




Dual Watermarking for Color Images: A New Image Copyright Protection Model based on the Fusion of Successive and Segmented Watermarking

Saad M. Darwish¹  · Layth Dhafer Shukur Al-Khafaji²

Received: 8 February 2019 / Revised: 14 August 2019 / Accepted: 30 September 2019 /

Published online: 16 December 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Watermarking has been suggested as a generic technique to solve various problems associated with topics in the areas of digital rights management and multimedia security. Most of the early methods were based on single watermark embedding, but there are great limitations when single watermark embedding algorithms are tried into practical applications. The multiple watermarks are intended to convey different information at the same time. Current approaches rely on adding many watermarks in different bands or channels by means of scaling factor and embedding locations that are mainly defined by experts. This brought many challenges in achieving equilibrium between security, robustness, and quality. The aim of this work is to introduce an intelligent dual watermarking model for colour images that ensure image security for copyright protection (dual watermarking for single purpose). To optimize the dual watermarking requirements, the proposed model that employs both successive (re-) and segmented watermarking techniques is to be implemented with a multi-purpose evolutionary algorithm. Genetic algorithm is adopted to determine the embedding locations and scaling factors for different watermarks according to the features of each host image to balance between imperceptibility and robustness. The wavelet transform is utilized for salient features extraction because of its excellent space-frequency localization of salient image features. In addition, the suggested model encrypts the watermarks with the aid of Walsh transform; so that it is difficult to handle the watermarks even after being extracted by the attackers. Experimental results show that the proposed model is more robust against common image manipulation attacks in terms of PSNR and NCC.

Keywords Dual Watermarking · Information Fusion · Image Copyright Protection · Optimization · Wavelet-based Feature Extraction · Walsh Encryption

✉ Saad M. Darwish
saad.darwish@alexu.edu.eg

¹ Department of Information Technology, Institute of Graduate Studies and Research, University of Alexandria, 136 Horreya Avenue, El Shatby 21526, P.O. Box 832, Alexandria, Egypt

² Computer Technical Engineering, Djlal University College, Baghdad, Iraq

1 Introduction

Extraordinary growth of Internet, peer-to-peer file sharing, and signal processing technologies have made the reproduction, manipulation, and distribution of multimedia data much easier than ever before. This unavoidably increases the demand for protection of copyrighted data. Digital watermarking is a promising technology for copyright protection [36]. Digital image watermarking techniques can be classified into [29, 48]: spatial and transform domain watermarking based on embedding domain of the host image. The watermark embedding techniques in spatial domain insert watermark directly by modifying the pixel value of the cover image. This technique has less computation time; however, it is less secure and not as robust as the frequency domain. The frequency domain embedded technique transforms data from the spatial domain into the frequency domain (reveals the most features of the image), and then embedded the hidden data in the image. This transform domain can strengthen resistance under attacks, and increase security.

To understand the concept of watermarking, a clear understanding of the difference between watermarking and other techniques like steganography, cryptography, and digital signature for data /image protection is required [6, 7, 9, 10, 21–23]. In steganography, data which is concealed has no association with the cover medium, and the necessity from such a system is that no suspicion should arise that a medium is carrying any concealed data. Watermarking is the subclass of steganography, but in this case, the data which is hidden has an association with the cover medium data. Cryptography scrambles a message so that it cannot be understood by unauthorized user. This does not happen in watermarking. Neither the cover medium nor the copyright data change its meaning [4, 8, 11, 12, 20]. Rather, copyright data is hidden to give the ownership information of the medium in which it is hidden. A digital signature validates the authenticity and integrity of a message, whereas a digital watermark is inside a multimedia message. Both digital signature and watermarking protect the integrity and authenticity of a document. A digital signature system is vulnerable to distortion, but a watermark system has to tolerate a limited distortion level [1, 13, 14, 17–19, 24, 25, 27, 28, 41, 54].

In order to identify and maintain proof of ownership, we need to extract watermark after embedding a watermark image in the host image. The extraction techniques of a watermark from the watermarked images are: blind, semi-blind, and non-blind. Blind watermarking does not need the original image to extract the embedded watermark from a watermarked image. The semi-blind watermarking technique needs some information about the original cover image to extract the embedded watermark. The Non-blind watermarking technique requires the complete cover image to extract the embedded watermark. Each watermark should follow its properties like robustness, imperceptibility, capacity, and security [2, 3, 16].

More recently, different watermarking strategies have been suggested in order to solve several problems, ranging from the detection of content manipulations to information hiding, to document usage tracing [35, 46]. Most of the early methods were based on single watermark embedding, but there are great limitations when single watermark embedding algorithms are tried into practical applications in few rare situations, like when multiple users share the copyright, it needs to support multiple users to embed their watermarks synchronously. This highlights the needs for multiple watermark embedding. Multiple watermarks are normally suggested as a method to provide extra security to an image by embedding two or more secret messages into the cover image. To advocate several goals, the multiple watermarks are embedded into the image; to achieve the robustness of image processing operations, which is the desired goal [37].

Unfortunately, there are still some problems that facing dual watermarking approaches and mainly depend on several different factors [31, 37, 43]: (1) adding multiple watermarks (noises) affect the perceptibility (quality) of the cover image. (2) The watermarks must be independent of each other during embedding and extraction phases. (3) The embedding of each watermark should be at a different location that must be known exactly at the extraction phase; i.e., the system requires extra data to save these locations and therefore needs extra payload. In general, building a robust dual image watermarking scheme that tackles the above challenges is required for many applications such as copyright protection, data integrity, tamper detection, fingerprinting, and broadcast monitoring. The attention here is to deal with the tradeoff between watermark capacity, extra payload, computational cost, and imperceptibility.

Recently several approaches have been presented that attempt to tackle the above problems. The existing multiple watermarking algorithms can be divided into three classes, namely: re-watermarking, composite watermarking, and segmented watermarking [31, 34, 38]. In re-watermarking, the watermarks are simply embedded one after the other. The problem which arises is that the watermarks interfere with each other. As a consequence, earlier embedded watermarks possibly get erased by later embedded ones. The advantage is that the embedders do not need to know each other and also the number of watermarks to embed do not need to be known in advance. Composite watermarking builds a single composite watermark from a collection of watermarks and then embeds the composite watermark into the cover image in a usual way. Suitable signal merging methods are required for increased performance. This approach has the need for a trusted party which does the composition and embedding of the single watermarks, and all watermarks have to be present at once.

Regarding segmented watermarking, it divides the cover image into several partitions and allocates each partition for a different watermark. Here, the number of divisions limits the number of watermark signals to be embedded. Besides, when the number of watermarks increases the size of each block decreases. Furthermore, the location of the embedding partitions has to be opened to the embedding algorithm, and each embedding algorithm has to know which partitions are already occupied. This type is one of the most commonly used algorithms. In all cases, it must be confirmed that the embedded watermark is not easily lost, and imperceptibility is also preserved [34, 51]. Recently, integrating the genetic algorithm (GA) into a watermarking scheme to improve its performance and effectiveness has received a great deal of attention among researchers working in this field [35, 36].

1.1 Problem statement

Current multiple watermarking approaches were introduced lately only to be found that they relied only on adding many watermarks in different bands or channels by means of a scaling factor and embedding locations that are mainly defined by experts. This brought many challenges in achieving a balance between security, robustness, and quality since each one can be achieved at the expense of the other and combining them does not give the ideal result. Attempting to attain the suitable trade-off between the previously mentioned requirements, this work is constructed to dispense the opinion of experts by replacing it with intelligent multiple watermarking schemes. However; this needed to bring certain facts about the image that response to various attacks after doing minor changes in the image that does not lead to any distortion or noise in the image which it's a problem itself.

1.2 Motivation of the work

Motivated by the challenges that are facing dual watermarking approaches and in order to cope with them, in this paper, the aim is to introduce an intelligent dual watermarking scheme for colour images that ensure the image can be used in a secure manner for copyright protection. To accomplish such goal, a multi-purpose evolutionary algorithm is presented to optimize additive embedding's scaling factor with the purpose of enhancing embedding strength that affects imperceptibility. Furthermore, it employs the same genetic algorithm with different fitness function to find the optimal embedding locations to achieve robustness against different types of attacks.

1.3 Novelty, contribution, and methodology

The novelty of the suggested model lies on the fusion of dual watermarks from re- and segmented watermarking classes in which both of them is positioned in different locations for easy extraction without affecting the perceptibility of the cover image and quality of the extracted watermarks. The configuration parameters of the fusion process (scaling factor and embedding locations) are semantically determined based on the features of both cover and watermarks images. Aiming to fill the gap of the stationary scaling factor and embedding locations inside existing dual image watermarking approaches, the proposed model adopts GA to find the optimality of these issues that will enhance both of watermarking capacity and imperceptibility in colour images.

To enhance the overall performance, the suggested system relies on (1) $YCbCr$ colour space that is employed in order to take advantage of the lower resolution capability of the human visual system for colour with respect to luminosity. (2) Walsh Hadamard Transform (WHT) that is used to secure dual watermarks. (3) Discrete Wavelet Transform (DWT) that is exploited to enhance imperceptibility by highlighting the most important features appropriate for embedding. (4) Singular Value Decomposition (SVD) that is engaged for matrix factorization to obtain a smaller set of values which has maximum signal content (i.e., dimension reduction to cope with embedding computational cost). Herein, the embedding is within the different colour channels to increase the capacity and achieve multi-purpose watermarking such as copyright protection and content integrity.

The rest of this paper is organized as follows: Section 2 describes some of the recent related works. The detailed description of the proposed model has been made in Section 3. In Section 4, the results and discussions on the dataset are given. Finally, the conclusion is annotated in Section 5.

2 Literature review

Conventional single watermark systems are mainly aimed at accomplishing a single goal, either for forgery detection or image copyright protection [36]. This limitation has resulted in the introduction of multipurpose (multifunction watermarking) and multiple watermarking algorithms. However, most of the recent studies have not indicated a clear distinction between multipurpose and multiple watermark (or cocktail watermarking) algorithms [15, 33, 39, 52, 53]. In order to solve the dual watermarking problems described above, the authors in [46] have suggested applying a de-interlacing process on the transformation sub-bands of host

image according to its even and odd row pixel value. It focuses on the robustness, imperceptibility, and capacity of the watermark in frequency domain against the unintentional and the intentional signals/distortion at the expense of the original image which can be modified due to piracy actions before embedding.

In recent years, swarm-based evolutionary algorithms have been received much attention from researchers [44, 45]. For instance, the authors in [45] presented a novel multiple objective optimized dual watermarking scheme for medical colour images. This approach integrated both of LWT domain and dual optimization technique that combines firefly and bat algorithms. The multiple objectives are perceptual quality, security, and robustness. Yet this method lacks immunity to geometric attack and has very complex computational processes.

In a recent study [43], the authors explored the multipurpose watermarking to hide both copyright and authentication information in the content of multiple watermarking. For this purpose, a wavelet transformation based on texture properties and secret sharing using visual cryptography is used. This scheme is highly robust, does not degrade the original signal, and very efficient in terms of quality. This method lacks the ability to be implemented on colour textures. Concurrently, in 2012, Liao [29] had examined other aspects of visual cryptography, wavelet transformation domain, and YC_bC_r colour model required to assure the re-watermarking concept in which all owners will have dual watermark authentication embedded in a protected colour image, and the number of ownership can be increased without re-computing.

Research reveals that all of the benefits of RGB color space are not attained as expected as there are many challenges and risk in this color space that work as barriers in the success of the RGB color space and make it more difficult to achieve expected benefits. To solve this problem, the author in [32] produced a novel hybrid digital watermarking technique based on the exploitation of both RGB and YC_bC_r colour spaces using spatial domain techniques. This method possessed invisibility, robustness, security, capacity, and complexity characteristics as opposed to the majority of methods which tend to focus only on invisibility and robustness. Yet the image will not survive under compression attack and will lose its commercial value in commercial images databases.

In another work, in 2013, Ouazzane et al. [38] highlighted the main concepts behind multiple levels transformation-based multiple watermarking along with two complementary directions: a “high-level”, and “low-level”. The authors analyzed the robustness and imperceptibility of watermarks in high and low-frequency sub-band at first and second level and find that second level is better than the first level in terms of robustness and imperceptibility at the expense of embedding capacity, watermarked image quality, and computational complexity. At present, wavelet and other frequency domain transformations have become a cutting edge and promising approach in the field of multiple images watermarking. For instance, the authors in [51] presented a proficient implementation of an authorized dual image watermarking system based on discrete wavelet Transform for medical data protection. It appears that by embedding both watermarks into one image, one could achieve extremely high robustness properties in a secure manner concerning a large spectrum of image processing operations.

The work in [15] suggested a new multiple watermarking approach in vector data rather than raster data. Based on the characteristics of vector data, the multiple watermarks were embedded additively in the cover data following additively rule. In the detection progress, the additive watermarks were extracted, and then the contents of watermarks were detected on the basis of correlation detection together with discriminant analysis. Since the embedding rule is

additively in the paper, the suggested scheme requires the original data coordinates that require extra space. In [53], a novel intelligent multiple watermarking techniques for integrity and copyright protection for information present in the source document image is presented. The sensitivity of the information content of a block is based on the homogeneity and relative energy contribution parameters. The appropriate watermarking scheme is applied based on sensitivity classification of the block. Although identifying each block sensitivity requires more accurate classification approaches.

Some works have been done recently for multi-purpose watermarking of medical images. For instance, the concept of signature watermark embedding using error-correcting code is investigated in [5]. In this case, the medical image is divided into two parts, namely Region of Interest (ROI) and Region of Non-Interest (RONI). The reference watermark which is used to detect the authenticity of medical images (integrity control) is embedded in the ROI image. Meanwhile, the signature watermark, which is used for the authority of ownership (proprietary rights) is embedded in the RONI image on the wavelet domain. This method reduced computational time at the expense of image quality, even though it is good still not significant.

Although image dual watermarking has been studied for a few decades, there is still room to make it more efficient and practical in real applications. According to the aforementioned review, it can be found that past studies were primarily devoted to: (1) devising different type of watermarking either multi-objective or multi-purpose watermarking that employs the image information (color spaces, regional statistics, salient image features, and image frequency domain), (2) Not addressing the issues associated with the choice of appropriate scaling factor for embedding (manually adjusted), and (3) Embedding locations are usually identified randomly or according to criteria that do not consider image characteristics into account. However, to the best of our knowledge, little attention has been paid to advising new optimal selection algorithm to determine both of scaling factor and embedding locations and improving its efficiency in the multi-watermarking algorithm as well.

3 The proposed dual watermarking model

This paper proposes a new method that combines both of the first and third watermarking categories (Re-watermarking and segmented) that does not rely on supervised training for determining pixel embedding locations. Furthermore, the original image is segmented into several parts, and each watermark is embedded into the specific share. In this case, the embedding process is based on two overlapped segmented areas, including color channels and wavelet sub-bands. This interleaving makes it hard to know the embedding locations and increases the efficiency of the watermark in facing various types of attacks. Besides, it takes the human visual system into consideration by embedding in specific color channels. The main diagram of the suggested hybrid dual watermarking is depicted in Fig. 1. The following subsections describe in details the steps of the system.

3.1 Problem formulation

A basic dual watermarking scheme for digital image can be defined as a 4-tuple (I, W, E, D) such that [29] [31, 34, 35, 37, 38, 43, 46]:

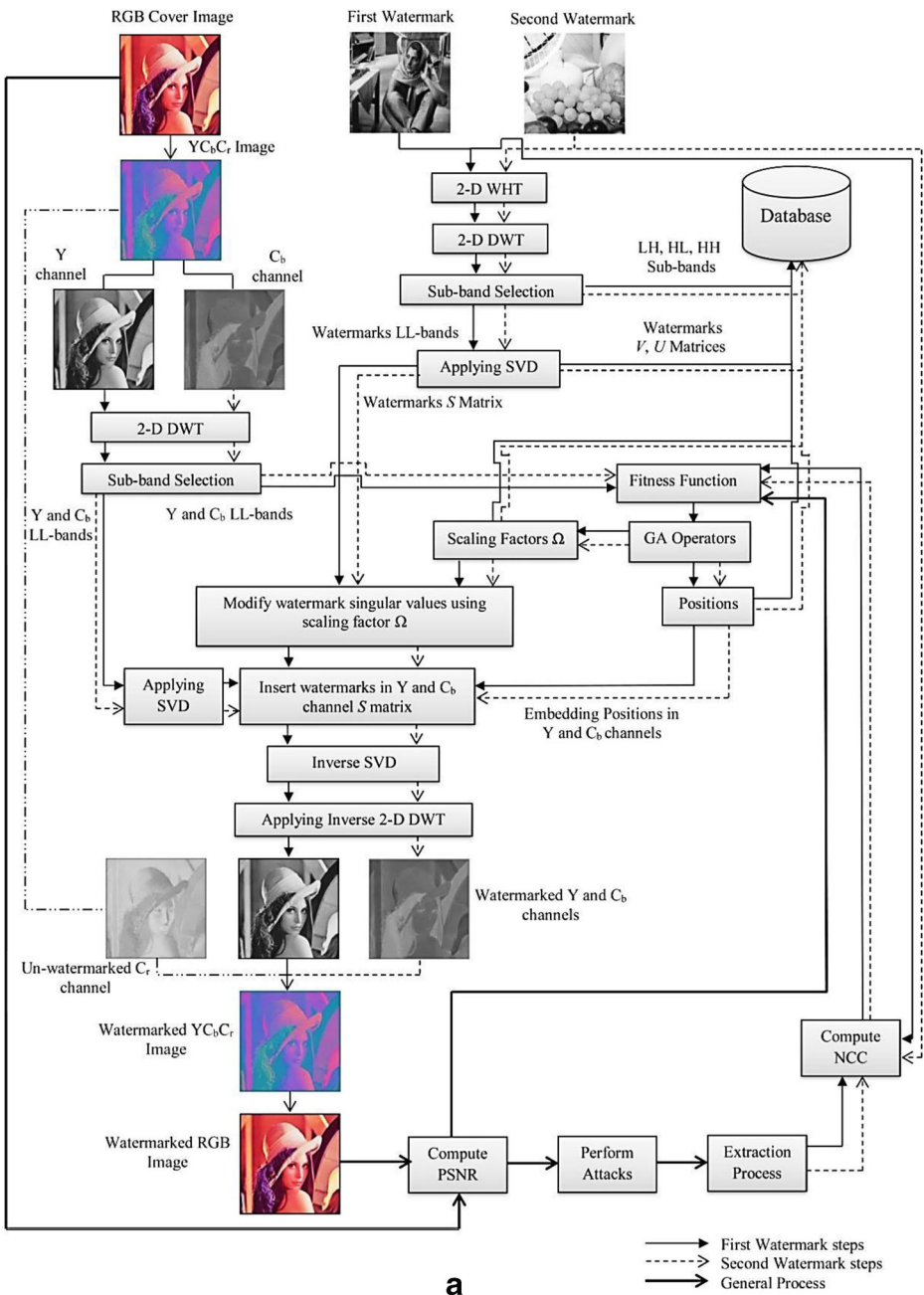


Fig. 1 The main diagram of the suggested system a Embedding process. b Extraction process

– I , the image data space (original un-watermarked image data), which is a set of pixels with value in the positive integers $Z^+ = \{|a| \geq 0 : a \in Z\}$. Each pixel is a set of coordinates, (x, y) for 2D space. An element of image data space is called an image of $a \times b$ size for 2D

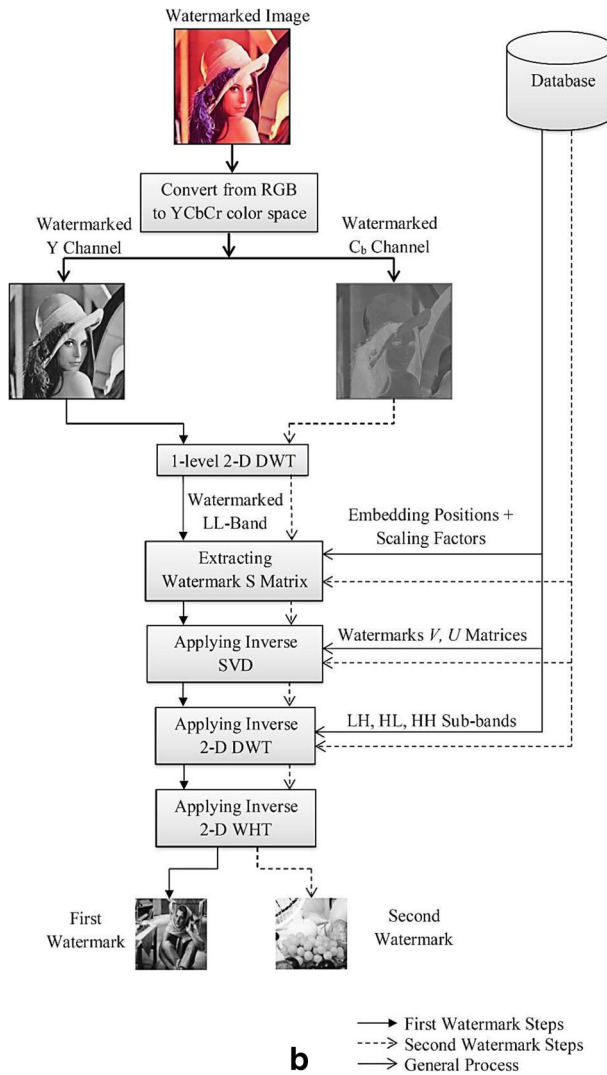


Fig. 1 (continued)

space, $a, b \in \mathbb{Z}^+$ and $x = \{1, 2, 3...a\}$, and $y = \{1, 2, 3...b\}$. $W = \{w_1, w_2\}, \hat{T}, \tilde{T}$, and \tilde{I} are the subsets of I , where:

- $w_1 \in W$ is the set of image data used for first watermark generation and $w_1 \cap I = \varphi$;
- $w_2 \in W$ is the set of image data used for second watermark generation and $w_2 \cap I = \varphi$;
- \tilde{T} is the set of watermarked image data;
- \tilde{I} is the set of estimated original image data;
- \tilde{w}_1 is the set of estimated of first image watermark.
- \tilde{w}_2 is the set of estimated of second image watermark.
- E is a function $E : I \times W \rightarrow \tilde{I}$ that is used for watermarks embedding.

- D is a function $D: \bar{I} \times W \times \perp \rightarrow \tilde{I} \times \tilde{w}_1 \times \tilde{w}_2$ that is used for watermark extraction, where $\perp = \{\perp_1, \perp_2\}$ indicates the embedding locations.
- The dual watermarks w_1 and w_2 are valid if and only if they are obtained from valid inputs (\bar{I}, \perp) using the valid first and second watermarks generation function W . Similarly, a watermarked image, \bar{I} is valid if and only if $E(I, w_1, w_2) = \bar{I}$ for valid inputs, $(I \times W)$. More formally, we can define a digital image watermarking scheme to be complete, if the following is true: for I, w_1, w_2 there exists $\tilde{I}, \tilde{w}_1, \tilde{w}_2$ where $I \approx \tilde{I}, w_1 \approx \tilde{w}_1, w_2 \approx \tilde{w}_2$ such that $D(E(I, W), (I, W)) = (\tilde{I}, \tilde{w}_1, \tilde{w}_2)$. Here, the symbol ‘ \approx ’ denotes the perceptual similarity between two images.

3.2 Watermarking embedding stage

Watermark embedding function considers where and how to embed the watermarks satisfying various requirements of the cover images. An embedding function takes the dual watermarks, w_1, w_2 and the original image data, I as input to output the watermarked image data, \bar{I} . The following steps are performed to embed two grayscale images as watermarks inside a color RGB cover image.

Step 1: Converting into $YCbCr$ Colour Space

The cover image is converted to $YCbCr$ colour space as it is better to model the human colour perception. This type of colour space allows more precise colour detectors to be created since colour intensity is removed when viewing the C_r or C_b vectors [31] [32]. Herein, the embedding is performed in Y , and C_b channels as the luminance channel represents the intensity of the image; it is the ideal space for data hiding whenever tolerance against JPEG compression and noise addition are the most important concerns; whereas the chrominance channel, C_b channel has more ability to defeat various types of attacks compared to chrominance space C_r [36].

Step 2: Securing Watermarks using WHT

The suggested model encrypts the watermarks to increase the security; so that it is difficult to handle the watermarks even after being extracted by the attackers. Herein, the WHT is employed because it contains only ± 1 , and no multiplications are required in the computation. The advantages of Hadamard transform include that its elements are real, and its rows and columns are orthogonal to each other [40]. The Hadamard matrix of m order is the (± 1) matrix with a size of $m \times m$, H_m satisfying the orthogonal condition:

$$H_m H_m^T = H_m^T H_m = m A_m \quad (1)$$

where H is the Hadamard matrix, T is a transposition sign, A_m is an identity matrix of m order that represents the number of rows and columns in the watermark image (square image in our case). One of the well-known Hadamard matrices is the Sylvester matrix, which is a matrix of order 2^k and can be recursively generated as follows:

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, H_1=1, k=1, 2, \dots, m, \quad H_m^{-1} = \begin{bmatrix} H_{m-1}^{-1} & \frac{1}{2}H_{m-1}^{-1} \\ H_{m-1}^{-1} & -\frac{1}{2}H_{m-1}^{-1} \end{bmatrix} \tag{2}$$

H_{2^k} is the watermark encrypted matrix, and H_m^{-1} is the watermark decrypted matrix [40].

Step 3: Salient Features Extraction using DWT

DWT is more frequently used in digital image watermarking due to its excellent spatial localization and multi-resolution techniques [38, 48]. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermarks are embedded efficiently. DWT decomposes the image into four sub-bands (level 1); the LL sub-band represents the coarse-scale of DWT coefficients while the other sub-bands LH, HL, and HH represent the fine-scale of DWT coefficients. In general, most of the image energy is found at the LL sub-band and therefore, the embedding of the watermarks in other sub-bands may degrade the quality of image [39]. Informal, the wavelet decomposition can be described as [5] [30]:

$$\varphi_{(j,k)}(x) = 2^{j/2} \varphi(2^j x - k) \tag{3}$$

$$\phi_{(j,k)}(x) = 2^{j/2} \phi(2^j x - k) \tag{4}$$

$$\varphi(x) = \sum_k^{N-1} g_k \sqrt{2\phi(2x-k)} \tag{5}$$

$$\phi(x) = \sum_k^{N-1} h_k \sqrt{2\phi(2x-k)} \tag{6}$$

$$WT_{LL} = \sum_k^{N-1} \sum_p^{N-1} h(k)h(p)_{LL} (2x-k)^j (2y-p)^{j-1} \tag{7}$$

$$WT_{LH} = \sum_k^{N-1} \sum_p^{N-1} h(k)g(p)_{LH} (2x-k)^j (2y-p)^{j-1} \tag{8}$$

$$WT_{HL} = \sum_k^{N-1} \sum_p^{N-1} g(k)h(p)_{HL} (2x-k)^j (2y-p)^{j-1} \tag{9}$$

$$WT_{HH} = \sum_k^{N-1} \sum_p^{N-1} g(k)g(p)_{HH} (2x-k)^j (2y-p)^{j-1} \tag{10}$$

where φ is the wavelet function and j , k , and p are integers represent scale (wavelet's width) and dilate (vertical and horizontal positions) the wavelet function. The function $\Phi(x)$ is the scaling function. h_0, h_1, \dots, h_{N-1} are the low pass wavelet coefficients, and g_0, g_1, \dots, g_{N-1} are the high pass wavelet coefficients, and N is the number of vanishing moments. DWT is applied on both the cover image in addition to the dual encrypted watermarks for the selected channels only.

Step 4: Step 4: Dimension Reduction using SVD

SVD is a matrix decomposition to obtain a smaller set of values which has maximum signal content from the derived wavelet coefficients [30]. These singular values represent the most energy of the signal. Because of translation, scaling properties of SVD it can be used as a tool to develop watermarking schemes [49]. The system applies SVD to the LL band for image watermarks in which for a given two matrices WT_{LL,w_1}, WT_{LL,w_2} of size $n \times n$, SVD operation decomposes it to three different matrices U, S , and V such that [30, 49]:

$$WT_{LL,W} = USV^T = \sum_{i=1}^n \lambda_i u_i v_i^T, (w_1, w_2 \in W) \quad (11)$$

where $u_i \in U$ and $v_i \in V$ are the left and right singular vectors respectively, $S = \text{diag}(\lambda_i)$ is a diagonal matrix of singular values $\lambda_i, i = 1, \dots, n$. For applying SVD to the cover image, the model divides each LL band of the selected channels into blocks of equal size to the LL band of the watermarks. After that, the SVD is applied for each block resulting $\lambda_{i,B}$ for each color channel. The number of vectors λ_i depends on the number of blocks B calculated by dividing the size of LL band of the cover image on the size of the watermark. The rationale of using SVD is that when a small perturbation is added to an image, the large variety of its singular values of S matrix does not occur, furthermore, it represents intrinsic algebraic image properties [49].

Step 5: Determining Optimal Embedding Positions and Scaling Factor

In general, determining the scaling factor for additive watermarking to control the strength of watermarks embedding is an important parameter to satisfy the perceptibility even when dual watermarks are embedded. Furthermore, finding the paramount locations for the watermarks embedding to achieve optimal robustness against various types of attacks represents an essential requirement for watermarking schemes [35, 36, 48]. The strength of embedding watermark and embedding locations are determined by utilizing the GA method to balance the robustness and perceptual transparency requirements [48] [49].

Given the singular values for every block of the selected cover image's color channels $S_{I,Cb}, S_{I,Y}, S_{I,Bi}$ and singular values of gray-scale watermark images S_{w_1}, S_{w_2} ; the algorithm first normalizes the singular values of the watermarks besides a random block, then the initial scaling factor Ω for that random block is calculated by aggregating the watermarks vector values S_{w_1}, S_{w_2} and dividing them by the aggregated vector values in the block $S_{I,Cb,Bi}, S_{I,Y,Bi}$ [35, 36, 48]:

$$\Omega_{I,Cb,Bi} = \frac{\sum_1^r \|S_{w_1}\|}{\sum_1^r \|S_{I,Cb,Bi}\|}, \Omega_{I,Y,Bi} = \frac{\sum_1^r \|S_{w_2}\|}{\sum_1^r \|S_{I,Y,Bi}\|} \quad (12)$$

r is length of $S = \text{diag}(\lambda_i)$; this initial value for the block is used to embed S_{w_1} in the corresponding block of $S_{I,Cb,Bi}$ and S_{w_2} in $S_{I,Cb,Bi}$ using additive embedding. The rationale of using this type of embedding is that it gives better quality and less distortion as compared to other embedding techniques in frequency domain [48] [49].

$$\bar{S}_{I,Cb,Bi} = S_{I,Cb} + \Omega_{I,Cb,Bi} \times S_{w_1}, \quad \bar{S}_{I,Y,Bi} = S_{I,Y} + \Omega_{I,Y,Bi} \times S_{w_2} \quad (13)$$

$\bar{S}_{I,Cb,Bi}, \bar{S}_{I,Y,Bi}$ are the result of the embedding both watermarks respectively in the randomly selected channel block. Then these modified singular values are combined with their left and right singular vectors of that random block by employing inverse SVD to get the watermarked LL band for each colour channel [49].

$$WT'_{LL,I,Cb} = U_{I,Cb} \bar{S}_{I,Cb,Bi} V_{I,Cb}^T, \quad WT'_{LL,I,Y} = U_{I,Y} \bar{S}_{I,Y,Bi} V_{I,Y}^T \quad (14)$$

After that, each watermarked LL band is combined with the other unaltered bands to form the watermarked colour channels Y'_W , and Cb'_W . The three colour channels are then merged to get the watermarked image in $YCbCr$ colour space; that are converted to RGB colour space to get watermarked image \bar{I} [34, 36, 48].

Given the initial watermarked image, the next step is to optimize the embedding locations by utilizing GA besides the optimal scaling factor given a specific objective function. In this case, an instance of a GA-based dual watermarking optimization problem can be described in a formal way as a four- tuple (P, Q, ζ, f) defined as [47, 49]:

- P is the solution space (initial population – a combination of 2^n indexed blocks) where n represent the number of bits needed to represent the block index. Each bit is signified as a gene and every block is represented as a chromosome.
- Q is the feasibility predicate (different operators- selection, crossover, and mutation). The crossover is the process of exchanging the parent's genes to produce one or two offspring that carry inherent genes from both parents to increase the diversity of the mutated individuals. Herein, a single point crossover is employed because of its simplicity. The purpose of mutation is to prevent falling into a locally optimal solution of the solved problem; a uniform mutation is employed for its simple implementation. The selection operator retains the best fitting chromosome of one generation and selects the fixed numbers of parent chromosomes. Tournament selection is probably the most popular selection method in the genetic algorithm due to its efficiency and simple implementation.
- ζ is the set of feasible solutions (new generation populations). With these new generations, the fittest chromosome will represent the best block of the cover's LL band that gives the optimal embedding location according to its index. This individual (block) will specify the optimal scaling factor explicitly according to the block's singular values.
- f is the objective function (fitness function). The individual that has higher fitness will win to be added to the predicate operators mate. Herein, the fitness function is computed based on $PSNR$ value that shows the extent of distortion introduced to the original cover image due to dual watermark insertion (transparency indicator) and NCC that specifies the degree of similarity between original watermarks and extracted watermarks of each block in the population for each generation (robustness indicator) [48].

$$f_{Bi} = (PSNR + \mu \times NCC)^2 + \frac{1}{1 - (PSNR + \mu \times NCC)} \quad (15)$$

B_i is the block with index i , and μ is a weight used to make a balance between transparency and robustness impact ($\mu = 1$). The fitness parameters $PSNR$ and NCC are calculated under different type of attacks such as Gaussian noise, cropping, and geometric attacks. Algorithm 1 illustrates the pseudo code of the GA.

Algorithm 1: Genetic Algorithm Pseudo Code.

| |
|---|
| <ol style="list-style-type: none"> 1. $t \leftarrow 0$ 2. <i>Generate Initial Population</i> [$P(t)$]; 3. <i>Evaluate Population</i> [$P(t)$]; 4. While not termination do 5. $P'(t) \leftarrow$ <i>Variation</i> [$P(t)$]; 6. <i>Evaluate population</i> [$P'(t)$]; 7. $P(t+1) \leftarrow$ <i>Apply GA Operators</i> [$P'(t) \cup Q$]; 8. $t \leftarrow t+1$ 9. End while |
|---|

During the embedding process, cover image ID, size, and some values will be stored in the database to be used later in the extraction process where the suggested system falls under the semi-blindness category. These values include S_{I, C_b, B_i} and S_{I, Y, B_i} of the original cover image, the embedding locations of both watermarks \perp_1 , and \perp_2 , the scaling factors used in the embedding process for both watermarks Ω_{I, Y, B_i} , and Ω_{I, C_b, B_i} , U , V matrices, LH, HL, HH sub-bands as additional data that are needed to fully extract the watermarks. As these matrices are sparse (most of items are zeroes) in natural, they do not need a large storage space.

3.3 Dual Watermarks Extraction

Extraction process is done in a reverse way to the embedding process, which includes the following steps [15, 29, 31, 33–35, 37–39, 43, 44, 46, 51–53]:

- 1- Given the watermarked image \bar{I} , match its' ID and size from the database to retrieve the right GA parameters that are needed in the extraction process. Then the watermarked image \bar{I} is transformed from RGB colour space to YC_bC_r colour space.
- 2- Separate YC_bC_r colour space into its basic channels and select both of Y and C_b channels for extraction process.
- 3- Apply DWT for both channels to obtain LL bands $WT_{LL, Y}$ and WT_{LL, C_b} .
- 4- Divide the $WT_{LL, Y}$ and WT_{LL, C_b} of the selected channels into blocks (the number of blocks was stored in the database) of equal size to the LL band of the watermarks' $WT_{LL, w}$.
- 5- Determine the watermarks' locations \perp_1 , and \perp_2 according to the values stored in the database (block number).
- 6- SVD is applied to the located blocks that contain the watermarks' coefficients to obtain \bar{S}_{I, C_b, B_i} , \bar{S}_{I, Y, B_i} that contain the singular values of the watermarks.
- 7- Retrieve the singular values of the dual watermarks' S_{w_1} , and S_{w_2} , then combining them with U and V vectors given from the database to get the LL band of each watermark WT_{LL, w_1} , and WT_{LL, w_2} . These matrices are extracted given both of S_{I, C_b, B_i} and S_{I, Y, B_i} that are previously stored in the database.

$$S_{w_1} = \frac{\bar{S}_{I,Cb,Bi} - S_{I,Cb,Bi}}{\Omega_{I,Cb,Bi}}, \quad S_{w_2} = \frac{\bar{S}_{I,Y,Bi} - S_{I,Y,Bi}}{\Omega_{I,Y,Bi}} \quad (16)$$

- 8- Given WT_{LL,w_1} , and WT_{LL,w_2} from the previous step, these bands are combined with their other three unaltered bands of the watermarks given from the database using inverse DWT to get the encoded watermarks (dual watermarks):

$$H_W(k) = \sum_{-\infty}^{\infty} \left((WT_{HH} + 1(k)g(-x + 2k)) + (WT_{LL} + 1(k)h(-x + 2k)) \right) \quad (17)$$

where H_W represent the encoded watermarks.

- 9- To acquire the dual watermarks, an inverse WHT is applied to acquire the watermarks \tilde{w}_1 and \tilde{w}_2 .

4 Experimental results

Experiments were conducted on a benchmark colour image dataset [42] as illustrated in Fig. 2. It is important to test an image watermarking software on many different images and for fair comparison the same set of sample images should always be used. Pictures can be interesting from the signal processing point of view: textured/smooth areas, size, synthetic, straight edges, sharp, blur, brightness/contrast, etc. They should also cover a broad range of contents and types. The database is divided into volumes based on the basic character of the pictures. Images in each volume are of various sizes such as 512×512 pixels, or 1024×1024 pixels. All images are 8 bits/pixel for black and white images, 24 bits/pixel for colour images. The following volumes are currently utilized that includes textures, aerials, [miscellaneous](#), [sequences](#). All images in the database are currently stored in PNG format. In this case, the images that are used as watermarks are converted to grey-scale version. In this paper, the suggested intelligent dual watermarking scheme that relies on genetic algorithms has been tested with several test images were each cover image has been tested at different sizes with different GA parameters to perceive the influence of these parameters on the model performance.

The suggested model has been implemented in MATLAB (R2015a) based on image processing and optimization toolboxes; running on a laptop computer (DELL 3000 Series) with the following specifications: Processor: Intel (R), Core (TM) i5 CPU, 5200 U @ 2.20 GHz (4CPUs) 2.20 GHz, RAM: 8 GB with Microsoft windows 10 Single language as running 64-bit operating system. PSNR (Peak Signal to Noise Ratio), and NCC (Normal Correlation Coefficient) were employed as criteria for performance evaluation. PSNR value shows the degree of alteration introduced to the original host image due to watermark insertion and NCC specifies the degree of resemblance between original watermark and extracted watermark [29, 46].

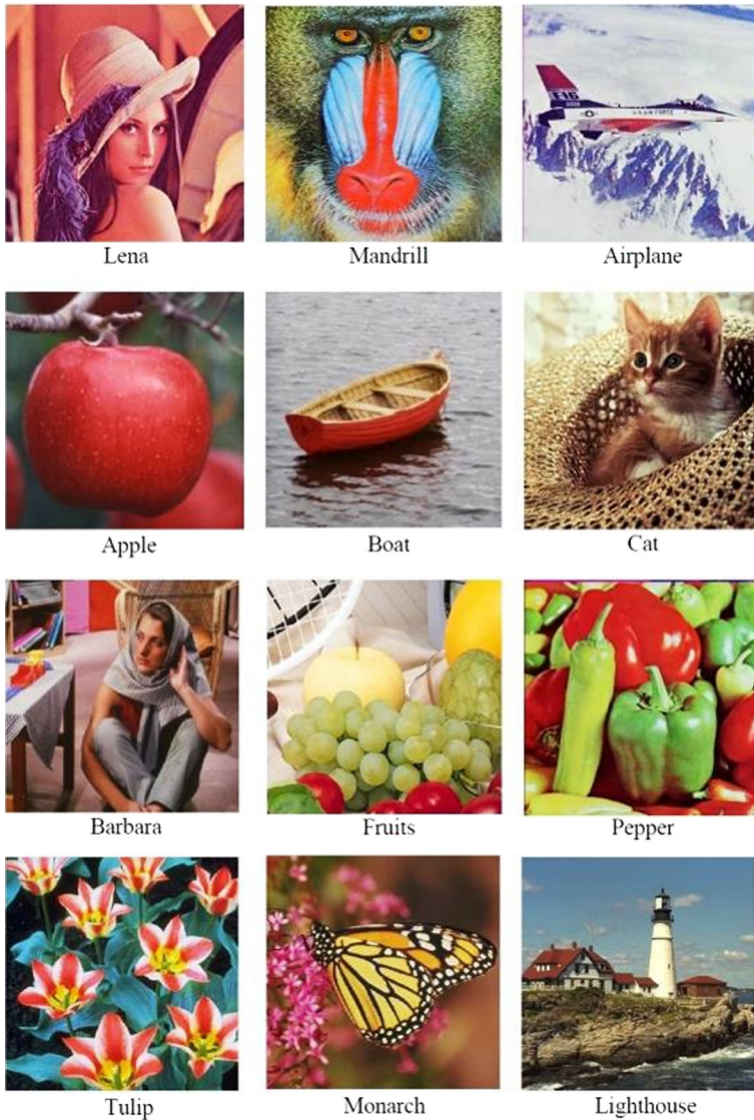
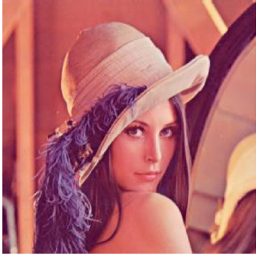


Fig. 2 Samples of Covers and Watermarks Dataset

Table 1 Genetic Algorithm Parameters

| Encoding Style | Binary Coding |
|------------------------|------------------------|
| Generation Number (GN) | Ranging from (5-50) |
| Population Size (PS) | Ranging from (5-50) |
| Crossover Rate | 0.7 |
| Type of Crossover | Single Point Crossover |
| Mutation Rate | 0.3 |
| Type of Mutation | Uniform Mutation |
| Selection Type | Tournament Selection |

Table 2 Watermarked Image Experimental Result

| Host Image | Watermarks | Watermarked Image | PSNR |
|---|---|---|----------------|
|  |  |  | 51.9496 |

$$PSNR = \left[\frac{255^2}{\frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (\bar{I}_{(x,y)} - I_{(x,y)})^2} \right] \tag{18}$$

where $I_{(x,y)}$ represent the original cover image, and $\bar{I}_{(x,y)}$ represent the watermarked image.

$$NCC = \frac{\sum_1^m \sum_1^n W_{(m,n)} \bar{W}_{(m,n)}}{\sqrt{\sum_1^m \sum_1^n W_{(m,n)}^2 \sum_1^m \sum_1^n \bar{W}_{(m,n)}^2}} \tag{19}$$

where $W_{(m,n)}$ represent the original watermark, and $\bar{W}_{(x,y)}$ represent the extracted watermark.

Table 3 Effect of Crossover and Mutation Rate of GA on Watermarking Imperceptibility


| Host Image | Size 1024 × 1024 | | PSNR | Size 512 × 512 | | PSNR |
|---|------------------|---------|---------|----------------|---------|---------|
| | GN | PS | | GN | PS | |
|  | 5 | 5 | 51.6957 | 5 | 5 | 51.9152 |
| | | 10 | 51.7170 | | 10 | 51.9225 |
| | | 20 | 51.7650 | | 20 | 51.9400 |
| | | 50 | 51.7425 | | 50 | 51.9233 |
| | | 5 | 51.6349 | | 10 | 5 |
| | 10 | 51.6923 | 10 | 51.9225 | | |
| | 20 | 51.7650 | 20 | 51.9400 | | |
| | 50 | 51.7425 | 50 | 51.9233 | | |
| | 5 | 51.6349 | 20 | 5 | | 51.9218 |
| | 10 | 51.6923 | | 10 | 51.9496 | |
| | 20 | 51.7650 | | 20 | 51.9400 | |
| | 50 | 51.7425 | | 50 | 51.9233 | |
| | 5 | 51.8039 | | 50 | 5 | 51.9360 |
| | 10 | 51.6923 | 10 | | 51.9496 | |
| | 20 | 51.7650 | 20 | | 51.9429 | |
| | 50 | 51.7425 | 50 | | 51.9233 | |

Table 4 Effect of Embedding Process in the Different Color Channels in Terms of PSNR

| Host Image | Y Channel | C_b Channel | C_r Channel |
|------------|-----------|---------------|---------------|
| Airplane | 52.105 | 52.330 | 52.068 |
| Pepper | 52.007 | 51.795 | 51.509 |
| Tulip | 51.930 | 51.895 | 51.878 |
| Lena | 51.277 | 51.844 | 51.135 |
| Mandrill | 51.657 | 51.778 | 51.352 |

Table 1 shows GA parameters that were taken for optimizing the suggested multiple watermarking scheme. It is clearly observed from Table 2 that the suggested system is imperceptible (subjective criteria).

4.1 Imperceptibility (quality) analysis- the effect of GA parameters

The first set of experiments was performed to show how the quality of the suggested model in terms of imperceptibility depends on GA parameters that includes Generation Number (GN), and Population Size (PS). The experiment was applied on Lena cover image with different sizes. Table 3 shows that the smaller the cover image's size, the better PSNR result is acquired.

Table 5 Dual Watermarking model Performance Evaluation with and without GA in Terms of PSNR (host image quality)















| Host Image (512×512) | without GA | | with GA | | |
|---|--|---------|---|---|----------------|
| | Scaling Factor (<i>Trial and Error</i>) | PSNR | Scaling Factor1 (<i>Optimized</i>) | Scaling Factor2 (<i>Optimized</i>) | PSNR |
|  | 0.01 | 40.0174 | 0.0037 | 0.0032 | 51.9496 |
| | 0.02 | 34.4952 | | | |
| | 0.03 | 31.4351 | | | |
|  | 0.01 | 41.4195 | 0.0037 | 0.0035 | 51.9762 |
| | 0.02 | 37.7022 | | | |
| | 0.03 | 35.3538 | | | |
|  | 0.01 | 40.0800 | 0.0036 | 0.0038 | 52.1654 |
| | 0.02 | 34.5613 | | | |
| | 0.03 | 31.3722 | | | |
|  | 0.01 | 35.0239 | 0.0035 | 0.0039 | 51.7724 |
| | 0.02 | 30.6110 | | | |
| | 0.03 | 29.5612 | | | |
|  | 0.01 | 35.8318 | 0.0037 | 0.0037 | 52.1086 |
| | 0.02 | 33.3917 | | | |
| | 0.03 | 31.4669 | | | |
|  | 0.01 | 34.4034 | 0.0040 | 0.0047 | 51.6666 |
| | 0.02 | 31.5886 | | | |
| | 0.03 | 28.8729 | | | |
|  | 0.01 | 35.6912 | 0.0039 | 0.0040 | 52.1726 |
| | 0.02 | 32.6490 | | | |
| | 0.03 | 31.6139 | | | |

Table 6 Dual Watermarking Model Performance Evaluation with and without GA in Terms of NCC (watermarks quality)

| Host Image (512×512) | without GA | | | with GA | | | |
|--|--|------------------|------------------|---|---|------------------|------------------|
| | Scaling Factor (<i>Trial and Error</i>) | NCC ₁ | NCC ₂ | Scaling Factor1 (<i>Optimized</i>) | Scaling Factor2 (<i>Optimized</i>) | NCC ₁ | NCC ₂ |
|  | 0.01 | 0.4757 | 0.5846 | 0.0037 | 0.0032 | 0.9999 | 0.9989 |
| | 0.02 | 0.4505 | 0.5844 | | | | |
| | 0.03 | 0.4425 | 0.5837 | | | | |
|  | 0.01 | 0.4270 | 0.6656 | 0.0037 | 0.0035 | 0.9979 | 0.9949 |
| | 0.02 | 0.4265 | 0.6640 | | | | |
| | 0.03 | 0.4258 | 0.6633 | | | | |
|  | 0.01 | 0.4270 | 0.5995 | 0.0036 | 0.0038 | 0.9939 | 0.9988 |
| | 0.02 | 0.4268 | 0.5987 | | | | |
| | 0.03 | 0.4263 | 0.5983 | | | | |
|  | 0.01 | 0.4295 | 0.5279 | 0.0035 | 0.0039 | 0.9969 | 0.9968 |
| | 0.02 | 0.4283 | 0.5272 | | | | |
| | 0.03 | 0.4278 | 0.5260 | | | | |
|  | 0.01 | 0.4943 | 0.5304 | 0.0037 | 0.0037 | 0.9959 | 0.9994 |
| | 0.02 | 0.4938 | 0.5296 | | | | |
| | 0.03 | 0.4931 | 0.5278 | | | | |
|  | 0.01 | 0.6061 | 0.5275 | 0.0040 | 0.0047 | 0.9990 | 0.9992 |
| | 0.02 | 0.6053 | 0.5268 | | | | |
| | 0.03 | 0.6032 | 0.5257 | | | | |
|  | 0.01 | 0.6344 | 0.5435 | 0.0039 | 0.0040 | 0.9988 | 0.9990 |
| | 0.02 | 0.6332 | 0.5423 | | | | |
| | 0.03 | 0.6312 | 0.5408 | | | | |

On average, an increasing of 0.3% PSNR was *obtained* by reducing the cover image to half size. One possible explanation for this result is that smaller size is associated with smaller search space; so that GA can acquire optimal solution [21]. It is also clear from the Table that the increase in population size has a limited effect on number of optimal solution in terms of PSNR when the number of generations is constant. There is an increase with approximately 0.02 with each increase of 5 for the size of the population. Regarding the effect of the number of generations on the convergence to the optimal solution; in spite of the fact that the more the number of generations, the more diversity of the population and therefore the chances of obtaining a better solution are high. There is no significant increase in the PSNR values when generation number increases. One possible explanation of this result is that, populations diversity often is stabilized after a certain generation, in the sense that solution with high fitness are obtained from the previous generations.

4.2 Imperceptibility analysis- the effect of colour channels

The second set of experiments was conducted to show how the PSNR values of the suggested model depend on the embedding in different colour channels in order to determine the most

suitable colour channels for the embedding process. It can be inferred from Table 4 that higher PSNR values are achieved in both of Y and C_b colour channels. For all test images, PSNR values are good and greater than the accepted ratio 30 and the differences between these values are small and negligible. One explanation of this result is that most of the visible information is in the Y channel (carry the intensity value of the pixel) and human eyes tolerate both lower spatial resolution and more aggressive quantization in the C_b and C_r channels that contains colour information of the pixel. Of course, the difference in the nature of the images in terms of degrees of colour leads to the preference of a colour channel over the other in the embedding. The proposed model depends on the color channels that achieve the highest PSNR in the embedding of dual watermarks. As stated in [5], the non-uniform colour spaces such as YC_bC_r colour space indeed provide a large amount of perceptual redundancy for embedding high-strength watermarking signals which can survive various attacks.

4.3 Imperceptibility analysis- the role of GA

The third set of experiments was implemented to illustrate the difference between embedding the watermarks at random locations with constant scaling factor that is identified by experts and the use of GA in the suggested model to find the optimality of these issues. As shown in Tables 5 and 6, the use of GA to find the optimal values of both scaling factor and embedding locations gives superiority results in terms of PSNR as compared with random values. Herein, the objective function comprises both of PSNR and NCC as a criteria to select the search space. The use of both PSNR and NCC achieve optimal quality in terms of imperceptibility by reducing the difference in pixels values between the cover image and the watermarked image. The use of GA improved the model performance in terms of PSNR and 30% for Lena image, 25% for Mandrill image. The average improvement in terms of image quality through employing GA for embedding is around 39%. This difference in PSNR values is due to the different contents of the image according to their colour characteristics. For watermarks quality in terms of NCC, utilizing GA improves the performance by average 60% in case of selecting embedding factors randomly. All GAs demand some compose of recombination, as this permit

Table 7 Comparison Results between Different Dual Watermarking approaches in Terms of PSNR and NCC without Attacks

| Images (512×512) | N. Mohananthini approach [34] | | | | C. Kumar et al. approach [54] | | | Proposed Dual Watermarking System | | |
|-----------------------------|-------------------------------|--------------------------------------|------------------------|--------------------------------------|-------------------------------|------------------|------------------|--|------------------|------------------|
| | Successive (re-) Watermarking | | Segmented Watermarking | | Segmented Watermarking | | | Hybrid Watermarking (Successive and Segmented) | | |
| | PSNR | NCC ₁ NCC ₂ | PSNR | NCC ₁ NCC ₂ | PSNR | NCC ₁ | NCC ₂ | PSNR | NCC ₁ | NCC ₂ |
| Lena | 37.9677 | 1 | 39.9373 | 1 | N/A | N/A | N/A | 51.9496 | 0.9999 | 0.9989 |
| Mandrill | 38.0453 | 1 | 40.0432 | 1 | 35.52 | 0.9990 | 0.9513 | 51.9762 | 0.9979 | 0.9949 |
| Pepper | 38.0328 | 1 | 40.0338 | 1 | N/A | N/A | N/A | 52.1654 | 0.9939 | 0.9988 |
| Airplane | 37.2668 | 1 | 39.6659 | 1 | N/A | N/A | N/A | 52.0803 | 0.9959 | 0.9994 |
| Barbara | 37.9993 | 1 | 39.9893 | 1 | 30.81 | 0.9999 | 0.9548 | 51.7115 | 0.9969 | 0.9987 |
| Apple | 37.9982 | 1 | 39.9983 | 1 | N/A | N/A | N/A | 51.6666 | 0.9990 | 0.9992 |
| Boat | 37.6514 | 1 | 39.6411 | 1 | 33.68 | 0.9999 | 0.9548 | 51.1578 | 0.9988 | 0.9990 |

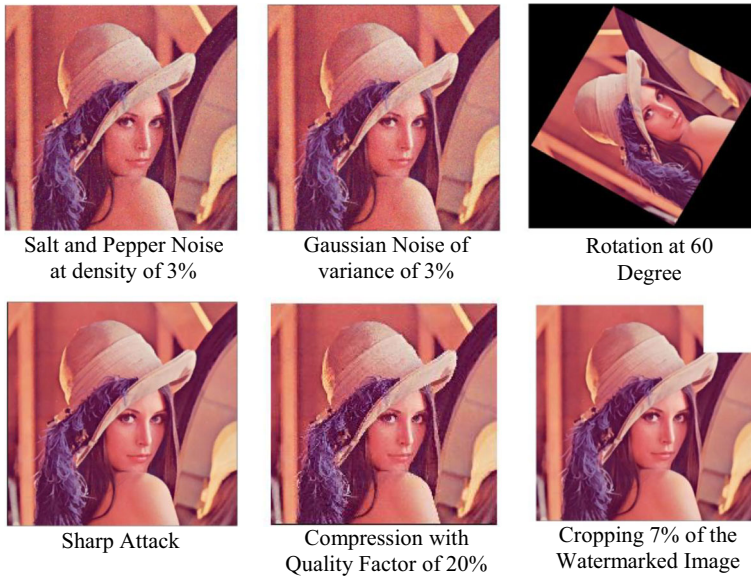














Fig. 3 Common Attacks

Table 8 PSNR Values for Multiple Watermarking Techniques under Different Attacks with different host images

| Attacks | Images | N. Mohananthini Approach [34] | | S. Vaidya Approach [50] | Proposed Model |
|-----------------------|----------|-------------------------------|-----------------------------|-----------------------------|---|
| | | Successive watermarking PSNR | Segmented watermarking PSNR | Segmented Watermarking PSNR | Hybrid watermarking (successive and segmented) PSNR |
| Salt and Pepper noise | Lena | 21.3882 | 21.3710 | N/A | 21.5771 |
| | Mandrill | N/A | N/A | N/A | 21.5635 |
| | Pepper | N/A | N/A | N/A | 21.4882 |
| Gaussian Noise | Lena | 21.2456 | 21.2425 | 20.10 | 21.2801 |
| | Mandrill | N/A | N/A | 20.15 | 21.2755 |
| | Pepper | N/A | N/A | 20.75 | 21.2701 |
| Speckle Noise | Lena | 28.6274 | 28.9107 | 27.88 | 28.9747 |
| | Mandrill | N/A | N/A | 27.80 | 28.8923 |
| | Pepper | N/A | N/A | 27.10 | 28.8726 |
| Cropping | Lena | 18.7839 | 18.8023 | N/A | 19.1883 |
| | Mandrill | N/A | N/A | N/A | 19.0726 |
| | Pepper | N/A | N/A | N/A | 19.0788 |
| Rotation | Lena | 9.8067 | 8.5919 | 8.53 | 9.8419 |
| | Mandrill | N/A | N/A | 8.02 | 9.7362 |
| | Pepper | N/A | N/A | 8.45 | 9.6928 |
| JPEG Compression | Lena | 37.4234 | 37.7035 | N/A | 37.8427 |
| | Mandrill | N/A | N/A | N/A | 37.8324 |
| | Pepper | N/A | N/A | N/A | 37.8316 |
| Sharpening | Lena | 25.3802 | 23.9824 | N/A | 34.9838 |
| | Mandrill | N/A | N/A | N/A | 34.8942 |
| | Pepper | N/A | N/A | N/A | 34.8625 |

Table 9 NCC Values for Multiple Watermarking Techniques under Different Attacks with different host images 512 × 512

| Attacks | Images | N. Mohananthini Approach | | | | S. Vaidya Approach | Proposed Model | |
|-----------------------|----------|--------------------------|------------------|------------------------|------------------|------------------------|---|--|
| | | [36] | | | | [35] | Hybrid watermarking (successive and segmented) | |
| | | Successive watermarking | | Segmented watermarking | | Segmented Watermarking | | |
| | | NCC ₁ | NCC ₂ | NCC ₁ | NCC ₂ | NCC _{1,2} | NCC ₁ | NCC ₂ |
| Salt and pepper noise | Lena | 0.8120 | 0.9918 | 0.8856 | 0.9978 | 0.9678 |  0.9977 |  0.9900 |
| | Mandrill | N/A | N/A | N/A | N/A | 0.9687 | 0.9981 | 0.9974 |
| | Pepper | N/A | N/A | N/A | N/A | 0.9688 | 0.9986 | 0.9980 |
| Gaussian noise | Lena | 0.7891 | 0.9906 | 0.8769 | 0.9743 | 0.9676 |  0.9570 |  0.9338 |
| | Mandrill | N/A | N/A | N/A | N/A | 0.9638 | 0.9598 | 0.9583 |
| | Pepper | N/A | N/A | N/A | N/A | 0.9654 | 0.9592 | 0.9583 |
| Cropping | Lena | 0.3360 | 0.9970 | 0.3833 | 0.3441 | N/A |  0.8869 |  0.9509 |
| | Mandrill | N/A | N/A | N/A | N/A | N/A | 0.8852 | 0.9626 |
| | Pepper | N/A | N/A | N/A | N/A | N/A | 0.8717 | 0.9618 |
| Rotation | Lena | 0.1364 | 0.9736 | 0.1240 | 0.1187 | 0.9652 |  0.4117 |  0.6323 |
| | Mandrill | N/A | N/A | N/A | N/A | 0.9661 | 0.4536 | 0.6882 |
| | Pepper | N/A | N/A | N/A | N/A | 0.9668 | 0.4673 | 0.68715 |
| JPEG compression | Lena | 1 | 0.9652 | 1 | 1 | N/A |  0.9747 |  0.9568 |
| | Mandrill | N/A | N/A | N/A | N/A | N/A | 0.9867 | 0.9634 |
| | Pepper | N/A | N/A | N/A | N/A | N/A | 0.9688 | 0.9587 |
| Sharpening | Lena | 0.8000 | 1 | 0.9078 | 0.9655 | N/A |  0.9096 |  0.9998 |
| | Mandrill | N/A | N/A | N/A | N/A | N/A | 0.9388 | 0.9998 |
| | Pepper | N/A | N/A | N/A | N/A | N/A | 0.9478 | 0.9999 |

the ingenuity of new solutions that have, by virtue of their parent’s success, a higher probability of showing a good performance. In GA, diversification tries to explore the search space more efficiently by generating solutions with higher diversity. This diversity is achieved by discovering the search space (solutions) that have highest objective function.

4.4 Imperceptibility analysis- comparative study

The fourth set of experiments was performed to compare the imperceptibility performance (with attacks) of the suggested dual hybrid watermarking system (successive and segmented) that employs GA to find the optimal embedding locations and scaling factors with related dual watermarking approaches that includes (1) N. Mohananthini approach [34] in which dual watermarking technique for both successive and segmented watermarking is applied separately based on image salient features extracted from DWT – SVD. This approach employed GA to find optimal scaling factor only. (2) S. Vaidya approach [50] in which dual watermarking technique for successive watermarking only is applied based on DWT-SVD for determining embedding locations. Finally (3) C. Kumar et al. approach [26] in which dual watermarking technique for segmented watermarking only is applied based on Non-Subsampled Contourlet Transform for determining embedding locations. As shown in Table 7, the proposed dual watermark approach achieves 37.1% improvement in terms of PSNR (cover image quality) compared to the other approaches that outperform in many cases with a very small ratio in terms of NCC (watermark quality) as compared with suggested model.

One possible explanation for this improvement is that the merge of the two watermarking techniques yields a solution to the issue of watermarks interference with each other. Furthermore, the suggested model is based on embedding the watermarks in the most suitable locations with optimal scaling factors, which is not presented in the other models that determines the optimal scaling factor only. However, the overlap between different embedding techniques as in the proposed model may cause some problems in locations' determination for watermarks extraction process; this may happen in simple cases which consequently decreases the NCC percentage. The other approaches relies on utilizing one watermarking technique to apply the dual watermarking, that embed watermarks in spaced locations without considering the quality of the host image.

4.5 Attacks Analysis

The fifth set of experiments was implemented to validate the robustness of the suggested model against different types of attacks. Different types of attacks as shown in Fig. 3 were implemented on the watermarked image. Tables 8 and 9 summarize the results in

Table 10 Statistical Inferences for NCC Values for the watermarks Images

| | Hybrid Watermarking (Successive and Segmented) | | | |
|-------------------------|--|----------------------|----------------------|----------------------|
| | without GA | | with GA | |
| | Extracted Watermark1 | Extracted Watermark2 | Extracted Watermark1 | Extracted Watermark2 |
| Sample Mean | 0.4956 | 0.5675 | 0.8766 | 0.9223 |
| Sample Variance | 0.0183 | 0.0083 | 0.0375 | 0.0145 |
| Sample Size | 7 | 7 | 7 | 7 |
| Calculated Value of t | - 0.0152 | | - 0.0312 | |
| Table Value of t | 1.895 | | 1.895 | |
| Result of Hypothesis | H_0 | | H_0 | |

terms of PSNR for the watermarked image and NCC for the watermarks for both the suggested model and the comparative approaches. The results confirm that the robustness of proposed model is superior to the existing methods for different cases with improvement of about 0.8% in terms of PSNR. The results also clarified that the rotation attack has achieved the least PSNR value as it changes the pixels' locations and consequently loss the synchronization between the original watermarks' locations and the stored locations in the database. Whereas, the JPEG compression attack has achieved the highest PSNR value as this type of attack is usually applied to the high-frequency components, on the contrary the proposed model embeds the dual watermarks in the low-frequency components; so that this attack has no significant impact on the quality of the watermarked image and the watermarks. In common, simple attacks like noises attempt to damage the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. From Table 9, as expected, the comparative approaches outperform with a very small ratio (0.8%) in terms of NCC (watermark quality) for different type of attacks as compared with suggested model. This is due to problems in locations' determination for watermarks extraction process; interference between embedding processes. The difference in the NCC values for the extracted watermarks form the same cover image is due to the nature of the characteristics of the image. Note that the correlation ratio between the extracted watermarks and the original ones is high in the presence of attacks because the suggested model determines the embedding parameters based on a fitness function that relies on NCC, which compare between the quality of the image before and after attacks in order to select the best parameters able to stand against attacks.

4.6 Statistical analysis

The following set of experiments was performed to determine the statistical inferences that are carried out for the multiple watermarking techniques with and without genetic algorithm. Table 10 gives the statistical inferences for the NCC values from the results given in Table 6 and Table 9 for different attacks, while Table 11 gives the statistical inferences for the PSNR values from the results given in Table 5 and Table 8 for different attacks. In this case, H_0 represents the hypothesis that the multiple watermarking techniques with genetic algorithm is better and H_1 represents the hypothesis that the multiple watermarking techniques without genetic algorithm is better. From Table 10 and Table 11, it is observed that the calculated value is less than the t table value at 5% level of significance; so the proposed model accept the H_0 and it is concluded that the multiple watermarking techniques with genetic algorithm is found to be better. The improvement resulting from the use of GA is due to the GA ability to balance between the exploitation and the exploration to optima the best values of scaling factor and embedding locations [33] [52]. Exploitation means that given a reasonable solution, the algorithm will keep refining that solution until it reaches a local optimum. While the exploration means that the algorithm will attempt to achieve a good coverage of the search space, so that it will not eventually find just any local optimum, but a good local optimum, ideally one that is close to the global optimum. However, it cannot be equated these two notions with the crossover and mutation functions. Both have effects that work towards both exploitation and exploration. The choice of which genes die and which get to reproduce also has a large influence on this balance.

Table 11 Statistical Inferences for PSNR Values for Lena Cover Image

| | Hybrid Watermarking (Successive and Segmented) | |
|-------------------------|--|---------|
| | without GA | with GA |
| Sample Mean | 21.1496 | 24.8126 |
| Sample Variance | 6.8571 | 7.5714 |
| Sample Size | 7 | 7 |
| Calculated Value of t | - 0.5013 | |
| Table Value of t | 1.895 | |
| Result of Hypothesis | H_0 | |

4.7 Time complexity analysis

The last set of experiments was conducted to evaluate the complexity of the suggested model. Time complexity analysis is a part of computational complexity theory that is used to describe an algorithm's use of computational resources; in most cases, the worst case running time expressed as a function of its input using big- O notation [15]. As the proposed system was built using Matlab, which in turn depends on calling many built-in functions, therefore, it is difficult to extract the big- O , herein; time was used as a measurement to evaluate the complexity of the system. As shown in Table 12, more processing time is needed for the suggested model as compared to the successive watermarking by 19.38%. More specifically, the suggested model takes about 2.654468 s for the embedding process and takes about 0.678911 s for the extraction process; thus, the time of extraction process is roughly equivalent to one fifth of the time of embedding process. In general, this relatively large time in the embedding process represents the offline phase of the proposed model. Consequently, the proposed model is applicable in real-time applications. A possible explanation is that the suggested model relies on a hybrid watermarking technique, unlike the other approaches that relies on embedding multiple watermarking based on single technique. This extra time has been used to improve the efficiency of the proposed model in terms of robustness against the attacks and imperceptibility.

4.8 Limitation of the suggested model

In general, the application of the proposed dual watermarking model faces some constraints that includes (1) the segmentation operation is built using square sized images, (2) the watermarks are grey scale images for simple embedding, finally (3) extra memory space are needed to store some information that are used in the extraction process as the suggested model is semi-blind.

5 Conclusion

The design of suitable dual watermark embedding involves multiple criteria and specifications. Finding suitable embedding locations and optimal embedding strength are, therefore, not a

Table 12 Average Time Consumed for the Whole System Performance in Seconds

| Time in Seconds | N. Mohananthini Approach [34] | | Proposed Model Hybrid Watermarking |
|-----------------|-------------------------------|------------------------|---------------------------------------|
| | Successive Watermarking | Segmented Watermarking | |
| | 2.792121 | 7.503938 | 3.333379 |

simple task. In recent times, the merging of optimization techniques with the image watermarking scheme to improve its performance and effectiveness in different areas has received considerable attention among researchers working in this field. Inspired by the challenges that faced the dual image watermarking and in order to deal with it, in this paper, a novel model has been established to produce an intelligent dual watermarking scheme for colour images that guarantee the possibility of protecting the rights of ownership and publication and to be used effectively in different applications, that take into account the image quality. Herein, multi-purpose genetic algorithm is utilized to optimize watermarking embedding parameters to achieve robustness and imperceptibility.

The suggested model achieves high capacity (Payload). Studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness. The main two issues of complexity are the speed of embedding and detection, and the number of embedders and detectors; the suggested model has low complexity. The proposed model has been evaluated using benchmark images. The results confirmed the capability of the proposed model in terms of robustness and imperceptibility. Utilizing genetic algorithm achieves 23% improvement in terms of peak signal to noise ratio compared to the traditional non-optimized dual watermarking methods. To set a plan for future works, the suggested model can be upgraded to exploit other color spaces that could improve the performance such as YUV, and CMYK. More features can be investigated in order to enhance the performance of the dual watermarking schemes by combining the DWT with other transforms. Furthermore, GA can be replaced with another appropriate optimization method to fine tuning watermarking embedding parameters. Finally, link the proposed model to the modern applications of e-business such as Blockchain.

References

1. Aakanksha T, Gupta B (2017) A Lightweight Mutual Authentication Protocol based on Elliptic Curve Cryptography for IOT Devices. *International Journal of Advanced Intelligence Paradigms* 9(2-3):111–121
2. Abdallah E, Hamza A, Bhattacharya P (2007) MPEG Video Watermarking using Tensor Singular Value Decomposition. *International Conference Image Analysis and Recognition*:772–783
3. Abdallah E, Hamza A, Bhattacharya P (2010) Video Watermarking using Wavelet Transform and Tensor Algebra. *SIViP* 4(2):233–245
4. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based Steganography Using Truth Table Based and Determinate Array on RGB Indicator. *International Journal of Signal and Image Processing* 1(3):196–204
5. J. Advith, K. R. Varun, and K. Manikantan, "Novel Digital Image Watermarking using DWT-DFT-SVD in YC_bC_r Color Space", *Proceedings of the IEEE International Conference on Emerging Trends in Engineering, Technology and Science*, pp. 1-6, India, Feb. 2016.
6. Alanizy N, Alanizy A, Baghoza N, Al Ghamdi M, Gutub A (2018) 3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography. *Journal of Research in Engineering and Applied Sciences* 3(4):118–124
7. Alaseri K, Gutub A (2018) Merging Secret Sharing Within Arabic Text Steganography for Practical Retrieval. *Journal of Computer Science Engineering* 4(9):1–7
8. Al-Ghamdi M, Al-Ghamdi M, Gutub A (2019) Security Enhancement of Shares Generation Process for Multimedia Counting-based Secret-Sharing Technique. *Multimed Tools Appl* 78(12):16283–16310
9. Al-Juaid A, Gutub A, Khan A (2018) Enhancing PC Data Security Via Combining RSA Cryptography and Video based Steganography. *Journal of Information Security and Cybercrimes Research (JISCR)* 1(1):8–18
10. Almazrooie M, Samsudin A, Gutub A, Salleh M, Omar M, Hassan S (2018) Integrity verification for digital Holy Quran verses using cryptographic hash function and compression, *Journal of King Saud University - Computer and Information Sciences*, Published by Elsevier, Published online: 8
11. Al-Otaibi N, Gutub A (2014) 2-Layer Security System for Hiding Sensitive Text Data on Personal Computers. *Lecture Notes on Information Theory* 2(2):151–157

12. Al-Otaibi N, Gutub A (2014) Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority. Proceedings of International Conference on Advanced Engineering Technologies (AET-2014), pp. 250-256, UAE, 25-26 December
13. Alsaïdi A, Al-lehaibi K, Alzahrani H, AlGhamdi M, Gutub A (2018) Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics* 8(3):33–42
14. Bthial M, Hassan N (2017) Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment. *International Journal of Cloud Applications and Computing* 7(2):27–40
15. Chetan KR, Nirmala S (2016) A Novel Intelligent Multiple Watermarking Schemes for the Protection of the Information Content of a Document Image. Proceedings of the International Conference on Computer Vision, Graphics, and Image processing, pp. 3-14, India.
16. Espinoza KR, Navarro EF, Ramos CC, Reyes RR, Miyatake MN, Meana HP (2018) Adaptive Removable Visible Watermarking Technique using Dual Watermarking for Digital Colour Images. *Multimed Tools Appl* 77(11):13047–13074
17. Gen WY, Xie D, Gupta BB (2018) A Study on the Collusion Security of LUT-based Client-Side Watermark Embedding. *IEEE Access* 6:15816–15822
18. Gupta BB (2018) *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. CRC Press, Taylor & Francis, 666
19. Gupta B, Agrawal D, Yamaguchi S (2016) *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. IGI Global
20. Gutub A (2010) Pixel Indicator Technique for RGB Image Steganography. *Journal of Emerging Technologies in Web Intelligence* 2(1):56–64
21. Gutub A, Al-Ghamdi M (2019) Image based Steganography to Facilitate Improving Counting-based Secret Sharing. *3D Res* 10(6):1–36
22. Gutub A, Al-Juaïd N (2018) Multi-Bits Stego-System for Hiding Text in Multimedia Images based on User Security Priority. *Journal of Computer Hardware Engineering* 1(2):1–9
23. Gutub A, Al-Juaïd N, Khan E (2019) Counting-based Secret Sharing Technique for Multimedia Applications. *Multimed Tools Appl* 78(5):5591–5619
24. Gutub A, Al-Qahtani A, Tabakh A (2009) Triple-A: Secure RGB Image Steganography based on Randomization. Proceedings of 7th ACS/IEEE International Conference on Computer Systems and Applications, pp. 400-403, Morocco, 10-13 May
25. Gutub M, Ankeer M, Abu-Ghalioun A, Alvi A (2008) Pixel Indicator high capacity Technique for RGB image based Steganography, *IEEE International Workshop on Signal Processing and its Applications*, pp. 1-4, U.A.E. 18-20 March
26. Kumar C, Singh AK, Kumar P, Singh R (2018) A Low Complexity Secure Force Encryption based Multiple Image Watermarking in NSCT Domain. Proceedings of the 2nd IEEE International Conference on Advances in Computing, Control and Communication Technology, pp. 92-96
27. Li D, Deng L, Gupta B, Wang H, Choi C (2019) A Novel CNN Based Security Guaranteed Image Watermarking Generation Scenario For Smart City Applications. *Inf Sci* 479:432–447
28. Li J, Yu C, Gupta B, Ren X (2018) Colour Image Watermarking Scheme based on Quaternion Hadamard Transform and Schur Decomposition. *Multimed Tools Appl* 77(4):4545–4561
29. Liao HW (2012) A Multiple Watermarking Scheme for Colour Images, Proceedings of the 3rd IEEE International Conference on Mobile, Ubiquitous, and Intelligent Computing, pp. 132-137, Canada
30. Liu J, Huang J, Luo Y, Cao L, Yang S, Wei D, Zhou R (2019) An Optimized Image Watermarking Method based on HD and SVD in DWT Domain. *IEEE Access* 7:80849–80860
31. Liu XL, Lin CC, Yuan SM (2016) Blind Dual Watermarking for Colour Images' Authentication and Copyright Protection. *International Journal of IEEE Transactions on Circuits and Systems for Video technology* 26(3):1–9
32. Lusson F, Bailey K, Leeney M, Curran K (2013) A Novel Approach to Digital Watermarking Exploiting Colour Spaces. *International Journal of Signal Processing* 93(5):1268–1294
33. Mathivadhani D (2012) *Multiple Watermarking Approaches using Enhanced Image Processing Techniques and Visual Cryptography*. Master Thesis, Department of Computer Science, Avinashilingam Institute for Home science and Higher Education, India
34. Mohananthini N (2015) *Analysis of Multiple Watermarking using Images*. Master Thesis, Department of Electrical Engineering, faculty of Engineering and Technology, Annamalai University, India
35. Mohananthini N, Yamuna G (2016) Comparison of Multiple Watermarking Techniques using Genetic Algorithm. *Journal of Electrical Systems and Information Technology* 3(1):68–80
36. Moosazadeh M, Andalib A (2016) A New Robust Colour Digital Image watermarking Algorithm in DCT Domain using Genetic Algorithm and Coefficients Exchange Approach, Proceedings of the 2nd International Conference of Web Research (ICWR), pp. 19-24, Iran

37. Natarajan M, Govindarajan Y (2014) Performance Comparison of Single and Multiple Watermarking Techniques. *International Journal of Computer Network and Information Security* 6(7):28–34
38. Ouazzane H, Mahersia H, Hamrouni K (2013) A Robust Multiple Watermarking Scheme based on the DWT. *Proceedings of the 10th IEEE International Multi-Conference on Systems, Signals & Devices*, pp. 1–6, Tunisia
39. Ouazzane H, Mahersia H, Hamrouni K (2013) A Robust Multiple Watermarking Scheme based on the DWT. *Proceedings of the 10th IEEE International Multi-Conference on Systems, Signals & Devices*, pp. 1–6
40. Parvathavarthini S, Shanthakumari R (2014) An Adaptive Watermarking Process in Hadamard Transform. *International Journal of Advanced Information Technology* 4(2):1–7
41. Parvez M, Gutub A (2011) Vibrant Colour Image Steganography using Channel Differences and Secret Data Distribution. *Kuwait Journal of Science and Engineering* 38(1B):127–142
42. Public-Domain Test Images for Home works and Projects. Available at: <https://homepages.cae.wisc.edu/~ece533/images/>
43. Radharani S, Valarmathi ML (2011) Multiple Watermarking Scheme for Image Authentication and Copyright Protection using Wavelet based Texture Properties and Visual Cryptography. *Int J Comput Appl* 23(3):29–36
44. Sejal S, Shah N (2016) A Novel Multiple Objective Optimized Dual Watermarking Scheme based on DWT-SVD using Firefly Algorithm", *Proceedings of the IEEE International Conference on Computing, Analytics and Security Trends*, pp. 46–51, India
45. Sejal S, Shah N (2016) A Novel Multiple Objective Optimized Colour Watermarking Scheme based on LWT-SVD Domain using Nature based Bat Algorithm and Firefly algorithm. *Proceedings of the 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology*, pp. 38–44, India
46. Singh S, Arya RK, Sharma H (2016) A Robust De-interlacing Multiple Image Watermarking Technique in DWT. *Proceedings of the IEEE International Conference on Computational Techniques in Information and Communication Technologies*, pp. 8–13
47. Soni N, Kumar T (2014) Study of Various Crossover Operators in Genetic Algorithms. *International Journal of Computer Science and Information Technologies* 5(6):7235–7238
48. Takore T, Kumar P, Devi G (2016) Efficient Gray Image Watermarking Algorithm based on DWT-SVD using Genetic Algorithm, *Proceedings of the IEEE International Conference on Information Communication and Embedded System*, pp. 1–6, India
49. Takore T, Kumar P, Devi G (2018) A Robust and Oblivious Grayscale Image Watermarking Scheme based on Edge Detection, SVD, and GA. *Lecture Notes in Electrical Engineering* 434:51–61
50. S. Vaidya, "Multipurpose Color Image Watermarking in Wavelet Domain using Multiple Decomposition Techniques", *Proceedings of the 2nd IEEE International Conference on Inventive Communication and Computational Technologies*, pp. 251–255, India, 2018.
51. Vinothini K, Mydhili S, Periyanyagi S, Sukanya G (2019) Dual Watermarking in Tele-radiology using DWT for Data Authentication and Security. *Proceedings of the 8th IEEE International Conference on Communication and Signal Processing*, pp. 887– 891
52. Wang Y, Yang C, Zhu C, Ren N, Chen P (2016) A Novel Multiple Watermarking Algorithm based on Correlation Detection for Vector Geographic Data. *Proceedings of the International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystems*. pp. 429–436. Springer. Singapore
53. Wirayuda T, Winanjuar SD, Muslimah U (2012) The Multiple Watermarking on Digital Medical Image for Mobility and Authenticity. *Proceedings of Operations Research*:457–462
54. Zhang J, Gao H (2019) A Compact Construction for Non-Monotonic Key-Policy Attribute-based Encryption. *International Journal of High Performance Computing and Networking* 13(3):321–330



Saad M. Darwish received the B.Sc. degree in Statistics and Computer Science from the Faculty of Science, Alexandria University, Egypt in 1995. He held the M.Sc. degree in information technology from the Institute of Graduate Studies and Research (IGSR), Department of Information Technology, University of Alexandria in 2002. He received his Ph.D. degree from the Alexandria University for a thesis in image mining and image description technologies. He is the author or coauthor of 50+ papers publications in prestigious journals and top international conferences and also received several citations. He has served as a Reviewer for several international journals and conferences. He has supervised around 60 M.sc and Ph.D. students. His research and professional interests include image processing, optimization techniques, security technologies, database management, machine learning, biometrics, digital forensics, and bioinformatics. Since June 2017, he has been a Professor in the department of information technology, IGSR.



Layth Dhafer Shukur Al-Khafaji received the B.Sc. degree in Computer Technical Engineering from Dijlah University College, Iraq in 2013. He held the M.Sc. degree in image processing from the Institute of Graduate Studies and Research (IGSR), Department of Information Technology, University of Alexandria in 2018. His research and professional interests include image processing, optimization techniques, security technologies, Computer Communications, database management, machine learning, biometrics, and bioinformatics.