مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

# Techniques for Digital Watermarking in Images: A Review

Hiba Al-khafaji[1] Bayadir Abbas Al-Himyari [2] Noor Fadel Hussain[3]

[1]Software, College of Information Technology, University of Babylon, Iraq. Email: hibamj.alkhafaji@uobabylon.edu.iq
[2]Information Security, College of Information Technology, University of Babylon, Iraq. Email: sci.bayadir.abbas@uobabylon.edu.iq
[3]Information Security, College of Information Technology, University of Babylon, Iraq. Email: noor.fadel@uobabylon.edu.iq
***Corresponding author email:** sci.bayadir.abbas@uobabylon.edu.iq

**Accepted:** **31/12/2023** **Published:** **31/3/2024**

## ABSTRACT

Multimedia protection has become a significant problem in the society where the intellectual property is threatened. Digital watermarking can be considered as a solution to protect the multimedia. Property protection is a common field of research compared to other fields such as identity verification and local manipulation localization. Imperceptibility and robustness are the most crucial requirements for multimedia watermarking. High distortion is provided by watermarks with high robustness. We must so strike a balance between them. Recently many works based on frequency range which can satisfy watermarking requirements such as high robustness and low distortion. Visual attention based image watermarking is considered one of image watermarking methods due to detect the most important regions for watermark embedding. The lack of robustness against malicious cyber-attacks makes watermarks easily detectable and destroyed. As a result, the proposed watermarking scheme becomes more complex and cannot withstand diversity Geometric and non-geometric attacks. Therefore, there are many existing visual attentions based image watermarks. This paper analyzes the techniques for image watermarking against various types of attacks and presents the applications of digital watermarking.

Key words: Digital watermarking, imperceptibility, robustness, distortion

## INTRODUCTION

The advance of digital information has led to deep alteration in society, which creates new opportunities for invention and new defiance. The powerful software, modern devices, such as digital camera, high characteristics scanners and MP3 audio player have enabled users to generate and tamper with data. Moreover, internet and wireless networks make transmission and changing information easy. Therefore, the security of multimedia is an important and challenging problem. The solution for this problem is digital watermarking and data hiding, which are used for defense of the ownership and prohibition of unauthorized rigging of multimedia data.

Data hiding and digital watermarking are techniques used to hide a secret message in digital media. These techniques have been advanced for different applications, including authentication, ownership protection, access control, and annotation [1]. There are two types of digital watermarking: visible and invisible. This paper is focused on invisible watermarking.

## Important of Digital watermarking

The protection of copyright in digital media has become a significant issue in a society where intellectual property is threatened. Copying of digital content, plagiarism, piracy and illegal distribution have all become easier and are causing a real threat. New multimedia management

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

has caused problems like content tagging, content retrieval and content filtering. Cryptography and digital watermarking techniques are considered to be efficient solutions to these problems.

In cryptography techniques, the secret information enciphers (by using a secret key) works in a way that it becomes unreadable except to the recipient who knows the secret key. But if the key is lost or stolen, then the system becomes insecure. At the same time digital watermarking aims to keep the existence of secret information undetectable. Therefore, watermarking is regarded more confidential than cryptography, since it hides the mere existence of a message rather than only protecting the content of a message [2].

## Applications of Digital Watermarking

The digital watermarking can be defined as a copyright or author authentication information which is embedded in digital media in such a way that it is imperceptible, secure and robust. There are many applications for watermarking. Table (1) below explains its applications and description [2, 3].

**Table 1: Applications of digital watermarking**

| Application | Description |
|---|---|
| Broadcast monitoring | It can be implemented by putting a unique watermark in each video clip in order to identify when and where each clip. |
| Copyright identification | Using watermark information as copyright data. |
| Content authentication | appears Authentication of original work, performance and protection against digital forgery |
| Access control | Determine the viewing control for applications such as pay television. |
| Copy control | Watermarking can be used as a strong tool to prevent illegal copying of multimedia. |
| Banking document authentication | Authentication of financial documents such as authentication banking. |
| Packaging and tracking | Inserting watermark on packages in order to track and protect it against forged consumable items including pharmaceutical products |
| Video hosting authentication | Piracy control by video authentication at video hosting servers |
| Temper detection | The watermark is added to the sensitive data, if the watermark is distorted this mean the data cannot be trusted. |
| Fingerprinting | For each copy of data a fingerprint should be added. |
| Telemedicine | It is the science which is used to solve the health problems [4]. |

## Characteristics of Digital Watermarking

There has been a speedy development in the increase of Multimedia and communications. With the expanded use of networks, intellectual properties can be gained, copied or retransmitted easily, this led to appear techniques to protect the multimedia. Watermarking is one of the more efficient ways used to protect digital media. In order to design a good watermarking system, we need to start with the identification of its properties (as shown in table 2) [2].

**Table 2: Characteristics of digital watermarking**

| **Characteristics** | **Description** |
|---|---|
| Robustness | The watermark must be detected after different types of attacks. |
| Imperceptibility | The watermark should be invisible and without distorting the host media. |
| Fragility | The watermark can be removed or destroyed. |
| Security | It can be defined as the ability of watermark to resist against the passive and active attacks. |
| Tamper-resistance | Tamper-resistance is a property related to robustness against the intentional attacks. |
| False positive rate attacks | This means the detector identifies an un watermarked piece as a watermark. |
| Capacity | The amount of information can be hidden in the cover or host media. |

## Classification of Watermark Attacks

Attack can be defined as any process trying to remove or modify the watermark in the host media. The types of watermark attack can be categorized into four groups: removal attacks which aim to damage or remove the watermark from the watermarked media such as noising, histogram equalization, blur and sharpen attacks. The second attack is Geometry attacks which is distortion of the watermark such as rotation, scaling and translation. Cryptographic attack is the third category of attacks. The aim of this kind of attack is to break the security of the watermarking system by removing the watermark or hiding a deceptive watermark. This category includes brute-force and oracle. The last group is protocol attacks which aim to add their own watermark onto the data in question. This type includes invertible and copy attack [5]. Figure 1 shows the classification of watermarking attacks.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية
ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

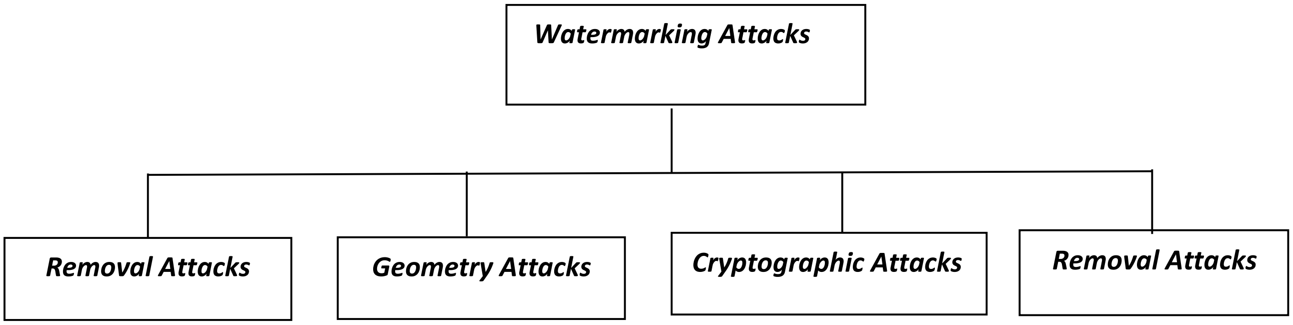

Figure 1: Classification of watermarking attacks

For removal attacks, the watermark is removed from the multimedia without distort the host media after the attacks. This type of attacks consists of quantization and de noising. These types of attacks destroy the watermark without damage the host media. The current algorithms defeat this types of attacks by using the frequency domains methods which are robust against these attacks such as DCT and DWT.

While Geometric attacks include scaling, cropping and rotation. This type of attack tries to damage the watermark detector synchronization instead of removing the watermark. Therefore, the synchronization process is very important to extract the watermark. However, this process is a high complexity. In order to stand against this types of attacks, the current watermarking techniques use the invariant domains and image feature dependent algorithms.

In cryptographic attacks, the watermark is removed or embed a fake watermark such as Brute-force search and Oracle which create a non-watermarked media. This type of attacks requires a high computational complexity, therefore, the attackers refrain from using this type of attacks. In the protocol attack, the attackers try to insert a fake watermark or predict the watermark then hide the watermark in the another data.

## Watermarking Techniques in Multimedia

Digital Watermarking is a technique for embedding a secret signal (watermark) into digital media such as image, video and audio in a robust, secure and imperceptible way. The term watermarking is derived from German term "wassermark". The goal of watermarking is to embed a unique signature to identify the origin or ownership of digital media for the purpose of copyright protection.

In 1282 the first watermark paper appeared in Italy, by adding a thin wire to the paper in order to identify the paper or to use as a trademark. After that digital watermarking gradually evolved until it was accepted as copyright protection [2].

There are many algorithms which can be used to hide the secret message. Some of these algorithms are robust, which means the attackers cannot destroy the message even after different manipulations. While the other algorithms can be fragile or semi fragile, the difference between them is the watermark which can destroy under any manipulation in fragile algorithms, and for semi fragile the watermark is robust to some attacks but fragile to others attacks. Depending on

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

the embedding domain it can be divided into two domains: Spatial and Frequency domain. Frequency domain watermarking can provide less distortion in the host media and more robustness compared to spatial domain [6].

## Spatial domain technique

In this technique the watermark directly hides in the digital media pixels. The robustness of spatial methods is less compared to frequency domain methods because it is based on direct manipulation of the pixels of multimedia. There are many algorithms that can be used in spatial domain, the main common algorithms can be presented below [7]:

1- **Least Significant Bit (LSB):** The most popular technique used to hide the watermark is the Least Significant Bits (LSB) of the multimedia pixels [8]. In this method the watermark converts into binary bits and hides into one or two bits (LSB) of the host pixels in a sequential or random positions, this means the number of watermark bits must be less than the host pixels' number. Lee et al. in [9], insert the watermark bits in random positions based on a secret key. Another work was presented by Bamatraf in [10] to hide two bits of the watermark in the third and fourth LSB of the cover image. To increase the security Sharifara et al. proposed a Zig-zag matrix to insert the watermark. This method is very easy to implement and with imperceptible distortion in the host media if it uses one or two LSBs and less distortion for using four LSBs. In addition, it is robust to salt-and-pepper, median filtering, Gaussian smoothing attacks [11].

Faheem et al. propose a watermarking technique that use a chaotic map and an image gradient to determine the least significant bit. Each non correlated block in the image is segmented, and the gradient of each block is computed. The image's gradient conveys the image's quick shifts. The watermark is jumbled using a chaotic substitution box (S-Box) in accordance with a piecewise linear chaotic map (PWLCM). The picture gradient is a method to determine where to embed a watermark and prevent image degradation since the embedding payload introduces a trade-off between resilience and imperceptibility. The watermark signal is implanted in accordance with the picture gradient by altering the least important portions of the original image. The direction and magnitude of the gradient in the image determine how much embedding can be done. The results demonstrate that the method is resilient to multiple image processing and geometrical attacks while preserving the watermark signal's imperceptibility when compared to alternative approaches. The results demonstrate that the method is resilient to multiple image processing and geometrical attacks while preserving the watermark signal's imperceptibility when compared to alternative approaches [12].

Another work is suggested by Faheem et al. based on using of the canny edge detection approach and the least significant bit (LSB). This method's main contribution is that it locates appropriate locations for watermark insertion and adds extra watermark protection by jumbling the watermark image. The gradient is computed for each non-overlapping block that makes up a digital image. Next, non-maximum suppression is used after convolution masks have been applied to determine the gradient's direction and magnitude. Lastly, the watermark is included in the hysteresis step using LSB. The chaotic substitution box is used to jumble the watermark signal, adding another layer of security. Because of the huge payload of LSB and its ability to contain a watermark following a canny edge detection

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

filter, the suggested solution is more secure. The embedded bits number is determined by the direction and size of the canny edge gradient. The suggested approach demonstrates strong resistance against geometrical attacks and image processing [13].

2- **Spread Spectrum Modulation (SSM):** This technique can be used in spatial domain and frequency domain. In this method the information is hidden by using linearly combining the cover image with a small pseudo noise signal which is modulated by embedded watermark [7]. Code-Division Multiple Access (CDMA) spread spectrum is a popular method and robust to cropping because the watermark bits are scattered in a random way over all the host image based on PN sequence which is generated using independent seeds for each watermark value [14, 15]. Also this approach can be applied in frequency domain by using Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT). This method is more robust compared to LSB method [16]. Ghrare et al. in [17] introduce and describe a hybrid watermarking method based on Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB). Since the three examples' recovered watermarks from the watermarked image were all very near to 1, the SSIM results were not altered. When compared to watermarked images created with standalone LSB and DWT, the PSNR and MSE values demonstrate that the quality of the images produced using the suggested technique is superior. Furthermore, the outcomes demonstrate that, in comparison to LSB and DWT approaches, the suggested hybrid strategy was more successful in terms of robustness and imperceptibility.

## Frequency Domain technique

In this technique the watermark is embedded in the spectral coefficients of the images. The frequency methods are more widely used compared to spatial domain because these methods are more robust and with less embedding distortion. The most common transforms are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) [5]. Some methods used a mix of two frequency approach to increase the robustness of the method used such as DCT and DWT [18].

1- **Discrete Cosine Transform (DCT)**

DCT can be classified into Global DCT and Block based DCT depending on the way the watermark is embedded. In DCT methods, the watermark is embedded into the DCT coefficients (low, middle or high frequency). This method is more secure against simple image processing operations like low pass filtering, brightness and contrast adjustment etc. While they are weak against geometric attacks like rotation, scaling, cropping, etc. Moreover, the advantage of embedding in the perceptually significant portion of the image is to be robust against image compression, because most compression approaches remove the insignificant portion of the image [5]. Betacourth et al. present a watermarking scheme to embed binary digits in the low and middle frequencies of DCT blocks of the host image. This method is robust against JEPG compression attacks [19, 20].

Rahardi et al. propose BRIW-DCT, a blind and reliable watermarking method that protects colour images' copyright by utilizing the Discrete Cosine Transform (DCT). The

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq| www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

host image's channels are separated into 8x8 pixel-sized non-overlapping image blocks. The DCT transformation converts each image block into a frequency domain. The DCT coefficients are changed in order to incorporate the watermark image into the host image. The watermarked image obtained a high SSIM value and a high PSNR value, according to the results. Furthermore, the watermarked image is subjected to a variety of attacks. The watermark image may be effectively recovered by BRIW-DCT from the manipulated image, yielding a low BER value of and a high NC value [21].

## 2- Discrete Wavelet Transform (DWT)

The transform is based on small waves, called wavelet. DWT is widely used in digital image processing, compression, watermarking, etc. The wavelet transform decomposes the image into levels, each level creates four sub bands, namely LL, LH, HL, and HH. The LL subband represents the original image in half resolution, also, it includes smooth spatial data with high spatial correlation. The LH and HL sub bands include vertical and horizontal orient high frequency details while the HH sub band contains the noise and edge information [22].

Tain et al. in [23], use the Integer Haar Wavelet Transform to produce the redundancy in an image and embedded a secret message by expanding the differences of a pair of pixels, this approach achieves high payload rates. Another work was proposed by Bhowmik et al. in [24], to evaluate robustness of watermarking techniques. It used wavelet transform against JPEG2000 and explained the effecting of a different set of parametric combination (sub band, wavelet kernel, hosting coefficient, embedding method) on the robustness under a common platform. The algorithm needs to choose various numbers of wavelet decomposing levels in order to select a desired sub band or combination of sub bands. Therefore, there is a balance between imperceptibility and robustness.

This work offers an integer wavelet transform (IWT) and singular value decomposition (SVD) based efficient image watermarking algorithm. The carrier images are first split up into blocks. Next, the low frequency portion of the process involves the singular value decomposition and the block-based integer wavelet transform. Ultimately, the resilience of digital watermarking is increased by efficiently extracting energy from the first unique value. The resilience and imperceptibility of image watermarking are simultaneously optimized through the application of genetic algorithms [25].

Another work for watermark integrity verification and patient identification are presented by Moad et al. This work uses a two-part watermark: the patient's encrypted photo is in the second component, and the patient's information fingerprint is in the first. A discrete wavelet transform is used to split the medical image into four sub-bands for the integration procedure. The resultant mid-frequency coefficients are then modulated to integrate the watermark bits. The capability of this method not only enables the integration of the patient's fingerprint and photos, but it will also be adequate for the potential addition of error-correcting code. The watermark could be imperceptibly hidden due to the integration process's coefficient modulation. The experiments show that watermark can be survived against various types of attacks [26].

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table (3) explains analysis of watermarking methods against various types of attack. It appears that LSB method can survive three types of attacks: Salt-and-Pepper Noise, Median Filtering and Gaussian Smoothing, and it is superior to the DWT. For CDMA spread spectrum method, it can be applied in spatial domain and frequency domain. This method is robust against cropping attack because the watermark hides in random positions in all the host media and more robust compared to LSB method. DCT method is robust against the compression attack, because most compression methods remove the insignificant parts of the image. This means all frequency methods are more robust and the watermark can be extracted after many kinds of attack.

**Table 3: Analysis of watermarking methods against various types of attacks**

| **Attacks** | **Spatial Methods** | **Frequency Methods** |
|---|---|---|
| Rotation | CDMA [16] | CDMA [16, 17] |
| Scaling | CDMA [16] | CDMA [16, 17] |
| Cropping | CDMA [14, 15] | CDMA [16, 17] |
| Sharpen | | DWT [23, 26], DCT [21] |
| Salt-and-pepper | LSB [11, 12, 13] | DWT [23, 26] |
| Gaussian | LSB [11,12, 13] | DWT [23, 26] |
| Median filtering | LSB [11, 12, 13] | |
| JPEG-Compression | | CDMA [16, 17], DCT [21] |
| JPEG2000 | | DWT [24] |
| Histogram Equalization | | DWT [23, 26] |

Overall, most of the spatial domain techniques tend to be less robust and secure compared to frequency domain techniques against different types of attacks, especially DWT. It has more advantages than other transformation, because DWT allows watermark to be embedded in regions where Human Visual System (HVS) is less sensitive. This is, in order to increase robustness of watermarking with less degradation of host quality, as well as, Wavelet coded image is a multi-resolution description of image to detect the features of the image. In addition, DWT has a spatial frequency locality it means any change in the transform coefficients does not affects the entire image. Therefore, it can be regarded as the best transform. To evaluate any watermarking system, we need to know its properties. Any watermarking system must be robust

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

against various kinds of attacks and secure, also, the watermark must be invisible, however, the most important requirements are robustness and imperceptibility. We need to find a balance between these requirements. Moreover, in recent research, there is an increasing interest to use some models such as saliency map in order to determine the best region which is used to embed the data without distortion.

## Visual Saliency based Watermarking

Visual attention plays an important role in various visual applications by detecting saliency map, which apply in computer vision and image processing tasks such as image segmentation, image compression, object tracking, data hiding, etc. Sur et al. in [27], suggest a watermarking method by using saliency model. The Least Salient Pixels are detected by using the visual attention model of Itti and Kock [1], and used to embed the watermark. The results show that the watermark is invisible and the perceptual error is less than the normal Least Significant Bits (LSB). In [28], the authors propose a watermarking method based on saliency to detect the salient regions by using graph. Then embed the watermark in the Least significant bits. The results show the proposed method is robust against different types of attacks such as adding noise, scaling, median filtering, and histogram quantization, in addition, the watermark is imperceptible. Oakes et al. [29], propose a visual attention based watermarking method. Visual attention is applied in wavelet domain to detect the salient regions. In this algorithm, more information (watermarks) are hidden in the uninteresting areas in the host image. Firstly, apply the visual attention model (VAM) on the Low-Low (LL) frequency sub band and use this mask for the high-low (HL), Low-High (LH) and high-high (HH) sub bands for X levels of wavelet decomposition. Repeat this process by re-applying the VAM to the LL sub band and generating mask for all sub bands with the same spatial resolution. This method is robust against various filtering and natural image processing attacks.

In [30], the authors present a visual saliency modulated Just Noticeable Distortion (JND) profile to get optimal watermarking algorithm by hiding less information (watermark) is hidden in most important regions and more information in less perceptual regions. The experiments show that the watermark is imperceptible and robust against different attacks. In [31], another watermarking work based on Just Noticeable Distortion (JND) with saliency map, which apply on Discrete Cosine Transform (DCT) to detect the best region in order to hide the watermark. The results show that the watermark can extract, after various attacks such as JPEG compression, salt-and-pepper noise. In [32], the authors suggest a data hiding method using Discrete Wavelet Transform (DWT). The main idea is to perform a 3-level selective DWT on the blue component of RGB cover image. Then generate the saliency map from Low-High (LH) because any changes made in these regions are imperceptible, the watermark is hidden in LH and HL. The results show that the watermark is invisible and robust against Low pass filtering, JPEG compression, Gaussian noise, salt-and-pepper noise and scaling. In [33], the authors suggest a novel reversible watermarking method of enhancing the local prediction in order to reduce the prediction error of every pixel value. In this method the original image is multiplied with its saliency map. After that compute the prediction error, if the absolute of it is smaller than the threshold, then the pixel uses to embed the watermark. Otherwise, the pixel is not used for embedding processes. This method has perfect reversible for watermark and original image, high embedded capacity and less distortion. In [34], the authors proposed a reversible watermarking method based on graphs

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

to extract stable feature regions. Firstly, feature points are extracted from image using Harries-Affine. Secondly, a graph is constructed using feature regions. Finally, embed the watermark in the selected stable regions. This method is robust against various geometric and signal processing attacks.

## Visual Saliency in Images

In past decades, many visual saliency approaches have been suggested to detect the important regions based on different low-level, middle-level and high-level properties. Visual saliency can be classified into different categories depending on various criteria. It can be categorized in two groups: human fixation and region of interest according to the type of task. For human fixation, methods try to identify the fixation points which human eyes would detect in the first glance. Also, depending on the model inspiration source, it can be divided into four groups. Biological inspired model which explores properties of human vision and tries to simulate the processes. Another type depends on extracting natural statistics from image. Moreover, computational is a common method to detect salient regions. Based on features level, saliency approaches can be grouped into two categories: bottom-up and top-down approaches. For bottom-up approaches, low-level features such as colour contrast, orientation and luminosity are used to detect salient regions. While, high-level features such as faces and objects are used to detect saliency in top-down approaches. Itti et al. in [35], proposed a biological inspired model. It is a bottom-up model using low-level features (colour, intensity and orientation) which are integrated by using centre-surround mechanism. A similar idea was proposed by He et al. in [36], to detect a saliency map based on improving Itti's model [1]. Firstly, extract early visual image features such as intensity, colour and orientation, at multiple scales. Secondly, create three conspicuity maps from earlier features. Thirdly, combine three conspicuity maps into a slinky map nonlinearly. Finally, the contribution rate of each conspicuity map to the saliency map is done in inverse proportion to the saliency area. The results show that the new method is better than the Itti's method. In [37], the authors present a saliency map method by using wavelet transform domain (DWT). First, convert the image to YCbCr then apply DWT (lifting based DWT) on Y, after that decomposed Y component to spatial domain (inverse DWT) and do the same with Cr Cb then compute saliency map. The results show that the method has more accurate salient regions compared to the previous methods without DWT. Vikram et al. [38] suggest a global contrast work based on random window sampling. A number of sub-windows generate from an input image, then for each window compute saliency as the difference of the pixel intensity value to the average intensity value of the window. To get the final map, linear combination of saliency value and median filtering are used. A similar idea to use global contrast was proposed by Cheng in [39], the contrast is measured by using a colour distance in CIELAB colour space. In this work the input image is segmented into regions then the histogram based contrast for each region is computed. This method is fast and low computational cost. A saliency based graph model was proposed by Harel et al. in [40], an input image is represented as a fully-connected graph. Each node represents as a feature and the distance between two pixels defines the weight of the node. Features comprise orientation maps which can be gotten by using a Gabor filter. Another work for a saliency based graph was presented by Gopalakrishnan in [41]. Two properties of image (global and local) are computed using a graph to detect salient regions. In addition, Yang et al. in [42], proposed a method to detect salience regions by ranking the similarity of image elements with foreground cues or background cues by graph-based manifold ranking. The saliency of

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

image elements is defined based on their relevance for the given seeds or queries. In this method the image is represented as a close-loop graph with super pixels as nodes. These nodes are ranked based on the similarity to background and foreground queries. A different method to detect saliency map was presented by Achanta et al. in [43] it called a Simple Linear Iteration Clustering (SLIC) algorithm for constructing superpixels by using K-means clustering. Convert RGB colour images into CIELAB colour space, the clustering procedure starts with initial cluster centres. Each pixel has been connected to the nearest cluster centre, an update step sets the mean of all the pixels in the cluster to the centre of the cluster. The update steps can be refined until the error convergences. Another work based on super pixels was presented by Sree et al. in [44], by using a modified watershed segmentation algorithm. Many features can be used to segment rocks images such as texture shading, shape and edges. Therefore, it can be easier to calculate these features as a group of spatially coherent pixels called super pixels than every pixel in the image. Firstly, the magnitude gradient of the original image is computed. Secondly, an area closing operation is performed on this magnitude gradient image. Finally, a watershed transformation to the resultant image is applied to get the desired super pixels. This algorithm is memory efficient and faster compared to the existing algorithms on rock images. In [45], the authors presented a saliency method called boundary connectivity, based on the principle that background regions are more than object regions. Firstly, the image is abstracted as a set of regular superpixels using Simple Linear Iterative Clustering (SLIC) [43]. Then an undirected weighted graph is constructed by connecting all adjacent super pixels and setting their weight as the Euclidean distance between their average colours. For any super pixels, the geodesic distance between them is defined as the accumulated edge weight along their short path on the graph. This method is more robust to measure background compared with the other methods, because most saliency methods use contrast prior to it, it means the segmentation depends on the high contrast between the objects and their surrounding regions, therefore, these methods can fail if the contrast is low. Also, this algorithm can naturally handle pure background images, while previous methods cannot. For top-down method, Goferman et al. [46] suggested a different type of saliency to detect the important regions of images. This method differs from the other methods because it aims to extract the salient regions containing the prominent objects and the parts of the background that convey the context. It includes four basic principles of human visual attention. Firstly, local level considerations (colour and contrast). Secondly, global considerations. Thirdly, visual organization rules. Finally, high-level factors (human faces). This method can be used in two applications: the first is image re-targeting to prevent the distortions in the important regions of the images. The second is summarizations to produce compact, appealing and informative summaries.

Wan et al. provide a watermarking technique that uses only bottom-up features, like texture and brightness, and is based on visual saliency (VS) and just noticeable difference (JND) in the DCT domain. Recent work on saliency detection has demonstrated that an improved saliency model that takes into account both top-down and bottom-up features would result in a notable enhancement of the saliency detection performance as a whole. The new two-layer VS-induced JND profile that is provided in this study is made up of top-down and bottom-up features that were taken from DCT blocks in the transformed domain. Since the camerapersons are used to facilitate the attention regions in focus, the top-down feature of focus is employed to guide the production of final salient regions in this model, while the brightness and texture features are adapted to calculate the bottom-up features maps. In order to improve the trade-off between

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

fidelity and resilience, the suggested two-layer saliency-induced JND model is further utilized to adjust the quantization step in the watermarking framework. The experimental findings demonstrate that the suggested technique outperforms the earlier watermarking schemes in terms of performance [47].

In order to produce high payload and high quality watermarked images, this research proposes a robust saliency-based picture watermarking technique. An improved salient object model is first suggested to generate a saliency map, and then a binary mask is suggested to divide a host image's foreground and background into distinct regions. Next, the watermark image is broken down by consulting the same mask. Subsequently, the watermark's RGB channels undergo encryption via Arnold, 3-DES, and multi-flipping permutation encoding (MFPE). Moreover, the blue channel's unique matrix has an embedded copy of the primary encryption key. Additionally, Okamoto-Uchiyama homomorphic encryption (OUHE) is used to encrypt the blue channel. These encrypted watermark channels are then incorporated and dispersed among the host channels. According to experimental findings, the suggested strategy achieves good image quality and high payload without sacrificing robustness. Furthermore, it works better than state-of-the-art (SOTA) techniques [48].

## Conclusion

There have been significant advancements in our understanding of data hiding strategies within the past 25 years. Various watermarking schemes on multimedia are discussed and broadly divided into two domains based on embedding domain, spatial and frequency. The frequency methods are more robust compared to spatial methods. It can be seen that the spatial methods such as Least Significant Bits is robust against Gaussian and salt-and-pepper. The spread spectrum method is robust against the cropping because the watermark is spread over all the host media. While, Discrete Cosine Transform is robust against the compression because the compression deletes the insignificant portion of the media. Also, Discrete Wavelet Transform is robust against Histogram Equalization, Salt-and-pepper and JPEG2000.

## Conflict of interests.

There are non-conflicts of interest.

## References

[1] M. Wu and B. Liu, Multimedia data hiding, Springer Science & Business Media, 2013.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography, Morgan Kaufmann, 2007.

[3] S. Kaur, E. Jaspreet Kaur, and E. Inderpreet Kaur, “Technicalities of digital watermarking: a review”, *International Research Journal of Engineering and Technology (IRJET)* 3, no. 2395-0056, 02. 2016.

[4] M. G. Wang, Y. J. Mao, W. Li, “The application of telemedicine technology,” in Frontier and Future Development of Information Technology in Medicine and Education, pp. 3261–3268. Springer, 2014.

[5] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, “Analysis of digital image Watermark attacks,” in 7th IEEE Consumer Communications and Networking Conference. IEEE, pp. 1–5, 2010.

[6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems journal, vol. 35, no. 3.4, pp. 313–336, 1996.

[7] Ž .Nataša, “Robust image authentication in the presence of noise,” 2015.

[8] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” in Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference. IEEE, 1994, vol. 2, pp. 86–90, 1994.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

[9] G. J. Lee, E. J. Yoon, and K. Y. Yoo, “A new lsb based digital watermarking scheme with random mapping function,” in International Symposium on Ubiquitous Multimedia Computing. UMC’08, IEEE, pp. 130–134, 2008.

[10] A. Bamatraf, R. Ibrahim, and M. Salleh, “Digital watermarking algorithm using lsb,” in International Conference of Computer Applications and Industrial Electronics (ICCAIE), pp. 155–159, 2010.

[11] A. Sharifara, G. B. Sulong, and M. R. Seraydashti, “Digital image watermarking using Different levels of intermediate significant bits with zig-zag embedding approach,” International Journal of Image Processing (IJIP), vol. 7, no. 1, pp. 62, 2013.

[12] Z. B.Faheem , M.Ali, M. A.Raza, F. Arslan, J. Ali, M. Masud, , & M. Shorfuzzaman, “Image watermarking scheme using LSB and image gradient,” *Applied Sciences* 12, no. 9. 2022, 4202.

[13] Z. B. Faheem, A. Ishaq, F. Rustam, I. de la Torre Díez, D. Gavilanes, M. M. Vergara, I. Ashraf, “Image watermarking using least significant bit and canny edge detection” *Sensors* 23, no. 3 pp.1210, 2023.

[14] N. F. Johnson and S. Katzenbeisser, “A survey of steganographic techniques,” in Information hiding. Norwood, MA: Artech House, pp. 43–78, 2000.

[15] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking digital image and video Data a state-of-the-art overview,” IEEE Signal Processing Magazine, 17 (5), 2000.

[16] J. C. Lee, “Analysis of attacks on common watermarking techniques,”.

[17] Ghrare, S. E., Alamari, A. A. M., & Emhemed, H. A., “Digital image watermarking method based on lsb and dwt hybrid technique, ” In *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, pp. 465-470. IEEE, 2022.

[18] L. Tian, N. Zheng, J. Xue, C. Li, and X. Wang, “An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection,” Signal Processing: Image Communication, vol. 26, no. 8, pp. 427–437, 2011.

[19] G. P. Betancourth, A. Haggag, M. Ghoneim, T. Yahagi, and J. Lu, “Robust Watermarking in the dct domain using dual detection,” in IEEE International Symposium on Industrial Electronics. IEEE, vol. 1, pp. 579–584, 2006.

[20] W. C. Wu and G. R. Ren, “A dct-based robust image watermarking using local moment,” in Data Mining and Intelligent Information Technology Applications (ICMiA), 3rd International Conference on. IEEE, pp. 122–126, 2011.

[21] Rahardi, M., Abdulloh, F. F., & Putra, W. S. "A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection." *International Journal of AdvancedComputer Science and Applications* 13, no. 7 (2022).

[22] M. Vetterli and C. Herley, “Wavelets and filter banks: Theory and design,” IEEE transactions on signal processing, vol. 40, no. 9, pp. 2207–2232, 1992.

[23] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits System Video Technology, vol. 13, no. 8, pp. 890–896, 2003.

[24] D. Bhowmik and C. Abhayaratne, “On robustness against jpeg2000: a performance evaluation of wavelet-based watermarking techniques,” Multimedia systems, vol. 20, no. 2, pp. 239–252, 2014.

[25] T. Zhu, W. Qu and W. Cao, “An optimized image watermarking algorithm based on SVD and IWT. ” The Journal of Supercomputing 78, no. 1 pp. 222-237, 2022.

[26] M. S. Moad, M. R. Kafi, & A. Khaldi, “Medical image watermarking for secure e-healthcare applications. ”Multimedia Tools and Applications 81, no. 30 pp. 44087- 44107, 2022.

[27] A. Sur, S. S. Sagar, R. Pal, P. Mitra, and J. Mukhopadhyay, “A new image watermarking scheme using saliency based visual attention model,” in Annual IEEE India Conference. IEEE, pp. 1–4, 2009.

[28] A. Basu, T. S. Das, S. K. Sarkar, and S. Majumder, “On the implementation of an information hiding design based on saliency map,” in International Conference on Image Information Processing (ICIIP), IEEE, pp. 1–6, 2011.

[29] M. Oakes, D. Bhowmik, and C. Abhayaratne, “Visual attention-based watermarking,” in IEEE International Symposium of Circuits and Systems (ISCAS). IEEE, 2011, pp. 2653–2656.

[30] Y. Niu, M. Kyan, L. Ma, A. Beghdadi, and S. Krishnan, “A visual saliency modulated Just noticeable distortion profile for image watermarking,” in 19th European Signal Processing Conference, IEEE, pp. 2039–2043, 2011.

[31] W. Wan, J. Liu, J. Sun, C. Ge, and X. Nie, “Logarithmic stdm watermarking using visual saliency-based JND model,” Electronics Letters, vol. 51, no. 10, pp. 758–760, 2015.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[32] C. Agarwal, A. Bose, S. Maiti, N. Islam, and S. K. Sarkar, “Enhanced data hiding Method using dwt based on saliency model,” in IEEE International Conference on Signal Processing, Computing and Control (ISPCC), IEEE, pp. 1–6, 2013.

[33] J. Fan and T. Chen, “Reversible watermarking using enhanced local prediction,” in IEEE International Conference on Image Processing (ICIP), IEEE, pp. 2510–2514, 2015.

[34] G. Yin, L. An, X. Gao, and D. Tao, “Feature regions based on graph optimization for robust reversible watermarking,” in IEEE International Conference on Image Processing (ICIP), IEEE, pp. 4758– 4762, 2015.

[35] L. Itti, C. Koch, E. Niebur, et al., “A model of saliency-based visual attention for rapid scene analysis,” IEEE Transactions on pattern analysis and machine intelligence, vol. 20, no. 11, pp. 1254–1259, 1998.

[36] D. He, Y. Zhang, and H. Song, “A novel saliency map extraction method based on improved itti’s model,” in International Conference on Computer and Communication Technologies in Agriculture Engineering. IEEE, vol. 3, pp. 323–327, 2010.

[37] C. W. H. Ngau, L. M. Ang, and K. P. Seng, “Bottom-up visual saliency map using Wavelet transform domain,” in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), IEEE, vol. 1, pp. 692–695, 2010.

[38] T. N. Vikram, M. Tscherepanow, and B. Wrede, “A saliency map based on sampling an image into random rectangular regions of interest,” Pattern Recognition, vol. 45, no. 9, pp. 3114–3124, 2012.

[39] M. M. Cheng, N. J. Mitra, X. Huang, P. H. Torr, and S. M. Hu, “Global contrast based Salient region detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 37, no. 3, pp. 569–582, 2015.

[40] J. Harel, C. Koch, and P. Perona, “Graph-based visual saliency,” in Advances in neural information processing systems, pp. 545–552, 2006.

[41] V. Gopalakrishnan, Y. Hu, and D. Rajan, “Random walks on graphs for salient object detection in images,” IEEE Transactions on Image Processing, vol. 19, no. 12, pp. 3232–3242, 2010.

[42] C. Yang, L. Zhang, H. Lu, X. Ruan, and M. H. Yang, “Saliency detection via graph-Based Manifold ranking,” in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 3166– 3173, 2013.

[43] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, “Slic superpixels Compared to state-of-the-art superpixel methods,” IEEE transactions on pattern analysis and machine intelligence, vol. 34, no. 11, pp. 2274–2282, 2012.

[44] S. R. SP Malladi, S. Ram, and J. J. Rodriguez, “Superpixels using morphology for rock Image segmentation,” in IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), IEEE, 2014, pp. 145–148, 2014.

[45] W. Zhu, S. Liang, Y. Wei, and J. Sun, “Saliency optimization from robust background detection,” in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2814–2821, 2014.

[46] S. Goferman, L. Z. Manor, and A. Tal, “Context-aware saliency detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 10, pp. 1915–1926, 2012.

[47] W. Wan, J. Wang, M. Xu, J. Li, J. Sun, H. Zhang, “Robust image watermarking based on two-layer visual saliency-induced JND profile ”, *IEEE Access* 7 pp. 39826-39841, 2019.

[48] A. Khan, K. Wong, “High payload watermarking based on enhanced image saliency detection ”, *Multimedia Tools and Applications* 82, no. 10 pp. 15553-15571, 2023.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

## الخلاصة

أصبحت حماية الوسائط المتعددة مشكلة كبيرة في المجتمع حيث تتعرض الملكية الفكرية للتهديد. يمكن اعتبار العلامة المائية الرقمية حلاً لحماية الوسائط المتعددة. تعد حماية الملكية مجالًا بحثيًا شائعًا مقارنة بالمجالات الأخرى مثل التحقق من الهوية وتوطين التلاعب المحلي. تعد عدم القدرة على الإدراك والمتانة من أهم المتطلبات لوضع العلامات المائية للوسائط المتعددة. يتم توفير تشويه عالي من خلال العلامات المائية ذات المتانة العالية. وعلينا أن نحقق التوازن بينهما. في الآونة الأخيرة، تم اعتماد العديد من الأعمال على نطاق التردد والتي يمكن أن تلبي متطلبات العلامة المائية مثل المتانة العالية والتشويه المنخفض. تعتبر العلامة المائية للصور المبنية على الاهتمام البصري إحدى طرق وضع العلامات المائية على الصور نظرًا لاكتشاف المناطق الأكثر أهمية لتضمين العلامة المائية. إن الافتقار إلى القوة ضد الهجمات الإلكترونية الضارة يجعل من السهل اكتشاف العلامات المائية وتدميرها. ونتيجة لذلك، يصبح مخطط العلامات المائية المقترح أكثر تعقيدًا ولا يمكنه تحمل التنوع الهندسي والهجمات غير الهندسية. لذلك، هناك العديد من العلامات المائية للصور القائمة على الاهتمامات المرئية. تحلل هذه الورقة تقنيات وضع العلامات المائية على الصور ضد أنواع مختلفة من الهجمات وتقدم تطبيقات العلامات المائية الرقمية.

الكلمات المفتاحية: العلامة المائية الرقمية، عدم الإدراك، المتانة، التشويه