

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/320687747>

An Improved Robust Image Watermarking Scheme Based on the Singular Value Decomposition and Genetic Algorithm

Conference Paper · October 2017

DOI: 10.1007/978-3-319-70010-6_65

CITATIONS

2

READS

108

3 authors:



Atheer Bassel

Universiti Kebangsaan Malaysia

10 PUBLICATIONS 19 CITATIONS

[SEE PROFILE](#)



Md Jan Nordin

Universiti Kebangsaan Malaysia

130 PUBLICATIONS 1,152 CITATIONS

[SEE PROFILE](#)



Mohammed Basil Abdulkareem

Al-Maarif University

2 PUBLICATIONS 4 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Multidimensional Forensics Facial Identification System for Video Forensics Application [View project](#)



Continuous sign language Recognition [View project](#)

An improved robust image watermarking scheme based on the singular value decomposition and genetic algorithm

Atheer Bassel ⁽¹⁾, Md Jan Nordin ⁽²⁾, Mohammed B. Abdulkareem ⁽³⁾

^(1,2) Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia 43600 Bangi, Selangor Darul Ehsan, Malaysia.

⁽¹⁾ Computer college, University of Anbar, Al Anbar, Iraq

⁽³⁾ Department of Computer engineering and technology, Almaaref University college. Al Anbar, Iraq

atheerbassel@siswa.ukm.edu.my, jan@ukm.edu.my, f_com22@yahoo.com

*: corresponding author, phone: +601139301106

Abstract:

This paper propose a robust image watermarking scheme based on the singular value decomposition (SVD) and genetic algorithm (GA). SVD based watermarking techniques suffer with an issue of false positive problem. This leads to even authentication the wrong owner. Prevention of false positive errors is a major challenge for ownership identification and proof of ownership application using digital watermarking. We employed GA algorithm to optimize the watermarked image quality (robustness) of the extracted watermarks. The former can be overcome by embedding the owner's components of the watermark into the host image, the latter is dependent on how much the quantity for the scaling factor of the principle components is embedded. To improve the quality of watermarking (robustness), GA is used for optimize the suitable scaling factor. Experimental result of the proposed technique proves the watermark image ownership and can be reliably identified even after severe attacks. The comparison of the proposed technique with the state of the art show the superiority of our proposed technique where it is outperforming the methods in comparison.

Keywords: Digital watermarking, singular value decomposition (SVD), genetic algorithm (GA), false positive problem.

1. Introduction

The definitions of digital watermarking emerge while trying to overcome the limitations of encryption and steganography in the enforcement and protection of intellectual property rights (I. Cox, Kilian, Leighton, & Shamoan, 1996; I. J. Cox, Kilian, Leighton, & Shamoan, 1997).

Compared to the idea of encryption, the watermark information is inserted into its original form and does not hinder users in listening to, viewing, watching, or manipulating the content. Unlike steganography, digital watermarking technologies are to establish the identity of information to avoid the unauthorized embezzlement. Generally, additional information is embedded directly into the original multimedia or host signal which is useful and valuable, and the message itself is necessary to be secret.

The two alternatives for the addition of a watermark to a digital image are the visible mark and the imperceptible mark. Visible watermarks impact an image in terms of its commercial. However, this thesis will consider this option. An example of visible watermark can be found in company logos. On the other hand, the imperceptible marks comprise the side information placed imperceptibly, typically alongside certain perceptual model. The imperceptible mark can be added either with or without the host image partition into blocks. This enables the embedding of more than one bit. In addition, within the spatial domain, the encoding is performable through direct change of pixel values. The transform domain maps image to other domain. Then, the domain's coefficients are changed to become Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) as well as Singular Value Decomposition (SVD). According to Lu (2004), the method of transform domain appears more robust against diverse types of attacks as opposed to the spatial domain.

With digital watermarking, image-related data are covertly embeddable via the manipulation of pixel values. However, this process is bound by a trade-off between the robustness against operations of image processing (attacks) and image quality. Considering that it is covert and comprises pixel values' manipulation, a watermark offers a way for enforcing certain image's integrity and authenticity. Generally, a robust watermark which can resist attacks is used for enforcing authenticity. Meanwhile, a fragile watermark that is easily destroyable by attacks is used for the detection of tampering; this enforces integrity. Within the watermarking community, there is a challenging issue associated to watermarking, that is, the issue of security. For the majority of watermarking systems available today, the processes of embedding and extraction are conducted on the plain media. Hence, it is compulsory that the watermark embedder is the owner of the original media or a trustworthy third party. This prevents the risk of the plain media being exposed. The processing conducted in the encrypted domain should not

cause worry to the media owner. In relation to this, Guo, Zheng and Huang (2015) mentioned that signal processing in the encrypted domain also termed as secure signal processing, offers a potential solution to this problem.

There are a lot of researchers who implemented SVD of watermark, especially during the embedding phase, and the watermark is in the host image (Emami & Omar, 2013; Run, Horng, Lai, Kao, & Chen, 2012). However, embedding via SVD can easily fail. Further, any reference watermark that is being explored for in an arbitrary image is easily discoverable by attackers. This strategy has led to the problem of false positive, when certain watermark was embedded. Here, the attacker can easily attest the ownership of the arbitrary watermarked image with no awareness of the initial watermark embedded in the host image. Therefore, the false positive rate for this application should be approximately zero and that proof of ownership cannot otherwise be reliable.

Another problem in ownership identification occurs in a situation where only scalar value of the scaling factor is employed in this trustworthy SVD- based image watermarking (Run et al., 2012). Employing the small value for scaling factor, the watermark's invisibility attained high peak signal to noise ratio (PSNR) of the watermarked image. However, the watermarked image is not as robust when there are some common attacks. The factor of scaling highly contributes to the control of the watermark images in terms of transparency and robustness (Jain, Arora, & Panigrahi, 2008). It is worth mentioning that high scaling factor causes the quality of watermarked image to be unacceptable, and yet the watermark is robust (Run et al., 2012).

In addition, this work will provide more information for the false positive, false negative and scaling factor. The drawback for defining the false positive and false negative should be taken into account; the false position means false watermark detection while false negative denotes failure in detecting the already available watermark. In this work, a simple model is employed to enable an analysis for the estimation of the distribution of probability of false positive as well as false negative for the technique proposed. In short, correlation coefficient (NC) is to be employed in order to ascertain the degree of the similarity between the original and extracted watermark image. The problem of false positive emerges in nearly all the SVD-based algorithms caused by the fact that there is only the process of embedding watermark into the original image.

The scaling factor is very important applying with optimization because a decrease in the scale factor value during the optimization process can generate high quality final outcome (Weber et al., 2011). The scaling factor in the proposed watermarking scheme employs control on the tradeoff between the imperceptibility and robustness.

In addition, there are some advantages and disadvantages of both spatial domain and frequency domain (transform domain). Table 1 shows the comparison between them and the advantages and disadvantages for both.

Table 1: Differentiation between special and transform domains

#	Domain	Advantages	Disadvantages
1	Spatial Domain	High embedding capability Short computational time High controllable imperceptibility	Susceptible to geometric attacks
2	Transform Domain	Robustness against attacks including Geometric attacks and compression	High computational time Restricted embedding capacity Lower controllable imperceptibility

Thus, based on the above, this work aims to:

1. Propose a GA for the embedding part of our process to make the system more robust.
2. Propose how the GA can define the chromosome (the population) and define the fitness function (objective) based on watermarking evaluation under the number of maximum iteration.
3. Evaluation and comparison with state of the art methods.

The rest of this paper is organized as follows. Section 2 introduces the review of algorithms for image watermarking in the transform domain involved in this paper. Section 3 describes the proposed method. Section 4 presents the experimental results and discussion. Finally, section 5 gives the conclusion.

2. Review of Algorithms for Image Watermarking in the Transform Domain

One implicit way of concealing watermarks in the host image is via the transformation of the image from the spatial domain to the transform domain and the embedding of the watermarks through the modification of the coefficients of the transformed image. A general block diagram of these types of watermarking is illustrated in Figure 3. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular value Decomposition (SVD) and Integer Wavelet Transform (IWT), are among the most popular transforms. The aim of concealing information in the transform domain is for attaining sounder performance in comparison with the spatial domain methods particularly with respect to robustness, invisibility, and detection complexity (Lee, Kim, Kwon, & Lee, 2005; L.-d. LI, GUO, & Lei, 2008; L. Li, Qian, & Pan, 2011; Memon, 2010; Shih & Wu, 2003; Thabit & Khoo, 2014).

2.1 Singular Value Decomposition (SVD)

Singular value decomposition comprises a linear algebra technique for symmetric matrix diagonalization. A digital image is also a matrix of integer numbers. As such, SVD is performable on digital images right away. The techniques of traditional transform including DFT, DCT and DWT just decompose a signal with respect to a standard basis set. In some sense, this is not an optimal representation. The attractive properties and unique features of SVD includes its stability with little disturbance. This is why SVD has been employed in numerous applications of signal processing. SVD is also a type of orthogonal transform and a numerical technique to diagonalize matrix, and thus, it can be used as a technique for linear algebraic within the transformed domain which contain foundation states, which, in some sense, are optimal. SVD decomposes a specified matrix into three portions such as left singular matrix U , right singular matrix V and singular matrix S , on an image size A with size $(M \times N)$. The expression is as the following (Lentilucci & Emmett, 2003).

$$A=USV^T \quad (1)$$

The matrix S comprises just the diagonal element and it is termed as singular values. The matrix S contains the singular values in downward order. Meanwhile, the matrix U and V comprise the image's decomposed and detailed information. Provide that A represents the rectangular matrix of the order $(n \times n)$. Thus, matrix S is allowed to contain maximum n diagonal elements. In

generally, these elements (S) symbolize the involvement of each layer of decomposed image in the final formation of image (Tian, 2003). The parent matrix (A) is reproducible with the smaller elements of matrix s but this reproduction of matrix A* will reduce the quality.

$$A = USV^T = \begin{pmatrix} u_{1,1} & \dots & u_{1,M} \\ \vdots & \ddots & \vdots \\ u_{M,1} & \dots & u_{M,M} \end{pmatrix} \times \begin{pmatrix} s_{1,1} & \dots & \mathbf{0} \\ \vdots & \ddots & \vdots \\ \mathbf{0} & \dots & s_{M,N} \end{pmatrix} \times \begin{pmatrix} v_{1,1} & \dots & v_{1,N} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \dots & v_{N,N} \end{pmatrix}^T = \sum_{i=1}^m \sum_{j=1}^n \sum_{k=1}^n u_{i,k} \times s_{k,k} \times v_{k,j} \quad (2)$$

Where: **U** denotes a (M × M) matrix, **V** denotes a (N × N) matrix and **S** denotes a (M × N) diagonal matrix with positive elements from the first to ending row in downward order. The diagonal elements of **S** are termed **SVs** of **A**, which are nonnegative and they are presumed to be downwardly organized. This fulfils the relation equation (2) where *r* denotes the matrix rank.

$$s_{1,1} \geq s_{2,2} \geq \dots \geq s_{r,r} \geq s_{r+1,r+1} = s_{r+2,r+2} \dots = s_{M,N} = \mathbf{0} \quad (3)$$

In watermarking that is grounded on SVD, a signal is treatable as a matrix and decomposed into three matrices. The SVD computation involves the discovery of the eigenvalues and eigenvectors of **AA^T** and **A^TA**. The eigenvectors of **A^TA** consist of the columns of matrix **V** and the eigenvectors of **AA^T** consist of the columns of matrix **U**.

Over the years, several algorithms such as genetic algorithm (GA), ant colony optimization (ACO), particle swarm optimization (PSO), bee algorithm (BA), firefly algorithm (FA), differential evolution (DE), as well as cuckoo search (CS) have been proposed to address tough engineering optimization problems. These proposed algorithms are considered as optimization algorithms that are effective in the solution of complicated problems in the digital image watermarking usage (Waleed, Jun, Abbas, Hameed, & Hatem, 2014). The usage of Nature Inspired Algorithm when using the digital image watermarking optimization has assisted in the challenging task of locating the optimal position and desirable parameters of watermark embedding (Mishra, Agarwal, Sharma, & Bedi, 2014).

In recent time, the digital watermarking techniques have been optimized to gain high quality of embedding and extracting operations. Particularly, meta-heuristic algorithms, namely, genetic algorithm, particle swarm optimization, firefly algorithm and differential evolution have been developed to perform the task of improving watermarking techniques (Mishra et al., 2014). Meanwhile, Run et al. (2012) and Wang, Lin and Yang (2011) proposed PSO algorithm to gain

the scaling factors and threshold respectively, in the watermark embedding operation. On the other hand, firefly has been implemented for watermarking by Mishra et al. (2014) for discovering the optimal values of the multiple scaling factors in the process of embedding. In the context of swarm optimization, Ali, Ahn, Pant and Siarry (2015) presented Artificial Bee Colony algorithm for watermarking process to attain the optimal threshold and parameters of compensation.

The still prevalent question is: How can these works be securely transferred and sent to the authorized parties only? Despite the fact that there are countless algorithms being applied to solve digital image watermarking problem, none of these can provide a comprehensive solution. In other words, different algorithms work well over different attacks (Gharghory, 2011; Waleed et al., 2014). Consequently, this work attempts to suggest a natural inspired meta-heuristic that is hopefully robust when used against resynchronization attacks such as rotation, nosing, filtering, cropping as well as dithering.

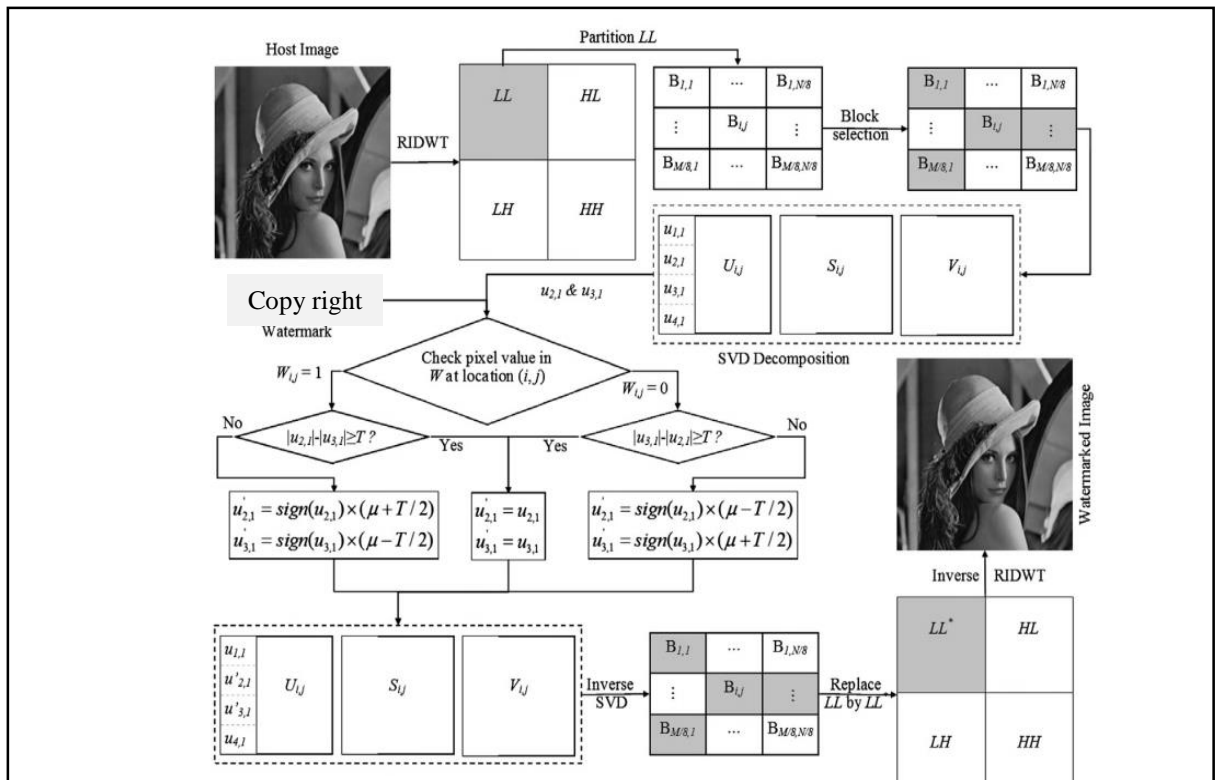


Figure 1: Embedding watermarking by SVD

2.2 Attack

It is possible for the copyrighted material to receive conceivable attacks from adversaries. These attacks could distort, tamper or eliminate the watermark from it. A process that causes distortion to the media watermark is considered as a watermark attack.

Dharwadkar and Amberker (2010) describe an attack as an attempt to obtain unapproved access to a network's or a system's services, resources, or information, or an attempt to compromise a network or a system in terms of its integrity, availability, or confidentiality. Owners of network or system can use practices and technologies that are competent in improving resistance to attacks or that could prevent attacks from interrupting communications or operations, or from compromising or damaging information.

Watermarks in digital images are useful for the purpose of ownership protection. A proposed method is employed so that the watermark can be sustained although changes (attacks) have been made on the watermarked image. Diverse types of attacks will be used. These include Gaussian noise, Image Cropping, Image Rotation, Dithering, Compression, Gaussian filter and Median filter, to prove the robustness watermarking.

2.3 Genetic Algorithm (GA)

Genetic Algorithm (GA) is a population based meta-heuristic which impersonates the process of natural evolution (Holland, 1975). GA handles a population of individuals and each individual represents a potential solution. GA is a multipath algorithm that performs parallel searches in order to reduce the trapping in the local minima. GA works with a coding of parameters (chromosomes) that help in evolving the present state into the succeeding state with the smallest amount of calculations.

One *chromosome (individual)* represents one candidate solution. A *gene* represents a subsection of one chromosome that encodes the values of the shift patterns for one nurse. In order to guide the search, GA uses the fitness of each string. The search for an optimal solution typically begins with a set of individuals that are randomly produced, termed as *initial population*. Then, GA develops the population by applying three operators: (i) selection, (ii) crossover, and (iii) mutation to generate new individuals called offspring. At the end of each

iteration, a new generation is created. This process keeps repeating until it reaches the termination criteria. Algorithm (1) shows the pseudo-code of basic GA.

Algorithm (1): Genetic Algorithm (GA)

Begin

Population := generate initial solutions;

Repeat the following until stopping criterion

Select two parents

Apply genetic operators (crossover and mutation)

Update population

End

End;

Shieh et al. (2004) proposed an innovative watermarking scheme based on GA. It is robust against watermarking attacks and the watermarked image quality is also considered. The robustness of the proposed algorithm improved the watermarked image quality with GA. The simulation results for both the watermarked image quality and the correlation values of the extracted watermark after certain attacks was poor.

Zhicheng et al. (2006) proposed the optimal watermarking embedding positions using GA to examine the correlation between the robustness and the quality of the digital image. It is a new approach to find the near optimal positions for embedding an authentication by GA.

Ali Al-Haj et al. (2008) introduced algorithms on optimized DWT-based image watermarking that can simultaneously offer perceptual transparency and robustness owing to the fact that these two watermarking requirements are contradictory, the DWT-based image watermarking problem as an optimization problem and its solution is via GA. In addition, an imperceptible and robust digital image watermarking system is described according to a combination of DWT.

Lai chih (2011) introduced a technique of image watermarking according to SVD and Tiny-GA. The cover image SVD are modified to allow the embedding of the watermark. The Tiny-GA makes available the systematic consideration on the improvements of the factor of scaling so that the embedded watermark can be controlled in terms of strength. This proposed system allows the

successful survival of embedded watermark following the attacks by image-processing operations.

P. Surekha and S. Sumathi (2011) proposed a new optimization method for digital images in the DWT domain based on GA algorithm. The watermark amplification factor is optimized and the quality of the watermarked images for a set of images is found to be good PSNR and correlation factor after different types of attacks.

3. The proposed Method

This section illustrates the steps of the proposed scheme. The DWT-SVD with GA has been used in different application and performance of the DWT-SVD scheme and GA demonstrated better performance as opposed to the methods used in the past in each specific application. The GA algorithm searches its population to obtain the best solution with all the potential combinations of the DWT-SVD sub-bands and factors of watermark amplification. It is important that the watermark strength or the amplification factor is optimized because this will improve the robustness of the algorithm against attacks. In the proposed the GA with watermarking, firstly, we deal with the scenario as set of solution in one population as optimization problem. Secondly, we calculate the fitness for each solution in my fitness including the image, watermark, attack image, extracted watermark and input parameter for DWT-SVD and GA. Finally, we compute the correlation between the original and extract watermark and the Peak signal to noise rate (PSNR), between the original image and after embedding image.

The procedure of the proposed technique as following, first, our technique finds the best solution in the population based on the objective function. Second, the algorithm will start the optimization process based on the GA procedure and update the population by adding the best solution obtained and delete the worst solution in the population. Finally, process will have terminated when stopping criteria meet. Figure 2 shows the solution.

Best X	L best								Best
1									

Figure 2: Solution representation

Where, the Best X, refers to the index of the solution in population, L best represent the length of the solution and Best represent the best fitness for each solution.

The size for image was 512×512 , the size of watermark image was 20×50 , and this study searching for the best size of watermarking image (32 bit).

Figure 3 shows the embedding and extracting watermarking by using SVD different sub-bands. In this work, the second sub-band is employed for embedding and extraction watermarking.

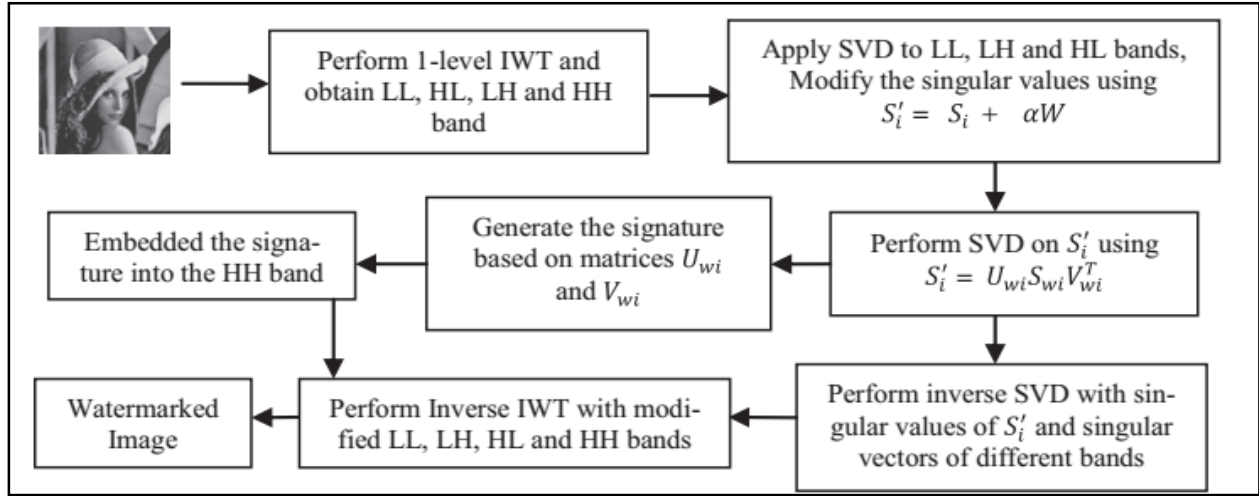


Figure 3: Embedding and extract watermarking using SVD different sub-band

The proposed scheme is as elucidated below:

3.1. Watermarking Embedding

Figure 3 presents the block diagram of the watermarking embedding of the DWT-SVD with GA scheme. SVD divide the image into three matrixes as U, S, and V. The Haar technique is used in DWT. The $w = (w_{11}, \dots, w_{ij}, \dots, w_{nl} \times n_k)$ denotes a watermark and each bit $w_{ij} \in \{-1, 1\}$, in this case, the length of solution was $\{-1, 0, 1\}$ in the population of GA. Subsequently, a watermark bit w_{ij} is embedded in LL_{ij} . These steps show how embedding is done without the GA algorithm optimization.

Step 1: Apply 2 level DWT utilizing the Haar technique, on the original image I to attain LL2 sub-band of size $m \times m$.

Step 2: Apply SVD on LL2 sub-band coefficients of the original image attained in step1 by:

$$[U, S, V] = \text{SVD}(\text{LL2}) \quad (4)$$

Step 3: Apply SVD on the watermark (W) by using

$$[U_w, S_w, V_w] = \text{SVD}(W) \quad (5)$$

Step 4: Embed S_w in to S values using

$$S' = S + \delta * S_w \quad (6)$$

Where δ is the scaling factor that imposes control over the tradeoff between imperceptibility and the watermarking's robustness.

Step 5: Calculate the LL2 sub-band coefficients utilizing

$$\text{LL2}' = U * S' * V^T \quad (7)$$

3.2. Watermarking Extraction

Watermark extraction is denoted by inverse watermark w' . The extraction is performed using DWT-SVD combination again to signed images.

Step1: Apply 2 level DWT using HAAR technique on the original image I and signed image I' (watermark + image) to attain LL2 and $\text{LL2}'$ sub-band coefficients.

Step2: Apply SVD on the LL2 and $\text{LL2}'$ sub-band coefficients utilizing

$$[U, S, V] = \text{SVD}(\text{LL2}) \quad (8)$$

$$[U', S', V'] = \text{SVD}(\text{LL2}') \quad (9)$$

Step3: Calculate the singular values of watermark utilizing

$$S'_w = (S' - S) / \delta \quad (10)$$

Step4: Recover the extracted watermark image utilizing

$$S' = S + \delta * W \quad (11)$$

$$W = U_w * S'_w * V_w^T \quad (12)$$

In Figure 4, we explain how the GA implementation in the embedding and extraction watermarking. GA helps building the system robustness under types of attacks and improves the ownership image.

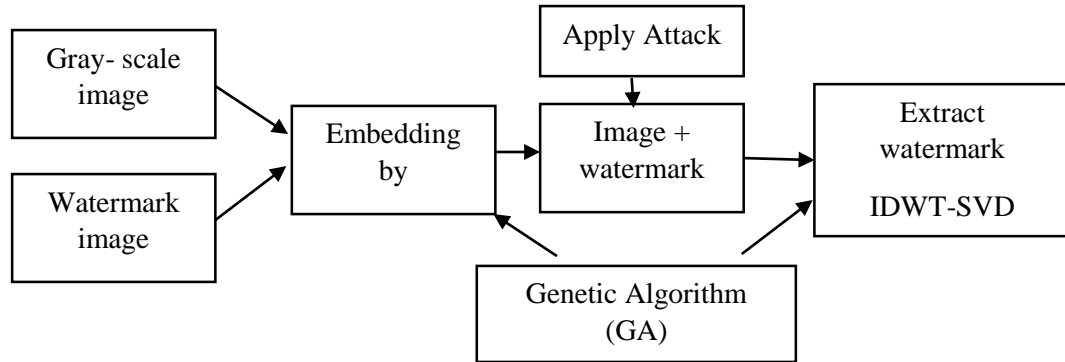


Figure 4: GA for embedding and extracting watermarking.

In this study, for the application of GA optimization, this discussion clearly demonstrates that any objective function that is utilized for optimizing watermark embedding should consider both PSNR and the correlation (watermark). This objective function is subsequently used to optimize the PSNR. The result of the proposed technique for PSNR optimization and correlation is better than the approaches used without optimization techniques. In addition, our result of our approach is better than the state of the art approaches which they used optimization.

For the embedding watermarking by using the GA generate the initial population by random. Here, each solution is a row vector of size $m \times m$ which equals to the watermark size. After this, for each solution i of the GA population, the execution of the watermark embedding algorithm is expressed as:

$$S' = S + \delta * S_w \quad (13)$$

Where δ is the scaling factor.

The procedure of extracting watermark by GA is as following:

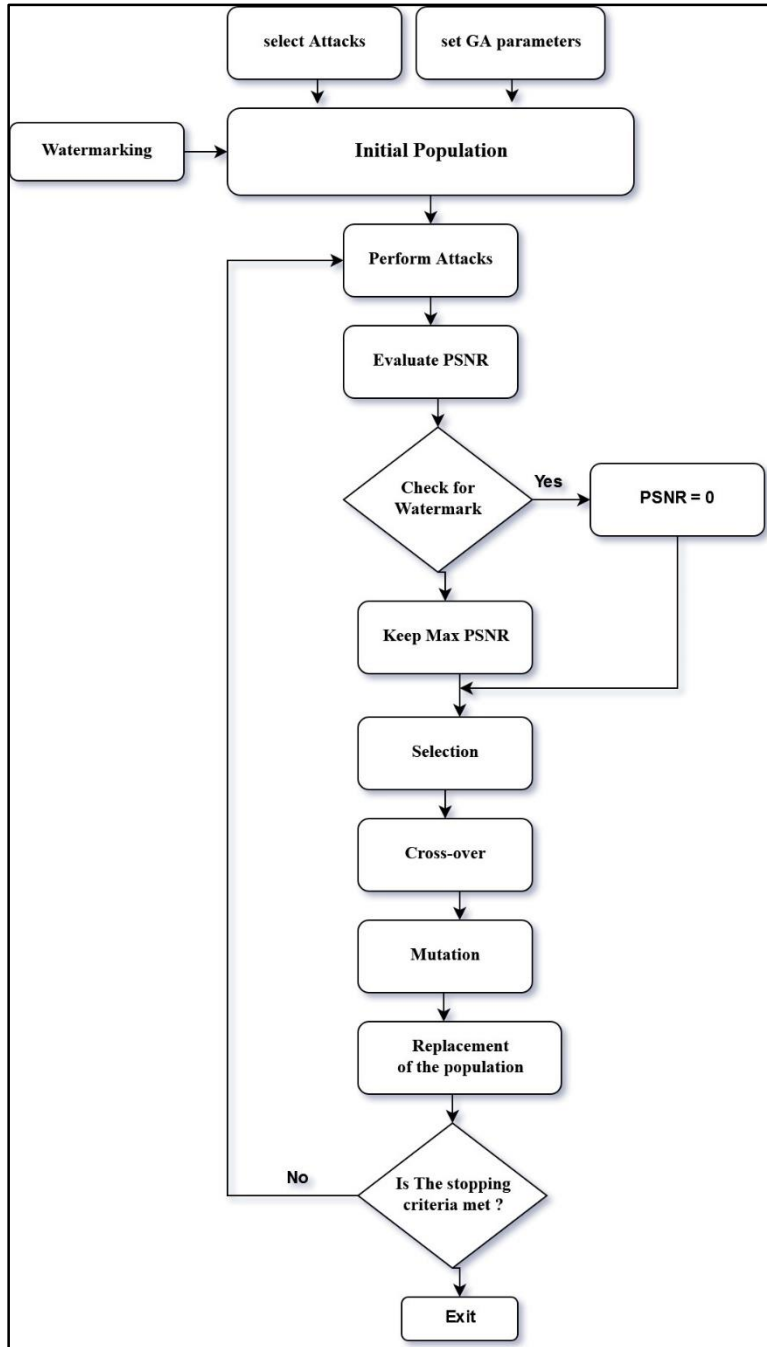
- 1- Apply T types image processing attacks on the signed image I' one by one attacks. This generates T different types of attacked watermarked images for the signed image I' .
- 2- Extract the watermarks from the attacked watermarked image.
- 3- Compare the PSNR between the original image I and signed image I' and the correlation values for attacked image.

- 4- Calculate the objective value of GA by using objective function is given in

$$\text{Objective function} = \text{PSNR} + 100 * \text{correlation} \quad (14)$$

Where: the correlation comprises the normalized cross-correlation between the original watermark and extracted watermark from each attacked signed image.

- 5- Choose the individuals with the best fitness values.
- 6- create new population through the crossover and mutation on the select individuals.
- 7- repeat the operations until the stopping criteria, the maximum amount of iteration (MAX-it) is achieved.



Figuer 5: Block diagram of the proposed GA steps, to attempt the removal of the watermark.

4. Experimental results and discussion

This section is dedicated to the performance evaluation of the recommended watermarking scheme and comparison with state of the art algorithms. In this experiment, the host images with size 512×512 , (gray scale image) and 50×20 grey scale image alongside the ‘copyright’

watermark for owner's signature are to be used. Table 2 shows all the rate of GA used in this study, starting from the size of population until the stopping criteria is reached. All the schemes take into account the same size of the host image and watermark images for the experimental analysis. The schemes are all coded in MATLAB and executed on a personal computer (intel pentium (R) Core i5 CPU at 3.40 GHz with 4 gigabyte RAM), running on windows 10 operating system (64-bit). The recommended parameter setting are used for running the schemes and comparison is made from the respective studies.

Table 2: Genetic Algorithm parametrization used in the experiment

Population size	30 (times number of variables)
Creation function	Uniform
Fitness scaling	Proportional // fit = PSNR + 100 × CORR
Parameter selection	Roulette wheel
Crossover function	Single point
Crossover probability	0.7
Elite count	1
Mutation function	Uniform
Mutation rate	0.01
Stopping criteria	100 iterations

The algorithm appears to be powerful against different types of attacks and proves the ownership image after attacks. In this study, we improve the imperceptibility and robustness of watermark under the types of attacks by using SVD-GA, and by building the powerful system. For the imperceptibility, it is important that the visible watermarking and the embedded watermark are imperceptible. Generally, the watermark technique is said to be imperceptible, when the original and the watermarked image are mutually. As shown the literature, the imperceptible by way of objective process is performed by taking into account the quantitative index, peak signal to noise ratio (PSNR).

$$PSNR = 10. \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (15)$$

Where the Mean Square Error (MSE) represents the aggregate squared error amid the altered and the actual image. Meanwhile, PSNR represents the peak error measure while MAX denotes the highest pixel's value.

For the robustness watermark under types of attacks, normalized correlation (P), is employed in the similarity assessment between the original watermark (w) and the extracted watermark (\hat{w}) as expressed below:

$$P(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2}} \quad (16)$$

Where: ρ represents the introduced watermark w and abstracted watermark \hat{w} in terms of correlation while N denotes the watermark image's measure.

In addition, the probability of the detection of false watermark is expressed as:




$$P_{fp} = p\{NC(W, W') \geq T_p | \text{no watermark}\} \quad (17)$$

Where: $p\{A/B\}$ denotes the probability of event A given that event B , T_p entails a threshold. Since $w(i)$ and $w'(i)$ are either 0 or 1, respectively, $w^2(i)$ and $w'^2(i)$ are either 0 or 1.

Table 3: State of the Art algorithms in comparison

#	Algorithm Symbol	References	Description
1	DCT-GA	(Shieh et al. 2004)	Discrete cosine transform with genetic algorithm to improve watermarked image quality.
2	SVD-Tiny GA	(Chin Lai 2011)	Singular value decomposition with tiny genetic algorithm to improve the visual quality of the watermarked image and the robustness of the watermark.
3	LSB-GA	(Kanan & Nazeri 2014)	Least significant bit with genetic algorithm to propose a tunable visual image quality and data lossless method.

We presented the discussion and comparisons between our algorithm and other previously published, we point out the superiority of our algorithm. The simulation result indicate that our watermarking is more robust and invisibility in the preposed method.

Original image	Watermark	Original image + watermark
		
The (PSNR) = 52.218		correlation = 0.968

Figuer 6: embedding watermark with original image using SVD-GA

In figuer 6 show the embedding watermark imge inside the original image (Lena image) by using the SVD and GA. Our propose method was better then when compear with another technique from the litratuer review. In our proposed the ratio for the PSNR was 52.21dB, and the correlation was 0.96.

In order to make a direct comparison of the propred method against the above algorithm, (Kanan & Nazeri 2014) the author callculate the PSNR, the ratio for the PSNR (Lena image) was 45.12dB. In 2011 by Chin Lai, the rate for the PSNR was 47.49dB, and the correlation was 0.99. The (Shieh et al. 2004) proposed a GA based on discrete cosine transform (DCT), the PSNR was 34.79dB, and the correlation was 0.74.

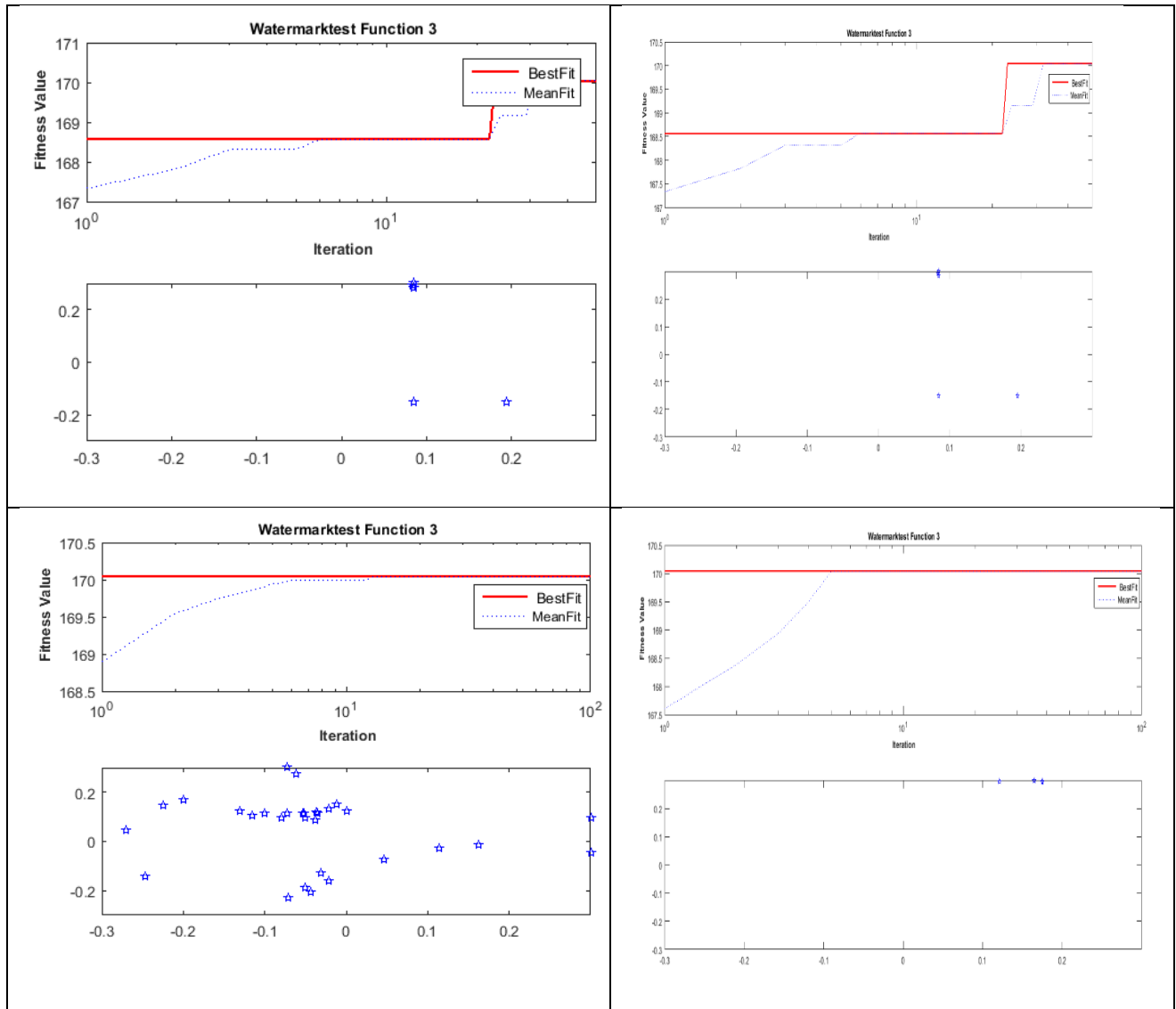


Figure 7: the performance of optimization with out attack

The figure 7 explain the evaluated performance of the optimization algorithm using Lena image 512×512 original image, testing and calculate the ratio of the best fitness. GA-based training procedure described, number of iteration was 100 and the population was 30 and the crossover was 0.7 and 0.1 for the mutation. We show the different result between figure a and b, where was the ratio of figure a for the population 30 and number of iteration 100, then the figure b was the population 10 and the number of iteration 50. In the end we choose the ratio of population 30 and the maximum iteration 100 when implementation the experiment under types of attack.

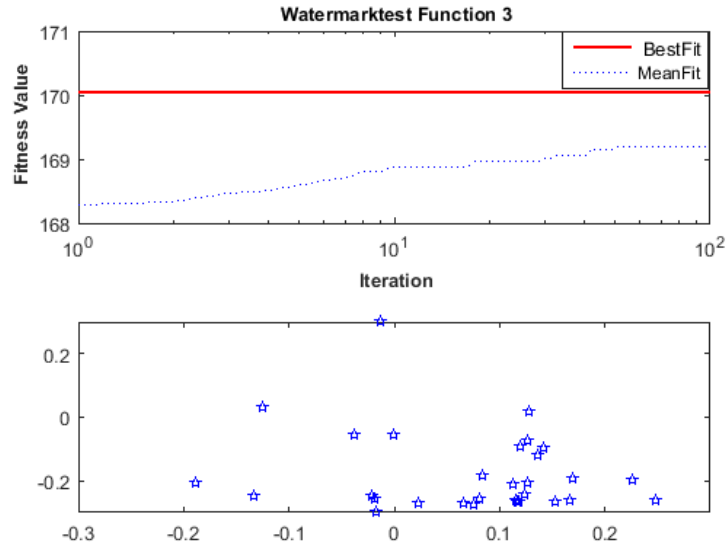


Figure 8: After 0.2 for Gaussian noise attack

In figure 8, we show the value of best fitness after applying the Gaussian noise attack was 170. A Gaussian noise was added to the watermarked image. The result of the GA optimization indicates that the fitness function was maximum (170). This result was obtained at the 100th iteration and 30 population size of the GA optimization process.

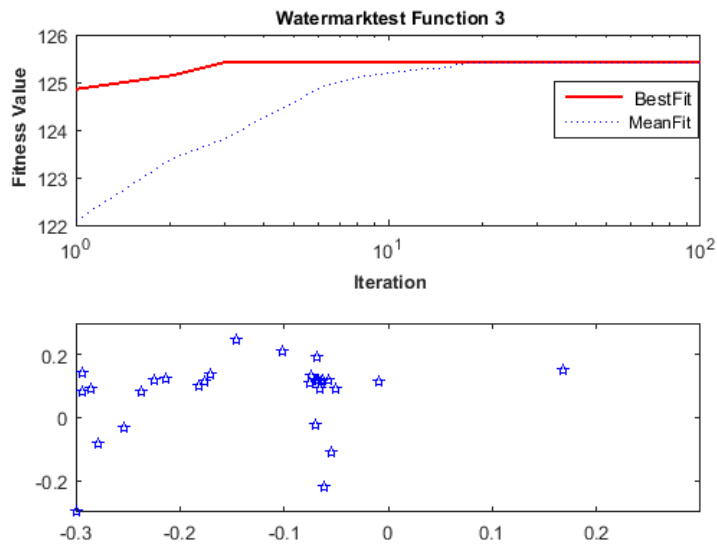


Figure 9: After 0.5 for Gaussian noise attack

A Gaussian noise was added to the watermarked image. The result of the GA optimization indicates that the fitness function was maximum (126). This result was obtained at the 100th iteration and 30 population size of the GA optimization process.

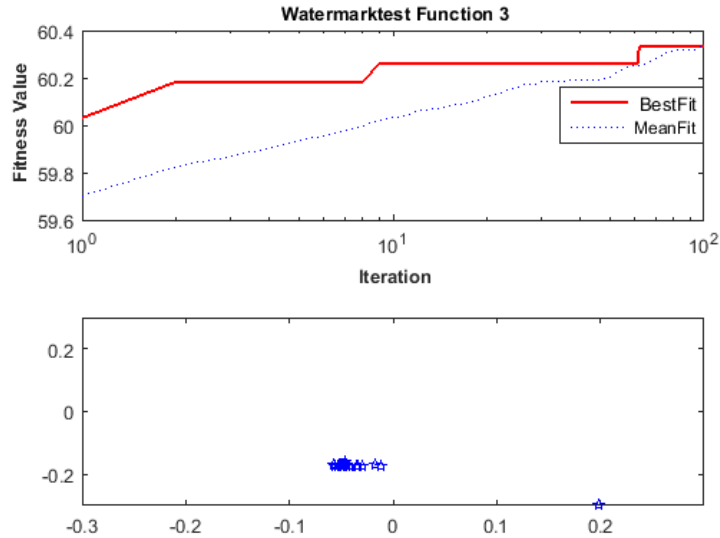


Figure 10: GA-based optimization after 60° of image rotation attack

In figure 10 show the result of GA optimization process indicates that the fitness function was the maximum (60.4), after 60° of image rotation attack. The watermarked image was rotated with different angles. This result was obtained at the 100 iteration of GA optimization process and 30 of population size.

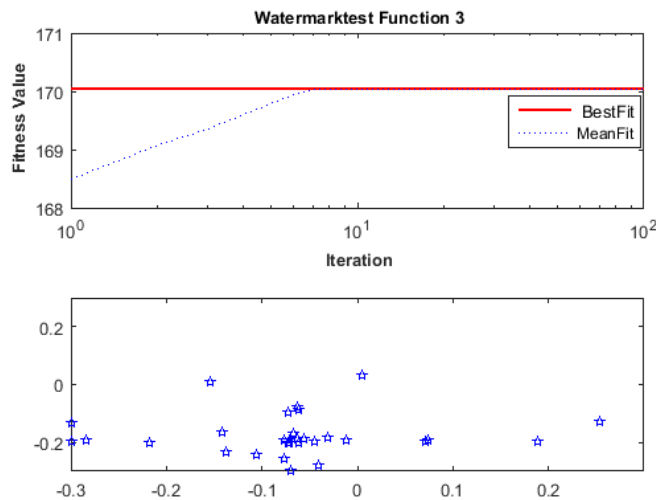


Figure 11: GA-based optimization after 90° of image rotation attack

In figure 11 show the result of GA optimization process indicates that the fitness function was the maximum (170), after 90° of image rotation attack. The watermarked image was rotated with different angles. This result was obtained at the 100 iteration of GA optimization process and 30 of population size.

5. Conclusion

In this paper, we proposed GA for digital image watermarking scheme. The proposed GA used to optimize the performance of scaling factor in matrix form. The result obtained shows that the proposed GA got high robust watermarking image. The performance evaluated by using different types of attacks. The correlation between the original watermark and the extracted watermarked image can prove the ownership images. In addition, we treated the problem of false positive in SVD by using the proposed GA. For the future work, we planning to investigate another technique in order to solve the false positive problem with less effort.

6. Reference

- Abbasi, A., & Seng, W. C. (2012). Robust Image Watermarking Using Genetic Programming. *Journal of Software and Systems Development*, 2012, 1.
- Ali, M., Ahn, C. W., Pant, M., & Siarry, P. (2015). An image watermarking scheme in wavelet domain with optimized compensation of singular value decomposition via artificial bee colony. *Information Sciences*, 301, 44-60.
- Atheer, Bassel & Md. Jan Nordin (2016). Digital Image Watermark Authentication Using DWT-DCT. *Journal of Engineering and Applied Sciences*, 3227-3232
- Cox, I., Kilian, J., Leighton, T., & Shamoan, T. (1996). *A secure, robust watermark for multimedia*. Paper presented at the Information Hiding.
- Cox, I. J., Kilian, J., Leighton, F. T., & Shamoan, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12), 1673-1687.
- Dharwadkar, N. V., & Amberker, B. (2010). An efficient non-blind watermarking scheme for color images using discrete wavelet transformation. *International Journal of Computer Applications*, 2(3), 60-66.

- Emami, M. S., & Omar, K. (2013). A low-cost method for reliable ownership identification of medical images using SVM and Lagrange duality. *Expert Systems with Applications*, 40(18), 7579-7587.
- Gharghory, S. M. (2011). Hybrid of particle swarm optimization with evolutionary operators to fragile image watermarking based DCT. *International Journal of Computer Science & Information Technology*, 3(3), 144-157.
- Gonzalez, R. C., Woods, R. E., & Eddins, S. (2004). Digital Image Processing Using MATLAB, Prentice Hall." *Upper Saddle River, NJ*.
- Guo, J., Zheng, P., & Huang, J. (2015). Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation*, 30, 125-135.
- Hussein, E., & Belal, M. A. (2012). *Digital watermarking techniques, applications and attacks applied to digital media: a survey*. Paper presented at the International Journal of Engineering Research and Technology.
- Jain, C., Arora, S., & Panigrahi, P. K. (2008). A reliable svd based watermarking schem. *arXiv preprint arXiv:0808.0309*.
- Lee, H.-K., Kim, H.-J., Kwon, K.-R., & Lee, J.-K. (2005). *ROI medical image watermarking using DWT and bit-plane*. Paper presented at the Communications, 2005 Asia-Pacific Conference on.
- LI, L.-d., GUO, B.-l., & Lei, G. (2008). Rotation, scaling and translation invariant image watermarking using feature points. *The Journal of China Universities of Posts and Telecommunications*, 15(2), 82-87.
- Li, L., Qian, J., & Pan, J.-S. (2011). Characteristic region based watermark embedding with RST invariance and high capacity. *AEU-International Journal of Electronics and Communications*, 65(5), 435-442.
- Lin, W.-H., Wang, Y.-R., & Horng, S.-J. (2009). A wavelet-tree-based watermarking method using distance vector of binary cluster. *Expert Systems with Applications*, 36(6), 9869-9878.
- Lu, C.-S. (2004). *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*: Igi Global.

- Meerwald, P., & Uhl, A. (2001). *Survey of wavelet-domain watermarking algorithms*. Paper presented at the Photonics West 2001-Electronic Imaging.
- Memon, N. A. (2010). *Watermarking of medical images for content authentication and copyright protection*. Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Swabi.
- Mishra, A., Agarwal, C., Sharma, A., & Bedi, P. (2014). Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. *Expert Systems with Applications*, 41(17), 7858-7867.
- Run, R.-S., Horng, S.-J., Lai, J.-L., Kao, T.-W., & Chen, R.-J. (2012). An improved SVD-based watermarking technique for copyright protection. *Expert Systems with Applications*, 39(1), 673-689.
- Shih, F. Y., & Wu, S. Y. (2003). Combinational image watermarking in the spatial and frequency domains. *Pattern Recognition*, 36(4), 969-975.
- Thabit, R., & Khoo, B. E. (2014). Robust reversible watermarking scheme using Slantlet transform matrix. *Journal of Systems and Software*, 88, 74-86.
- Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE transactions on circuits and systems for video technology*, 13(8), 890-896.
- Waleed, J., Jun, H. D., Abbas, T., Hameed, S., & Hatem, H. (2014). A Survey of Digital Image Watermarking Optimization based on Nature Inspired Algorithms NIAs. *International Journal of Security and Its Applications*, 8(6), 315-334.
- Wang, Y.-R., Lin, W.-H., & Yang, L. (2011). An intelligent watermarking method based on particle swarm optimization. *Expert Systems with Applications*, 38(7), 8024-8029.