Frequency Domain for Color Image Authentication Proofing

Sabah Karri Gaid, Khalid Kadhim Jabbar
Department of Computer Science, Mustansiriyah University, College Of Education
khalid_jabbar@yahoo.com, Sabah9375@gmail.com

Abstract Digital watermarking is the process of embedding data known as a watermark into a multimedia object so that the watermark can later be identified or recovered to claim its object. The use of an embedded watermark would enable the owner of the work hardware to be identified. In the proposed method the Particle-Swarm-Optimization (PSO) algorithm has been applied to embed a binary watermark bit in the optimal color sub-bands, resulting in a less extreme value after the PSO point. The embedding level, which uses Discrete Wavelet Transform (DWT) to embed binary bits in the resulted image in the low-frequency domain, must be able to withstand intended attacks while maintaining high quality, as well as assess image authentication and localize tampering areas (s). Various consistency metrics and waveform removal attacks are used to evaluate the algorithm in an experimental environment. The results show that the model can support imperceptible watermarking as well as high attack resistance.

Keywords Watermark, Binary Image, Color Images, Authentication, Frequency Domain, Dwt, Pso

1. INTRODUCTION
Today, image Authentication plays an important role in most all practicability applications, like the military, the medical industry, and broadcasting. Digital images are simple to manipulate using sophisticated image editing software. Therefore, becomes an important area of study [1]. Image authentication is the application of image processing and domain knowledge to decide whether an image or video is a reasonable representation of the real picture. It could be said that schemes try to improve trust by properly validating the data[2]. Data protection and network security concerns must be resolved to avoid unauthorized access to the information of customers. It is a necessity to prevent misuse of data online. To safeguard confidential information, methods such as encryption, decryption, crypography, steganography, and digital watermarking are utilized[3,4].

According to a recent study, digital watermarking is the most suitable technique of image authentication. Watermarking method for authentication purposes can be categorized as fragile, half-fragile, and robust. A watermark is used to fortify the security and authenticity of data, images, and video files[5]. A fragile watermark is protected and already replaceable even at small accidental or intentional interventions. Besides, this is something commendable in Islam because according to legal rule “prevention is better than cure” and “there should be neither damaged nor reciprocating injury”. Therefore watermarking techniques can be used in image and video encoding/decoding, [6,7]. The proposed method aimed to embed the binary watermark bits in the optimal color sub-bands based on Particle-Swarm-Optimization (PSO) algorithm that produce the less extreme value after the PSO stage. The embedding stage using DWT is used to embed the binary bits in the resulted image in the
low-frequency domain, these processes lead to the produce watermarked image has to have the ability to survive an intended attack with high quality, it should be able to assess image authentication and localize tampering area(s).

1.1. Theoretical consideration

Some many technologies and algorithms have been included in the stages of the CAD system in this part. We will look at some of the techniques that were used in our proposed method to extract and select features.

1.1.1. Digital Watermarking
digital watermarking is an efficient way of preserving the copyright of image files. The principle of integrating a special pattern (watermark) into the host signal ensures that certain information, such as the identity of the owner or the approved user, is indissolubly linked to the data[8].

Watermarking is the process of integrating data into a multimedia object called a watermark, tag, or label so that an object, audio, image, or video as shown in fig can be identified or extracted later to claim the object, for instance. If the object is copied, it also carries the knowledge in a copy [9]. The detail is available in the image or video with the visible watermark. The data is typically a textural or a logo representing a media. The photo to the right has a clear watermark. When a TV broadcaster attaches its logo to the corner of the video, it’s also a clear watermark. Knowledge is applied to audio, image, or video as digital data in invisible watermarking, but can not be seen as such (although it is possible to detect the hidden information). A significant added to copyright protection mechanisms that prevent or discourage unauthorized copying of digital media is invisible watermarking. Steganography is often used for digital watermarking, where the hidden message within the digital signal is transmitted by two parties.

Further use of invisible watermarking is the annotation of digital images with descriptive details [10,11]. In any watermarking algorithm, Mohanty defined the three components:

1. Retain the watermark.
2. an encoder algorithm of insertion.
3. a decoder (verification and extraction algorithm).

There is a special watermark for each owner. An owner can also use various watermarks to distinguish the buyers of many copies of the format content. Code 1, an S sign, and generates 1’ with an encoder fun.

The watermarking process includes the embedding, extraction, distribution, decision stage of the four phases. In the embedding phase, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. The above-mentioned watermarked image is subsequently distributed via digital channels in the distribution stage (on an Internet site). During the extraction process, an attempt is made to reclaim the watermark or signature from the spread watermarked image; finally, the extracted watermark is compared to the original watermark in the determination stage to check for any differences that may have occurred during distribution. Calculating the Hamming distance is a standard method of doing so.

\[ \text{HD} = (W \mod . W) ||W\mod|| ||W|| \]

where both the numerator and denominator are dot products.

HD obtained above is compared to a threshold, T, to determine how close W mod is to W [12,13].

1.1.2. Discrete Wavelet Transform (DWT)

Embedding watermark in original data takes place in two main domains: spatial, and frequency domain. In the spatial domains, the watermark is embedded in the original data by directly modifying
the pixel's values. There are different techniques for embedding watermark in a spatial domain such as Least Significant Bit (LSB) and Local Binary Pattern (LBP) [14,15].

Frequency domain techniques divide the signal into pieces and compress each piece of information into a set of coefficients, taking into account the correlations of pixels in space and conceptual insights in spatial-frequency information. Discrete Cosine Transform (DCT) and DWT are common transformation methods [16]. The DWT is a hierarchical decomposition of an image. It's particularly useful for processing non-stationary signals. The transform is based on waves of varying frequency and limited duration. Wavelet provides frequency and spatial information in a time-domain fixed-length analysis with the window shape fixed. There is a widespread in the high-frequency signal, DCT variant. Also, there is an impressive rate gap in its low-frequency part information that can be extracted from the signal [17].

The basic idea behind DWT is to multi-reactivate the image by assigning different spatial regions to distinct frequency locations, then convert the sub-coefficient image's Following DWT, the original image is decomposed into 4 districts into 2 low-frequency districts (LL) and 3 high-frequency (L, H, HL) using the 2 equations.

\[ \text{Lo}_m = \frac{f_{2m} + f_{2m-1}}{\sqrt{2}} \quad (m=1,2,3,\ldots,N/2) \quad \ldots \ldots \ldots \ldots \ldots (1) \]

\[ \text{Hi}_m = \frac{f_{2m} - f_{2m-1}}{\sqrt{2}} \quad (m=1,2,3,\ldots,N/2) \quad \ldots \ldots \ldots \ldots \ldots (2) \]

Where \text{Lo}_m is the low dimension approximation, \text{Hi}_m is the high dimension approximation and f is the signal value [18, 19].

The sub-level frequency district information can be retrieved by DWT transforming the information from the low-frequency district. Figure 1 shows a two-dimensional image after three DWT decompositions.

Where L represents a lowpass filter, H is a highpass Frequency decomposes the image into HL1, LH1, and HH Also sub-district information: LL2, HL2, and HH2 the original image can be partitioned for the n-wavelet decomposition The data of low-frequency district resembles the original picture. More of the image's signal information is in this frequency. The LH and HL vertical and horizontal frequency distribution dimensions represent the detail of the original image [20].

HVS describes human eyes as sensitive to changes in the overall image quality, but not districted or edge quality. As a result, the big amplitude of the watermarking signal was difficult. Then it has more of a concealment effect. To paraphrase: DWT's speed of decomposition is equal to HVS's image frequency dispersion. By implementing DWT, the concealing and the stability of the watermark can be balanced. Once the transformed domain becomes the major [21].

1.1.3. Particle Swarm Optimization (PSO)

PSO is a computational optimization method that is part of the Swarm Intelligence field [22]. PSO is a metaheuristic because it makes very few assumptions about the problem that needs to be solved. Any optimization problem can be solved with PSO. It is, nevertheless, particularly effective
for the optimization of problems with multimodal (many optima) and/or non-linear objective functions [23]. PSO also does not employ the gradient of the issue being optimized, making it ideal for problems with non-differentiable goal functions or ill-defined or changing definitions. The particles that make up the swarm in PSO are each a potential solution to the challenge at hand. A fitness value is assigned to each particle based purely on its position in the search space [24].

A stopping criterion is being applied to find the problem’s root cause. It is a possibility that all particle positions remain unchanged, or several iterations are reached. The motion of the particles have is dictated by their current location and by all particles found thus far in their surroundings. The entire swarm, a specific number of particles closest to it in the search space according to some distance metric, or a preset collection of particles might make up a particle's neighborhood (using a connection graph). Each particle $p$ effectively consists of two vectors see figure (2): a position vector $\mathbf{Z}_p$, and a velocity vector $\mathbf{V}_p$.

The coordinates in the search space are represented by the position vector (solution space). The iteration velocity vector represents the movement of each particle. whenever the location and velocity vectors are updated [24]:

1. Evaluate each particle's fitness.
2. Update the individual and global best fitnesses and locations.
3. Update each particle's velocity and position. For a particle $p$, its velocity $\mathbf{V}_p$ at time $t+1$ is updated as follows [25]:

   \[ \mathbf{V}_p(t+1) = w \cdot \mathbf{V}_p(t) + R(0,c1) \cdot (\mathbf{P}_l - \mathbf{Z}_p(t)) + R(0,c2) \cdot (\mathbf{P}_g - \mathbf{Z}_p(t)) \]...

   Where:
   - $w$ is the inertia weight ($0 \leq w \leq 1$).
   - $\mathbf{Z}_p$ is the vector denoting the position of particle number $p$.
   - $\mathbf{P}_l$ is the best position particle $p$ has found so far (“local best”).
   - $\mathbf{P}_g$ is the best position found so far by all particles in particle $p$’s neighborhood (“global best”).
   - $R(0, ci) (i \in \{1, 2\})$ can be written as $ci \cdot R(0, 1)$, where $R(0, 1)$ is a random diagonal square matrix with each element independently randomly drawn from the uniform distribution in [0, 1].
   - $c1$ and $c2$ are the acceleration coefficients or constants, determining the scale of the movement towards $\mathbf{P}_l$ and $\mathbf{P}_g$.

For a particle $p$, its position $\mathbf{Z}_p$ at time $t+1$ is updated as follows:

\[ \mathbf{Z}_p(t+1) = \mathbf{Z}_p(t) + \mathbf{V}_p(t+1) \]...

The updating rule can, alternatively, be written for the $m$-th dimension (or element) of a particle, as follows:

\[ \mathbf{V}_pm(t+1) = w \cdot \mathbf{V}_pm(t) + rand(0,c1) \cdot (\mathbf{P}_lpm - \mathbf{Z}_pm(t)) + rand(0,c2) \cdot (\mathbf{P}_gpm - \mathbf{Z}_pm(t)) \]...

where rand($0$, $ci$) is a random number in [0, $ci$].

The parameter $\mathbf{P}_l$ can be seen as the amount of resistance to a change in the movement of the particles. The vector $\mathbf{V}_p(t)$ can be seen as the momentum of the particle, a force that maintains that each particle can only depart about its current direction. The vector $\mathbf{V}_p(t)$ can be seen as a cognitive or memory component, the tendency for a particle to take into account the value of its own best position found so far. Finally, the vector $\mathbf{V}_pg$ can be seen as the social component—the tendency for a particle to take into account the best solution found so far by the other particles in its neighborhood.
The values in $\vec{V}_p$ (for particle p) are usually kept within a certain range, to avoid exploding velocities. However, this does not necessarily prevent the particles from moving beyond the search space boundaries. To rule this possibility out completely, one can also clamp the values of the position vectors, $\vec{Z}_p$ (for particle number p).

2. RELATED WORK

There is much research done earlier to design authentication systems for digital images, we will review some of the most important researches in this domain as follows:

- In 2018 [26]. The authors propose to secure the authenticity of images by several methods. Photographic image authentication methods are gaining popularity due to their significance in the field of multimedia communications and multimedia networking applications. Image authentication methods presently in use are cryptographic authentication, robust image hashing authentication, and watermarking authentication. This paper will summarize various methods for authentication for multimedia applications.

- In 2018 [27]. It’s a nice technique and thought-provoking information hiding technique, while at the same time the authors introduce information hiding basics. There will be a discussion about whether or not we should contain and hide the method of publishing the information. The examination of the LSB hidden information procedure depends on the carrier image, as the success or failure of the results is directly related to the quality of the information stored in the carrier image. The outcome demonstrates that the LSB algorithm provides a sophisticated means of processing while at the same time keeping the whole picture clear.

- In 2018 [28]. Digital document protection was achieved by the dual image-based watermarking system developed based on LBP. The proposed method of data watermarking involves partitioning host images into three-times overlapping blocks. Then generate XOR system vector (s) with secret watermark bits and perform XOR with system vector. An authentication code that was generated from the shared secret key between two individuals can be embedded within both images. The watermark and authentication codes can be recovered from the cover image at the receiver end. Once an authenticator has been validated and the re-authentication code has been generated, the user can enter the registration process. Our proposed system will be more effective than its opponents. The proposed scheme is secure and robust and can detect if objects have been altered.

- In 2019 [29]. A multi-image authentication method depends on the intensity equation has been discussed. First, blocks are chosen from multiple plain images by evaluating their spatial frequency coefficients. Then, a phase-encoded block with significant blocks is formed with a random intensity mask by bonding the logistic map. The complex-valued amplitude is turned into a real-valued signal by using Fresnel diffraction. Communication can be reconstructed by using intensity information. The image is verified when it is computed as the nonlinear

![Figure (2): The movement process illustrated for a two-dimensional search space, $w = 1$ and $R(0, ci) = 1$. [25]](image-url)
relation between only the significant partial blocks. The first time to use the intensity equation technique to implement optical multiple-image authentication. The simulations prove that the proposed approach is feasible.

- In 2020 [30]. They suggested embedding authentication coding in the two of the third preliminary color channels and adjusting the residual one to remedy the distortion of the grayscale values. The outcome shows up that embedding each four-bit code for the two-color channels yielded a mean 33.260 dB of PSNR but give a suitable detection.

3. PROPOSED METHOD

The proposed method is summarized by a set of critical stages that work in concert to verify image authentication, beginning with identifying the best areas for masking and then embedding the binary watermark bits inside the colored image under the DWT domain, as well as the retrieval stage of the binary image. The core stages include PSO, embedding, and authentication localization. The first stage, which utilizes the PSO algorithm to determine the least intense color region for later use in the embedding stage, and the second stage, which utilizes the DWT characteristics to embed the binary watermark bits in the host (color image).

To obtain a watermarked image (semi-fragile) in the low-frequency domain, the third stage involves sensing the proposed method's quality level by retrieving the binary watermark that was previously embedded and determining whether its quality is high and distortion-free. The final stage involves ensuring that the host is free of the intended tampering, as well as ensuring that the host is free of the intended tampering, the main stages of the proposed method shown in figure (3):

![Diagram of the proposed method](image)

**Figure (3):** The main stage of the proposed method
3.1. PSO Stage

PSO is a theoretical technique in computational science that optimizes a problem through an iterative process that attempts to improve a candidate solution in terms of a given quality measure. It solves the velocity and position problems by generating a population of candidate solutions, here referred to as particles. Each particle's movement is guided by its best-known specific area, but it is also focused on its best-known search-space positions, which change as other particles discover better positions.

This is expected to direct the swarm toward the optimal solutions. PSO was invented to simulate social behavior, as a stylized representation of organisms moving in a bird flock or fish school. The algorithm was simplified and it was discovered to be optimizing itself. PSO is a heuristic algorithm in the sense that it makes few or no assumptions about the problem being optimized and can search a very large space of candidate solutions. However, optimization algorithms such as PSO do not guarantee the discovery of an optimal solution. Additionally, PSO does not use the gradient of the optimized problem, indicating that it does not require the optimization problem to be specialized in the way that standard optimization methods such as gradient descent and quasi-newton methods do.

The PSO strategy is based on the behavior of a swarm of particles and determines the location of each particle based on its experience by searching in different areas in terms of dimensions and exploiting the best location encountered by it or its neighbors by updating its values each time the search is conducted in the various spaces.

With regards to the first value, it determines the particle's optimal position over other particles. We can follow the path of that particle and the second value follows that particle across all generations of the swarm; these two values are responsible for particles moving into the optimal positions via an iterative and random process. The proposed method relies on treating the R, G, and B primary color layers independently to obtain the Max and Min values. Which we will require later in a series of critical stages following the implementation of the RPLAN function on each color value (1-256), and then defining three variables x1, x2, and x3 for use in the Cluster process. After determining the Max and Min values for each color value, those values are used to calculate the cluster center, by taking the mean value and comparing it to the contiguous ones, and making the appropriate decision.

K-means algorithm is among the most popular clustering algorithms. It starts with an initial set of colors (initial color map, for example). Each color pixel is then appointed to the nearest color to the color on the color diagram. Then the color map is re-calculated as the centroids of the computing clusters. This interaction is rehashed until combined. The K-implies calculation has been demonstrated to combine to a neighborhood ideal, as already referenced; a significant disservice of K-implies is its reliance on beginning conditions.

From the figure above, after reading the color image, the main color layers R, G, and B are dealt with to perform the RPLAN operation on each color layer to determine the MAX and MIN values for each color layer (1-256), the goal of this process is to take advantage of them Later in the Cluster process, as well as in determining the least intense color area (the least color intensity), which will be the region prepared for concealment, the following algorithm demonstrates the working method of the PSO stage illustrates in the figure (4).
3.2. Embedding Stage

As it is known to everyone, the process of verifying the image authentication after the binary watermark bits embedding stage using an algorithm that developed by researchers in this field, and the embedding stage is either in the spatial domain or in the frequency domain, and each field has an improvement and its challenges, which are reflected in the strength and type of watermarked image resulting after embedding stage, moreover, the type of the host image that used plays a key role in the success of the embedding stage, as dealing with the gray image is less affected and the amount of distortion occurring in it as a result of adding the binary data is almost imperceptible with noting the quality of the watermarked image is of high quality in all the objective assessment, and subjective measures, while dealing with the color image is more influenced by all factors due to the color nature of the color image in addition to the different types of colored images, which makes the process of dealing with it more sensitive and we must obtain an image that resists the tests (intended attack, unintended attack) and it is not clear that it contains watermark bits. This task is difficult as well as it needs to be done at the same time. Dealing with the image within the frequency domain, which is what we suggest, also requires additional experimentation for us to guarantee the method's safety.

The proposed and achieving compatibility between PSO on one side and transform, which will be chosen; on the other side, because the embedding stage will be in two basic stages, the first achieved using by PSO algorithm which will define for us the best color region and the second is using DWT transform during the embedding stage, which will be the inclusion process through its scope.

Figure (4): General flowchart of PSO stage
On the other hand, consideration was given to the diversity in the color images used: high texture, low texture, smoothed, painted, and digital image. This diversity aimed to ensure the strength of the proposed method in the process of including watermark bits in more than one type of image used. Our proposed contribution to the proposed method is the embedding stage that aimed to embed the binary watermark bits in the host in which the least bound color regions were determined using the PSO algorithm, the modulation process was performed under DWT transform within the low-frequency domain because it does not affect the quality of the resulting image after the embedding stage, i.e watermarked image. The most commonly used collection of discrete wavelet transforms, on the other hand, was developed by Belgian mathematician Ingrid Wavelet transformations in 1988. This formulation is based on using recurrence relations to generate increasingly finer discrete samplings of an implicit mother wavelet function; each resolution is two times larger than the preceding one. Daubechies defines a family of wavelets in her seminal article, the first of which is the Haar wavelet. Since then, interest in this field has exploded, and several variations of the original wavelets of the Wavelet transform have been created.

In numerical analysis and functional analysis, and wavelet transform for which the wavelets are discretely sampled is a DWT. As with other wavelet transforms, temporal resolution is a key advantage over Fourier transforms: it captures both frequency and location data (location in time).

Let a HxW original image that resulted after PSO stage O_p with the size of (256×256 pixels) be a host image for XXY logo watermark W with the size of (128×128 pixels). The resultant will be watermarked image WI (256×256 pixels). At the first, DWT transform is applied to whole O_p to produce a DWT level that computed as HH, HL, LH, and LL, then we chose LL, where LL represents the selected sub-band from the low-frequency domain (the least color intensity) and it represents the low-frequency domain, it used to embed the watermark bits. The embedding process is based on the embedded watermark bits inside the selected coefficient of a low-frequency domain of the resulted image after the PSO stage, As a result of multiple experimental analyses (will be discussed later in the coming chapter.

The embedding stage includes a set of main processes by which the binary watermark bits are embedded in the host that resulting after the PSO stage, where the least intense color regions have been identified which we will deal with in this stage, the start from the process of reading the color image that resulted after PSO stage, then applied DWT to the whole O_p to calculate the different DWT levels of the (HH, HL, LH, and LL), then we will choose the low-frequency domain (LL) to deal with it because of the embedding stage with LL does not affect the quality of the resulting watermarked image. On the other hand; each bit of original watermark W are compared with the corresponding bits in O_p, this comparison depends on searching for the first bit in O_p, if the current bit value is in W = 0, then the first bit must be searched for in O_p =o and so on with the rest for both Op and W, the condition is met followed by a simple substitution operation between the W bits and the corresponding bit of Op.

After the comparison and embedding are completed, IDWT is performed to reconstruct the image to obtain a Watermarked image as (W1), the most important processes that were adopted in the embedding stage for the proposed method are shown in figure (5).
3.3. Extraction Stage

The purpose of this stage is to retrieve the binary watermark bits and ensure that they are fully recovered while maintaining the quality of the host and the recovered binary watermark, which, when compared to the original watermark bits, allows us to pinpoint the location of the manipulation with high accuracy on the host if we want to ensure the color image’s reliability and its freedom from manipulation. Figure (6) shows the basic operations associated with the recovery phase. After reading the watermarked image whose content may have been altered, the DWT algorithm that was previously used in the embedding stage is used to calculate the various levels of image fragmentation, which are HH, HL, LH, and LL, because the process of retrieving the watermark bits will be in the low-frequency domain (LL), which was previously dealt with in the embedding stage, and after reading the watermarked image whose content may have been altered, and after reading the watermarked image whose.

After the DWT is executed on the whole WIo’, the frequencies levels are computed as: (HH, HL, LH, LL) for each level and then choose the low-frequency domain (LL) specifically and start a process of reading and comparing each bit in the (LL), if the first bit of LL \[x(i, j)\] = 0, then perform swapping process between LL \[x(i, j)\] with the first corresponding bit of \(W\), \(W\), where \(W\) represents an array that adopted to collect the recovered binary watermark bits from \(W\) and so the comparison process continues for all (LL) bits in \(W\), finally IDWT is executed to reshape the image and get \(W\).
3.4. Authentication Proofing and Alternation Localization Stage.

The color image is one of the most important media that can be easily manipulated with the availability of easy-to-use software that is widely available and some of them are free, the proposed method aims to verify the reliability of the color image by including binary data in the standardized site under frequency domain by utilizing the proprieties of DWT according to approved standards to preserve the quality of the color image, and on the other hand to protect it from manipulation, If it found. The "WI" authentication verification stage begins by executing DWT to the whole "WI" and then calculating the different DWT levels (HH, HL, LH, and LL), then choose (LL) and an extraction stage is executed to extracted the binary watermark bits to produce the recovered watermark as Wr'.

When the binary image retrieval phase is completed, IDWT is executed to reconfigure both of Wr' and the O'.

The comparison process between W bits and Wr' that extracted from altered watermarked image WLr' bits is by reading both the W bits and comparing them with the Wr' bits, so if the bit in the position (n) in Wr' equals to the value of the bit in W of the corresponding location, then this means that the corresponding bit in altered watermarked image WLr' is reliable and does not contain tampering. Furthermore; if the bit value is in the position (n + 1) in Wr' is not equal to the value of the corresponding bit in W, so this means that the bit corresponding to the same position (n + 1) in the host is not reliable and has been tampered with it, and therefore the action will be by making the value of that bit in the strait equal to 0. The stage of proving the reliability of the image and determining the location of manipulation is shown in figure (7).
4. RESULTS AND DISCUSSION

In this section, some experimental results have been shown to demonstrate the effectiveness and success of the digital watermarking technique for the embedding of watermark images inside a host image, DWT domain and lastly extracting the watermark at the receiver end. In the proposed method samples that used in the practical side, each color image with a size of 256x256 Bit Map Image file format with different texture,  the binary watermark with the size of 128x128 (24-BMP). Initially we need to consider a host image which is generally in RGB form, figure (8) show the binary image which makes it a watermark while figure (9) shows the original image’s, and original image's histogram.

Figure (8): The watermark binary image
13

Figure (10) shows our samples that resulted after the applied PSO stage, and figure (11) illustrates images after the DWT stage, the watermarked image with a histogram that resulted after the embedding stage illustrated in figure (12).

5. CONCLUSIONS
Watermarking is a vast field that is undergoing a lot of investigation. In this field, commercial players are competing for domination. Though a clear winner has yet to be identified, photographs will likely be protected against copyright infringement using a mix of various cryptographic techniques (such as encryption) and watermarking. A suitable watermarking algorithm can be chosen based on the intended requirements and the desired level of security. The proposed method effectively conceals information through the use of a watermark image, The PSO algorithm proved to be an effective
algorithm to find low-level regions that were used to mask the watermark. The watermark image is embedded into the host image using the DWT coefficient process. And we use the Arnold Transform to generate the watermark image; at the other end, we use the inverse Arnold Transform to extract the watermark image. The proposed method demonstrates the efficient use of wavelet domain watermarking.

6. REFERENCES

[1] Chuang, Jun-Chou, and Yu-Chen Hu. "An adaptive image authentication scheme for vector quantization compressed image." Journal of Visual Communication and Image Representation 22.5 (2011): 440-449.

[2] Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." Journal of Computer and System Sciences 80.5 (2014): 973-993.

[3] Singh, Bhupesh Kumar, and Tanu Dua. "Image Authentication Using Digital Watermarking."

[4] Zhao, Xi, Philip Bateman, and Anthony TS Ho. "Image authentication using active watermarking and passive forensics techniques." Multimedia Analysis, Processing and Communications. Springer, Berlin, Heidelberg, 2011. 139-183.

[5] Mousavi, Seyed Mojtaba, Alireza Naghsh, and S. A. R. Abu-Bakar. "Watermarking techniques used in medical images: a survey." Journal of digital imaging 27.6 (2014): 714-729.

[6] Al-Otum, Hazem Munawer. "Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique." Journal of Visual Communication and Image Representation 25.5 (2014): 1064-1081.

[7] Li, Ming, Di Xiao, and Yushu Zhang. "Attack and improvement of the fidelity preserved fragile watermarking of digital images." Arabian Journal for Science and Engineering 41.3 (2016): 941-950.

[8] I. J. Cox and M. Miller, “The First 50 Years of Electronic Watermarking”, EURASIP Journal of Applied Signal Processing, Vol. 2, pp.126-132, 2002.

[9] Mohanty, Saraju P. "Digital watermarking: A tutorial review." URL: http://www.csee.usf.edu/~mohanty/research/Reports/WMSurvey1999Mohanty.pdf (1999).

[10] Sarkar, Rashel, R. Hemavathy, and G. Shobha. "An invisible watermarking technique for image verification." (2012).

[11] J. Fridrich, “Robust Digital Watermarking based on Key-Dependent Basis Function”. Portland,

[12] Khatau, Subhashree, and Debaraj Rana. "DWT based Image Watermarking for Information Security."

[13] Nikam, Miss Bhagyashri Dattatray, and Mrs SB Gaikwade. "Review on Digital Watermarking Techniques."

[14] Abdullahatif, Mohammad, et al. "Properties of digital image watermarking." 2013 IEEE 9th international colloquium on signal processing and its applications. IEEE, 2013.

[15] Tao, Hai, et al. "Robust image watermarking theories and techniques: A review." Journal of applied research and technology 12.1 (2014): 122-138.

[16] El-Shazly, E. H. M. "Digital Image Watermarking in Transform Domains." (2012).

[17] Kashyap, Nikita, and G. R. Sinha. "Image watermarking using 3-level discrete wavelet transform (DWT)." International Journal of Modern Education and Computer Science 4.3 (2012): 50.

[18] Grzeszczak, Aleksander, Mrinal K. Mandal, and Sethuraman Panchanathan. "VLSI implementation of discrete wavelet transform." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 4.4 (1996): 421-433.

[19] Tzanetakis, George, Georg Essl, and Perry Cook. "Audio analysis using the discrete wavelet transform." Proc. Conf. in Acoustics and Music Theory Applications. Vol. 66. 2001.

[20] Tiansheng, Mei, Li Sukang, and Tan Xiaomei. "A digital watermarking algorithm based on DCT and DWT." Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009). Academy publisher, 2009.

[21] Choudhary, Rita, and Girish Parmar. "A robust image watermarking technique using 2-level discrete wavelet transform (DWT).” 2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS). IEEE, 2016.
[22] Maimon, Oded, and Lior Rokach, eds. Soft computing for knowledge discovery and data mining. Springer Science & Business Media, 2007.
[23] Shi, Yuhui, and Russell Eberhart. "A modified particle swarm optimizer." 1998 IEEE international conference on evolutionary computation proceedings. IEEE world congress on computational intelligence (Cat. No. 98TH8360). IEEE, 1998.
[24] Mehdi Akhoondzadeh, and Kamal Azizi. "Particle swarm optimization (PSO)." Evolutionary and swarm intelligence algorithms. Springer, Cham, 2019. 11-23.
[25] Kennedy, James, and Russell Eberhart. "A Study on Image Authentication Methods." Proceedings of ICNN'95-international conference on neural networks. Vol. 4. IEEE, 1995.
[26] Marakumbi Prakash, and Jayashree V. Khanapuri. "Particle swarm optimization." International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 12 Dec 2018 www.irjet.net p-ISSN: 2395-0072.
[27] Chen, Chen. "Study on Information Hiding Technology Based on Digital Image." IOP Conference Series: Materials Science and Engineering. Vol. 394. No. 3. IOP Publishing, 2018.
[28] Pal, Pabitra, Biswapati Jana, and Jaydeb Bhaumik. "Watermarking scheme using local binary pattern for image authentication and tamper detection through dual image." Security and Privacy 2.2 (2019): e59.
[29] Sui, Liansheng, et al. "An optical multiple-image authentication based on transport of intensity equation." Optics and Lasers in Engineering 116 (2019): 116-124.
[30] Hong, Wien, et al. "A Color Image Authentication Scheme with Grayscale Invariance." IEEE Access (2020).
[31] Azmi Shawkat Abdulbaki, Ahmed J. Obaid & Alyaa Hashem Mohammed (2021) ECG signals recruitment to implement a new technique for medical image encryption, Journal of Discrete Mathematical Sciences and Cryptography, DOI: 10.1080/09720529.2021.1884378.