.

[4] Shih, F.Y., 2017. *Digital watermarking and steganography: fundamentals and techniques*. CRC press.

[5] Abdelhafeez, A., Mohamed, H.K. and Khalil, N.A., 2023. Rank and Analysis Several Solutions of

Healthcare Waste to Achieve Cost Effectiveness and Sustainability Using Neutrosophic MCDM Model. *Neutrosophic Systems with Applications*, *2*, pp.25-37.

[6] Ziou, D. and Jafari, R., 2014. Efficient steganalysis of images: learning is good for anticipation. *Pattern Analysis and Applications*, *17*(2), pp.279-289.

[7] Zielińska, E., Mazurczyk, W. and Szczypiorski, K., 2014. Trends in steganography. *Communications of the ACM*, *57*(3), pp.86-95.

[8] Ibaida, A. and Khalil, I., 2013. Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. *IEEE Transactions on biomedical engineering*, *60*(12), pp.3322-3330.

[9] Chen, S.T., Guo, Y.J., Huang, H.N., Kung, W.M., Tseng, K.K. and Tu, S.Y., 2014. Hiding patients confidential datainthe ECG signal viaa transform-domain quantization scheme. *Journal of medical systems*, *38*(6), pp.1-8.

[10] Edward Jero, S., Ramu, P. and Ramakrishnan, S., 2014. Discrete wavelet transform and singular value decomposition based ECG steganography for secured patient information transmission. *Journal of medical systems*, *38*(10), pp.1-11.

[11] Giakoumaki, A., Pavlopoulos, S. and Koutsouris, D., 2006. Secure and efficient health data management through multiple watermarking on medical images. *Medical and Biological Engineering and Computing*, *44*(8), pp.619-631.

[12] Lei, B., Tan, E.L., Chen, S., Ni, D., Wang, T. and Lei, H., 2014. Reversible watermarking scheme for medical image based on differential evolution. *Expert Systems with Applications*, *41*(7), pp.3178-3188.

[13] Raúl, R.C., Claudia, F.U. and Trinidad-BIas, G.D.J., 2007, February. Data hiding scheme for medical images. In *17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07)*.

[14] Ginsberg, J., Mohebbi, M.H., Patel, R.S., Brammer, L., Smolinski, M.S. and Brilliant, L., 2009. Detecting influenza epidemics using search engine query data. *Nature*, *457*(7232), pp.1012-1014.

[15] Kim, H.J., Lee, H., Kim, Y.K. and Chang, J.W., 2022. Privacy-preserving k NN query processing algorithms via secure two-party computation over encrypted database in cloud computing. *The Journal of Supercomputing*, *78*(7), pp.9245-9284.

[16] Liu, P. and Zhang, W., 2022, July. Towards practical privacy-preserving solution for outsourced neural network inference. In *2022 IEEE 15th International Conference on Cloud Computing (CLOUD)* (pp. 357-362). IEEE.

[17] Doan, K., Quang, M.N. and Le, B., 2017, December. Applied cuckoo algorithm for association rule hiding problem. In *Proceedings of the Eighth International Symposium on Information and Communication Technology* (pp. 26-33).

[18] Dorigo, M. and Gambardella, L.M., 1997. Ant colony system: a cooperative learning approach to the traveling salesman problem. *IEEE Transactions on evolutionary computation*, *1*(1), pp.53-66.

[19] Mishra, A., Agarwal, C., Sharma, A. and Bedi, P., 2014. Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. *Expert Systems with Applications*, *41*(17), pp.7858-7867.

[20] Run, R.S., Horng, S.J., Lai, J.L., Kao, T.W. and Chen, R.J., 2012. An improved SVD-based watermarking technique for copyright protection. *Expert Systems with applications*, *39*(1), pp.673-689.

[21] Mishra, A., Agarwal, C., Sharma, A. and Bedi, P., 2014. Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. *Expert Systems with Applications*, *41*(17), pp.7858-7867.

[22] Ali, M. and Ahn, C.W., 2014. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal processing*, *94*, pp.545-556.

[23] Bath, P.A., 2004. Data mining in health and medical information. *Annu. Rev. Inf. Sci. Technol.*, *38*(1), pp.331-369.

[24] Jothi, N. and Husain, W., 2015. Data mining in healthcare–a review. *Procedia computer science*, *72*, pp.306-313.

[25] Kim, J.C. and Chung, K., 2019. Associative feature information extraction using text mining from health big data. *Wireless Personal Communications*, *105*, pp.691-707.

[26] Loukhaoukha, K., Chouinard, J.Y. and Taieb, M.H., 2011. Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization. *J. Inf. Hiding Multim. Signal Process.*, *2*(4), pp.303-319.

[27] Liao, T., Socha, K., de Oca, M.A.M., Stützle, T. and Dorigo, M., 2013. Ant colony optimization for mixed-variable optimization problems. *IEEE Transactions on Evolutionary Computation*, *18*(4), pp.503-518.

[28] Goldberger, A.L., Amaral, L.A., Glass, L., Hausdorff, J.M., Ivanov, P.C., Mark, R.G., Mietus, J.E., Moody, G.B., Peng, C.K. and Stanley, H.E., 2000. PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. *circulation*, *101*(23), pp.e215-e220.

[29] Moody, G.B. and Mark, R.G., 1990, September. The MIT-BIH arrhythmia database on CD-ROM and software for use with it. In *[1990] Proceedings Computers in Cardiology* (pp. 185-188). IEEE.

[30] Edward Jero, S., Ramu, P. and Ramakrishnan, S., 2014. Discrete wavelet transform and singular value

decomposition based ECG steganography for secured patient information transmission. *Journal of medical systems*, *38*(10), pp.1-11.

[31] Darwish, S.M., Shendi, T.A. and Younes, A., 2019. Chemometrics approach for the prediction of chemical compounds' toxicity degree based on quantum inspired optimization with applications in drug discovery. *Chemometrics and Intelligent Laboratory Systems*, *193*, p.103826.

[32] Ramu, P. and Swaminathan, R., 2016. Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. *Expert Systems with Applications*, *49*, pp.123-135.

[33] Ibaida, A. and Khalil, I., 2013. Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. *IEEE Transactions on biomedical engineering*, *60*(12), pp.3322-3330.

[34] Trobisch, P.D., Bauman, M., Weise, K., Stuby, F. and Hak, D.J., 2010. Histologic analysis of ruptured quadriceps tendons. *Knee Surgery, Sports Traumatology, Arthroscopy*, *18,* pp.85-88.

[35] Kojima, T., Ohtani, N., Matsumoto, T. and Parampalli, U., 2011, October. On multiple information embedding by digital watermarking based on complete complementary codes. In *Proceedings of the Fifth International Workshop on Signal Design and Its Applications in Communications* (pp. 100-103). IEEE.

[36] Zhang, Q., Xu, X. and Liang, Y.C., 2006. An improved artificial immune algorithm with a dynamic threshold. *Journal of Bionic Engineering*, *3*(2), pp.93-97.

[37] Dasgupta, D. ed., 2012. *Artificial immune systems and their applications*. Springer Science & Business Media.

[38] https://physionet.org/content/mitdb/1.0.0/

[39] Pasha, M. J. ., Rao, C. R. S. ., Geetha, A. ., Fernandez, T. F. ., & Bhargavi, Y. K. . (2023). A VOS analysis of LSTM Learners Classification for Recommendation System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 179–187. https://doi.org/10.17762/ijritcc.v11i2s.6043

[40] Muñoz, S., Hernandez, M., González, M., Thomas, P., & Anderson, C. Enhancing Engineering Education with Intelligent Tutoring Systems using Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/116

[41] Venu, S., Kotti, J., Pankajam, A., Dhabliya, D., Rao, G. N., Bansal, R., . . . Sammy, F. (2022). Secure big data processing in multihoming networks with AI-enabled IoT. Wireless

[42] Communications and Mobile Computing, 2022 doi:10.1155/2022/3893875