*Asian Journal of Research in Computer Science*

*9(3): 34-51, 2021; Article no.AJRCOS.69033*
*ISSN: 2581-8260*

# Image Authentication Based on Watermarking Approach: Review

**Basna Mohammed Salih Hasan[1*], Siddeeq Y. Ameen[2] and Omer Mohammed Salih Hasan[3]**

*[1]IT Department. Technical College of Informatics Akre, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.*
*[2]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.*
*[3]IT Department, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.*

***Authors' contributions***

*This work was carried out in collaboration between all authors. Author BMS designed the study, performed the statistical analysis, wrote the protocol and wrote the first draft of the manuscript. Authors SYA and OMS managed the literature searches. All authors read and approved the final manuscript.*

***Article Information***

DOI: 10.9734/AJRCOS/2021/v9i330224
Editor(s):
(1) Dr. Dariusz Jacek Jakóbczak, Koszalin University of Technology, Poland.
Reviewers:
(1) Simrandeep Singh, Chandigarh University, India.
(2) S. Bhargavi Latha, GRIET, India.
(3) C. Ananth, Annamalai University, India.
Complete Peer review History: http://www.sdiarticle4.com/review-history/69033

***Review Article***

***Received 27 March 2021***
***Accepted 07 June 2021***
***Published 10 June 2021***

## ABSTRACT

Digital image authentication techniques have recently gained a lot of attention due to their importance to a large number of military and medical applications, banks, and institutions, which require a high level of security. Generally, digital images are transmitted over insecure media, such as the Internet and computer networks of various kinds. The Internet has become one of the basic pillars of life and a solution to many of the problems left by the coronavirus. As a result, images must be protected from attempts to alter their content that might affect important decision-making. An image authentication (IA) system is a solution to this difficult problem. In the previous literature, several methods have been proposed to protect the authenticity of an image. Digital image watermark is a strategy to ensure the reliability, resilience, intellectual property, and validity of multimedia documents. Digital media, such as images, audio, and video, can hide content. Watermarking of a digital image is a mechanism by which the watermark is embedded in multimedia and the image of the watermark is retrieved or identified in a multimedia entity. This

**Corresponding author: E-mail: basna.mhmed@dpu.edu.krd;*

paper reviews IA techniques, watermark embedding techniques, tamper detection methods and discusses the performance of the techniques, the pros and cons of each technique, and the proposed methods for improving the performance of watermark techniques.

*Keywords: Image authentication; watermarking; machine learning; image processing.*

## 1. INTRODUCTION

Authentication techniques for digital images have recently gained great attention due to their importance for a large number of multimedia applications, and in general, digital images are transmitted through insecure media such as the Internet and computer networks of various kinds, and the application may require a high level of security such as military applications. And, as a result, medical images must be protected from attempts to change their content, as such changes may influence decisions based on these images [1].

A watermark is a seal, signature, or sign placed within the multimedia, that is, pictures, audio, videos, and even products, to show the ownership rights of the product or material to the owner [2]. Unlike many techniques that seek to hide or encrypt content, the watermark appears as a symbol embedded within the material in a way that does not affect accuracy and guarantees ownership, and so that it is not affected by attempts to delete, steal or copy, and one of the most important things that include the watermark is money.

A watermark is a stamp, trademark, or symbol that is embedded in multimedia, such as photographs, audio, videos, and even objects, to demonstrate the owner's ownership rights to the object or content [3,4]. Unlike several other techniques that aim to conceal or encrypt information, the watermark exists as a signal inserted within the material in a manner that does not impair accuracy or ensure control, and that is unaffected by attempts to erase, snatch, or duplicate, and one of the most critical items that involve the watermark is money [5]. A watermark can be used in a variety of ways, and similar to your official signature, it can be applied as a distinctive mark to your images or designs to allow consumers to monitor your company [6,7].

Authentication plans are divided into two sections in the literature: utilizing digital signatures or digital watermarking [8] (Fig. 1).

Machine Learning (ML) is a data analysis technique that automates the process of developing analytical models. It is a subfield of artificial intelligence based on the principle that systems can learn from data, recognize patterns, and make decisions with little human intervention. In recent years, machine learning has established itself as the preferred tool in a wide variety of engineering disciplines. Not only are machine learning techniques used in traditional contexts such as speech and handwriting recognition, but they are increasingly being used at the security-critical applications [9-11].

Image processing and the internet have simplified the replication, modification, reproduction, and distribution of digital photographs without any loss of content at low expense, with roughly instant delivery. Web techniques have evolved and developed so rapidly that the privacy and safety of data are threatened [12]. Therefore, The complexities of the current and forthcoming risks to preserve digital information include content verification, copyright security, and duplicate protection [13-16].

Information security is a result of the need to transfer private information over insecure internet networks. In the field of informatics and communications, authentication is the mechanism by which it is possible to ascertain the authenticity of the identity of a person or entity, as he claims, to prevent identity impersonation. The main purpose of this paper is to summarize the opinions and suggestions of researchers in placing a watermark on images that help in the promotion and protection of private data.

This paper reviewed IA Methods and the Watermark Approach. in section 1 introduction of the basic concepts, section 2 listed IA (techniques, attacks, and performance), in section 3 details from watermarking (techniques, attacks, and performance), section 4 discussing articles on IA based on a watermarking approach that have been introduced and published in last four years. in section 5 Conclusions are drawn from the research.

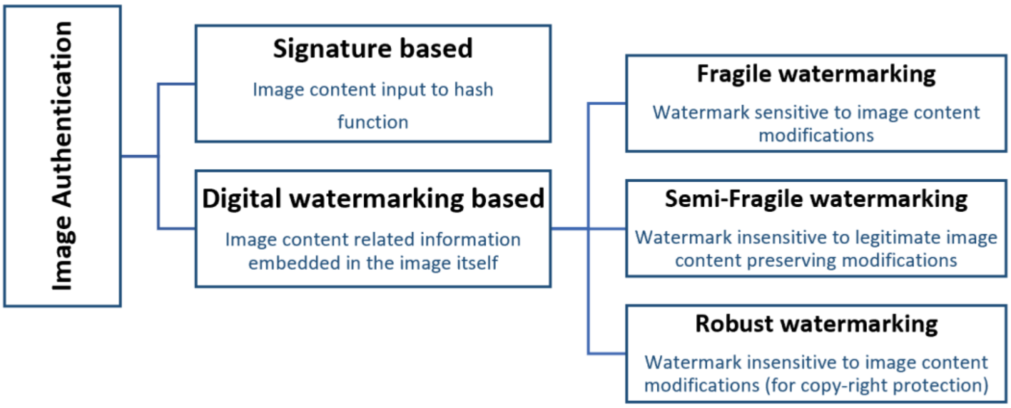
Image Authentication
Signature based
Image content input to hash function
Digital watermarking based
Image content related information embedded in the image itself
Fragile watermarking
Watermark sensitive to image content modifications
Semi-Fragile watermarking
Watermark insensitive to legitimate image content preserving modifications
Robust watermarking
Watermark insensitive to image content modifications (for copy-right protection)

**Fig. 1. A scheme for classifying IA systems [1]**

## 2. IMAGE AUTHENTICATION

### 2.1 Image Authentication Techniques

Image Authentication (IA) techniques are generally classified into two classes: Active and Passive Authentication. Active authentication is the process of embedding a symbol within the media and guarantees its ownership, it includes two types digital watermarking and digital signatures. Passive authentication is used to detect tampering. It is classified as forgery-dependent methods and forgery independent methods. It shown in [17,18] Fig. 2.

### 2.1.1 Active authentication

Techniques for For the authentication method, prior image information is indispensable. It concerns the hiding of data where such coding is integrated into the image at the time of generation. The originality of the image is checked by this code. In addition, active authentication approaches are categorized as digital watermarking and digital signatures in two forms. Digital watermarks are inserted in the photographs during the collection of the image or the compilation stage and secondary data, normally derived from the image, is embedded in the digital signatures at the point of acquisition. There was a variety of studies both on digital and digital signatures. The key disadvantage to these methods is that prior information on the image becomes essential at the point of filming with special equipment [20,21].

### 2.1.2 Passive authentication

Passive authentication, also known as image forensics, is a technique for authenticating photographs without the need for any prior information other than the image itself. Passive strategies are predicated on the premise that, although tampering can leave little visible evidence, it is likely to change the underlying statistics [22]. These discrepancies are what allow for the detection of tampering. Furthermore, passive techniques are divided into forgery-dependent and forgery-independent categories. Forgery-dependent detection

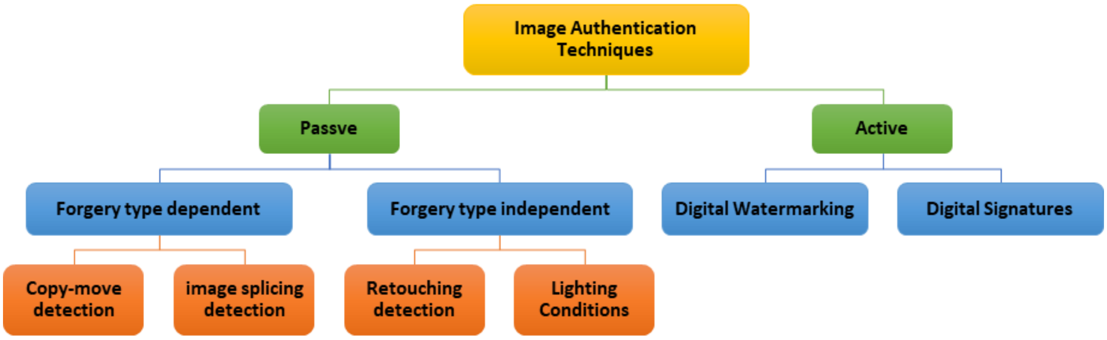

**Fig. 2. Image Authentication (IA) techniques and forgery detection [19]**

methods are designed to detect particular forms of forgeries such as copy-move and splicing that are dependent on the type of forgery performed on the image, while forgery independent methods detect forgeries regardless of the type of forgery performed on the image [23].

## 2.2 Image Authentication Attack

Cryptographic identification has the disadvantage of the not strong attached signature. The conversion of the format and all image processing operations may be destroyed. The automated watermarking fills this void where the signature can be integrated explicitly with the original filename. Although the watermark still has the original disk, it does not have to be individually stored and transmitted. In addition, once your file is altered, the watermark will change, which would enable you to understand not only that your file has been handled but how it is updated as well [24].

Two new SARI attacks have been proposed. The first assault is a histogram modification of DCT coefficients, which preserves the relationship between two DCT coefficients with identical DCT mean values. The assault applies to IA systems that do not use non-zero thresholds [25]. The second proposed attack is an oracle attack, which makes use of an oracle to find the secret pairs employed by SARI while generating a digital image signature [26-28].

## 2.3 Image Authentication Performance

IA settings to make it more effective and efficient:

**Security:** The authentication system must have an appropriate level of security to protect authentication data and can completely overcome risks and fraud attempts and provide a safer and more diversified use of authentication.
**Complexity:** It is important to use authentication algorithms that are more effective and efficient and easy to apply in real-time and not complicated or slow
**Robustness:** To avoid false authentication, the authentication mechanism must tolerate content tampering. Only authentication values that apply a choice rule to service algorithm type are appropriate. This property is only valid for algorithms that provide a selective authentication service [29].

# 3. IMAGE AUTHENTICATION THROUGH WATERMARKING APPROACH

## 3.1 Image Watermarking Techniques

A watermark is a signature or mark that is placed in multimedia, such as pictures, audio, and video clips, to retrieve the original copy and prove its ownership. The watermark appears as an embedded symbol within the material so that it does not affect accuracy, guarantees ownership, and is not affected by deletion or theft attempts. [30] It is divided into two types, visible (also known as a public watermark), and invisible (known as a secret watermark). There are many places to apply a watermark, whether it is visible or invisible. Like your official signature, it can be added as a trademark for your images or designs so that customers can track your business through it. Although it provides a solution to guaranteeing copyright, it may carry flaws if misused, as it may cause the focus to change in the image [31], as illustrated in Fig. 3.

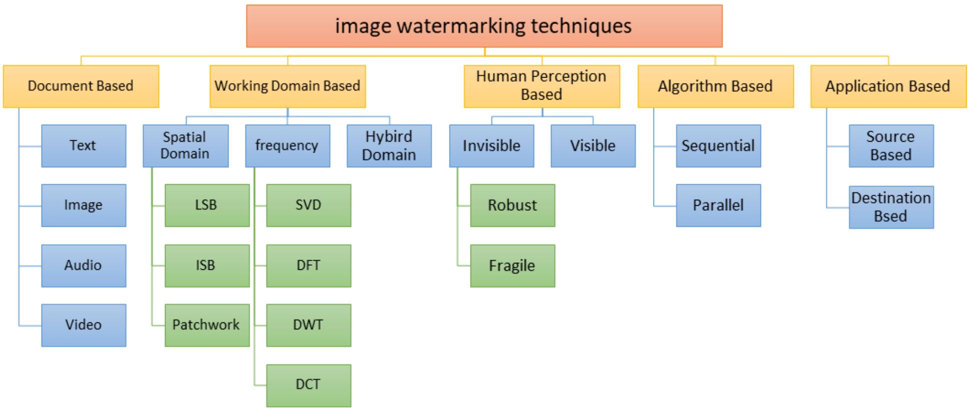

**Fig. 3. Classification of image watermarking techniques [32]**

This section provides a review of watermark techniques under the spatial domain and perception-based watermark and a review of the latest available literature on the topic.

### 3.1.1 Watermarking based on the spatial domain

The watermark is embedded in the original data using these techniques by directly modifying the pixel values. Algorithms in this domain are fast, simple, and capable of extensive embedding. Additionally, this domain enables multiple watermark embeddings to increase resistance to various attacks, particularly geometric attacks such as cropping, translation, and rotation, because the possibility of removing all watermarks becomes slim. The primary disadvantage of spatial domain-based watermarking is that it cannot withstand numerous removal attacks such as noise addition, sharpening, blurring, and median filtering. Additionally, determining the embedding technique used enables the attacker to easily change or alter the hidden watermark. There are various techniques for embedding a watermark in a spatial domain such as least significant bit(LSB), local binary pattern(LBP) and histogram modification [33] Show Fig. 4.

Recently, several advancements in LSB substitution have been suggested, such as a single-bit, multi-bit, or pseudo-random number generator. Like A. Soualmi, & et al. [35], proposed a novel blind effective spatial domain watermarking technique for ensuring the accuracy of digital medical images. The suggested method benefits from the integration of disorderly sequence and QIM to incorporate watermark pieces into the MinEigen value characteristics. The proposed technique is blind, in that the combined data can be deduced solely from the key used during the incubation phase, without requiring access to the original picture or watermark. The numerical findings demonstrate a strong level of resistance to experimental assaults.

M. Vazhora Malayil and M. Vedhanayagam [36], introduced a novel reversing watermarking scheme are embedding capacity and capability medical image recoverability. The original image capability of the new embedded system is three times the original image scale, and it is possible to recover the initial image without any errors in the absence of attacks. The experimental studies have observed that the current system performs picture recoveries with a smaller bit error rate compared to the popular reversible watermarking system used. After multiple assaults, Like adding noise, filtering of images, histogram processing, etc. on the watermarked file, a thorough examination of the bit error rate is produced.

M. Ghadi and et al. [37], proposed the use of texture analysis and association mining guidelines to provide for IA for blind space-based image watermarking. The concept is to categorize highly textured locations to incorporate a watermark into the host picture. The experimental results suggest that this approach is capable of generating interesting imperceptibility, robustness, and incorporation rate ratios while requiring little execution time.

### 3.1.2 Watermarking based frequency domain

Watermarking in a frequency domain is increasingly common because these schemes have a variety of advantages such as: (i) It is possible to achieve statistical independence between pixels as well as high-energy compression. (ii) the watermark is scattered irregularly over the entire spatial image, making it more challenging for adversaries to decipher and interpret the mark. (iii) Watermark can be hidden into a significant area, thus providing them more robust against several attacks (iv) Cropping danger to the spatial realm hardly affects the domain of transformation [38]. Fig. 5.

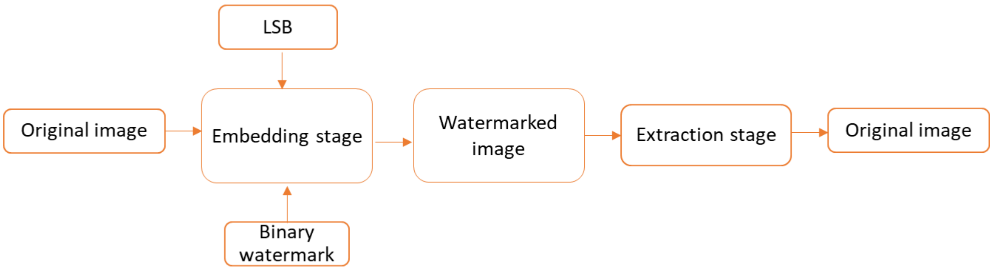

**Fig. 4. Watermarking under the spatial domain [34]**

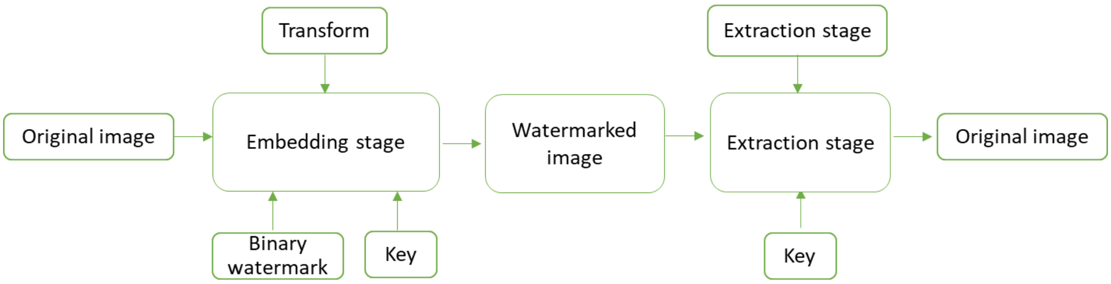

**Fig. 5. IA under transform domain[39]**

### 3.1.3 Discrete Cosine Transformation (DCT)

The (DCT) function determines an image's two-dimensional discrete cosine transform (DCT). The DCT has the property that, for a typical image, the majority of the image's visually significant information is concentrated in a few DCT coefficients. DCT is a typical and very general method of transforming domain watermarking technique. Background (FM) and (H) at the lower and right borders appear as the picture is separated into various frequency bands (low (FL) in the upper left corner). Middle frequency band FM, since it does not impair picture clarity, is the perfect band to embed watermarks. The watermark can be captured by human eyes in a low-frequency FL ensemble. And the FH high-frequency watermark band will lead along with edges to local distortion. This method can withstand compression, noise, sharpening, and filtration attacks. This approach is easier than the watermarking technique for the spatial domain [40].

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 🟩 | 🟩 | 🟩 | 🟩 | |
| FL | | 🟩 | 🟩 | 🟩 | 🟩 | | |
| | 🟩 | 🟩 FM | 🟩 | 🟩 | | | |
| 🟩 | 🟩 | 🟩 | 🟩 | | | | |
| 🟩 | 🟩 | 🟩 | | | | | |
| 🟩 | 🟩 | | | | FH | | |
| 🟩 | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Fig. 6. DCT Frequency 8X8 block [41]**

The following defines the two-dimensional DCT of an M-by-N matrix .

$$B\rho q = ap\ aq \sum_{m=0}^{M-1} \quad \sum_{n=0}^{N-1} Amn\ cos \frac{\pi(2m+1)p}{2M} cos \frac{\pi(2n+1)q}{2N}\ , 0 \le p \le M-1, \quad 0 \le q \le N-1 \qquad (1)$$

$$ap = \begin{cases} 1/\sqrt{M}, \\ \sqrt{2/M} \end{cases} \quad p = 0\ ,\ 1 \le p \le M-1 \qquad aq = \begin{cases} 1/\sqrt{N}, \\ \sqrt{2/N} \end{cases} \quad q = 0\ ,\ 1 \le q \le N-1 \qquad (2)$$

The values $B_{pq}$ are called the *DCT coefficients* of A.

The DCT transform is invertible, and its inverse is given by

$$Amn \ = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha p\ \alpha q\ Bpq\ cos \frac{\pi(2m+1)p}{2M}\ cos\ \frac{\pi(2n+1)q}{2N}\ , 0 \le m \le M-1\ , 0 \le n \le N-1 \qquad (3)$$

$$ap = \begin{cases} 1/\sqrt{M}, \\ \sqrt{2/M} \end{cases} \quad p = 0\,,\ 1 \le p \le M-1 \qquad aq = \begin{cases} 1/\sqrt{N}, \\ \sqrt{2/N} \end{cases} \quad q = 0\,,\ 1 \le q \le N-1 \tag{4}$$

The inverse DCT equation can be interpreted as meaning that any M x N matrix A can be written as a sum of MN functions, where MN represents the M functions and N represents the N parameters.

$$\alpha\rho\ \alpha q\ cos\frac{\pi(2m+1)p}{2M} cos\frac{\pi(2n+1)q}{2N}, \quad 0 \le p \le M-1\ , \quad 0 \le q \le N-1 \tag{5}$$

The basic functions of the DCT are known as the basis functions. In other words, when Bpq are calculated, the weights each of the basis functions receives are derived.The 64 basis functions are illustrated by this image for 8-by-8 matrices.

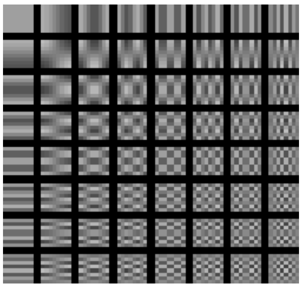

**Fig. 7. An 8x8 matrix has 64 functions (basis functions)**

From left to right, and from top to bottom, horizontal frequencies increase. DC basis function: Sometimes called the DC basis function, the constant-valued function (DC basis function) at the upper left corner is known as the DC basis function, and the corresponding DCT coefficient ($B_{00}$ coefficient) is known as the DC coefficient.

### 3.1.4 Discrete Wavelet Transformation (DWT)

DWT decomposes a given signal into a number of time series of coefficients describing the evolution of the signal in the corresponding frequency band.The image of DWT is divided into different frequency bands about equivalent range through multiple resolution breakdowns. This means that the approach of imperceptible marking with the separate processing of these bands by DWT is quite effective. In four sub-images, DWT divides into 1 rough portion and 3 depth components. Approximation portion as LL and detailed components as LH, HL, and HH. LL provides data on a image's low-frequency components as smooth zones, with high-frequency image elements as rough edges as the HH portion. The intermediate frequency bands of image are used in LH and HL. To achieve the next levels, the LL band can be decomposed further and the decomposition step proceeds until the desired data regarding the image are obtained. The Fig. 8. indicates two degradation stages within DWT [34].

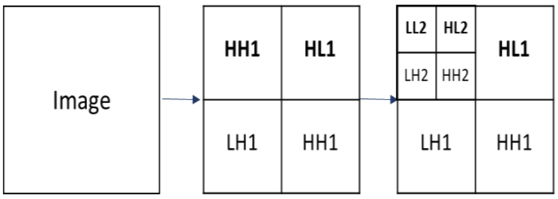

**Fig. 8. 2 level decomposition of DWT [42]**

A two-dimensional scaling function, *φ(x,y),* and three 2-D wavelets, *ψH(x, y), ψV(x, y),* and *ψD(x, y),* are required. Each is the product of two 1-D functions. Excluding products that produce 1-D results, like *φ(x)ψ(x),* the four remaining products produce the separable scaling function.

$$\psi^{H}(x, y) = \psi(x)\ \varphi(y) \tag{6}$$

$$\psi^{V}(x, y) = \varphi(x)\psi(y) \tag{7}$$

$$\psi^{D}(x, y) = \psi(x)\ \psi\ (y) \tag{8}$$

These wavelets measure functional variations- intensity changes in images- along different directions: ψH measures variations along columns (for example, horizontal edges), ψV responds to variations along rows (like vertical edges), and ψD corresponds to variations along diagonals. the directional sensitivity is a natural consequence of the separability in Eqs.(6) to (8); we simply take the 1-D FWT of the rows of *f* (*x*, *y*), followed by the 1-D FWT of the resulting columns. Fig. 9.

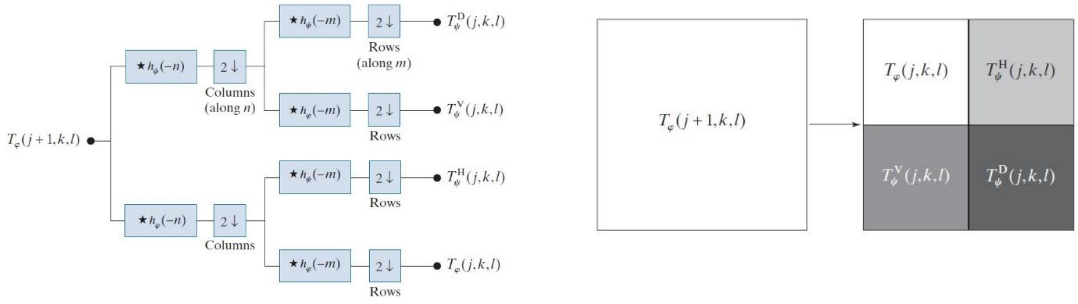

**Fig. 9. The analysis filter bank and resulting decomposion**

### 3.1.5 Discrete Fourier Transform (DFT)

The Fourier transform gives functions that are defined over an unlimited interval. The overlap of sinusoidal functions lacks periodicity. In terms of magnitudes and phases, the DFT function gives a quantitative view of the frequency information. It is also robust to different geometrical attacks including rotation, translation, cutting, etc. Inverted scaling in the Fourier domain reasons the scale of a spatial domain signal. If the space scale grows, the frequency and amplitude rise to maintain a constant area [43].The Fourier Transform of a function can be derived as a special case of the Fourier Series when the period, *T→∞*

$$\mathrm{x(t)} = \sum_{n=-\infty}^{+\infty} \mathrm{Cn}^{\mathrm{e}^{1jn\omega o}} \qquad (9)$$

Where $c_n$ is given by the fourier series analysis equation,

$$C_n=\frac{1}{T}\int_T \mathrm{x(t)e^{-jn\omega0t}\,dt} \qquad (10)$$

Which can be re written

$$T_{Cn}=\int_T \mathrm{x(t)e^{-jn\omega0t}\,dt} \qquad (11)$$

*As T→∞ the fundamental frequency,* $\omega0=\frac{2\pi}{T}$*, becomes extremely small and the quantity* $n\omega0$ *becomes a continuous quantity that can on any value (since n has a range of ±∞) so we define a new variable* $\omega = n\,\omega0$*; we also let* $X(\omega)=Tc_n$*. Marking these substitutions in the previous equation yields the analysis equation for the fourier trnansform (also called the Forward Fourier Transform).*

$$\mathrm{X(\omega)} = \int_{-\infty}^{+\infty} \mathrm{x(t)e^{-j\omega t}\,dt} \qquad (12)$$

*Likewise, we can derive the Inverse fourier transform(i.e., the synthesis equation)by starting with the synthesis equation for the fourier series (and multipy and divide by T).*

$$\mathrm{x(t)} = \sum_{n=-\infty}^{+\infty} \mathrm{Cne^{jn\omega0t}} = \sum_{n=-\infty}^{+\infty} \mathrm{TCne^{jn\omega0t}}\,\frac{1}{\mathrm{T}} \qquad (13)$$

As T→∞, 1/T= $\omega0 = 2\pi$. Since $\omega0$ is very small (as T gets large, replace it by the quantity $d\omega$). As before, we write *ω=nω0* and *X(ω)=Tcn*. A little work (and replacing the sum by an integral) yields the synthesis equation of the Fourier Transform.

$$\mathrm{x(t)} = \sum_{n=-\infty}^{+\infty} \mathrm{X(\omega)e^{j\omega t}}\frac{\mathrm{d\omega}}{2\pi} = \frac{1}{2\pi}\int_{-\infty}^{+\infty} \mathrm{X(\omega)e^{j\omega t}d\omega} (14)$$

### 3.1.6 Singular Value Decomposition (SVD)

SVD was perhaps one of the best linear algebra methods with any roles in compression snapshots as defined by Waldemar and Ramstad in the fields of snapshot compression (1997). SVD has probably been the most effective for watermarking, thanks to its solid architecture and ability to maintain the maximum visual quality due to its powerful nature and its ability to maintain visual quality [39].

Singular value decomposition takes a rectangular matrix of gene expression data (defined as A,where A is a *n x p* matrix) in which the *n* rows represents the genes, and the p columns represents the experimental conditions. The SVD theorem states:

$$A_{nxp} = U_{nxn}\,S_{nxp}\,V^{T}_{pxp}$$

Where, $U^TU = I_{nxn}$, $V^TV = I_{pxp}$ (i.e. U and V are orthogonal)

Where the columns of U are the left singular vectors (gene coefficient vectors); S ( the same dimensions as A) has singular values and is diagonal (mode amplitudes); and $V^T$ has rows that are the right singular vectors (expression level vectors). The SVD represents and expansion of the original data in a coordinate system where the covariance matrix is diagonal. Calculating the SVD consists of finding the eigenvalues and eigenvectors of $AA^T$ and $A^TA$. The eigenvectors of $A^TA$ make up the columns of V , the eigenvectors of $AA^T$ make up the columns of U. Also, the singular values in S are square roots of eigenvalues from $AA^T$ or $A^TA$. The singular values are the diagonal entries of the S matrix and are arranged in descending order. The singular values are always real numbers. If the matrix A is a real matrix, then U and V are also real.

Below a simple review of the latest papers that worked on this, R. K. Singh [44] & A. Anand [45], Proposed a dual system of watermarking based on a combined DWT and SVD approach. The key benefits of this technique are that they have a new approach for various safety features, and that methodology is an appealing method for smart healthcare about EPR data protection.

F. Kahlessenane [46], presented a robust and blind watermarking technique, enabling integration in a computerized tomography scan of an electronic patient record. To ensure copyright rights of medical photographs, a watermarking method is established. Patient information is integrated into this method into the DWT image coefficients. The bits of the label is integrated with the combination of parity of successive coefficients after a topological reorganization of the LL sub-band coefficients. The results of the experiment demonstrate the solution to many geometric or disruptive attacks give excellent imperceptibility and excellent resistance.

S. Thakur & et al [47], Proposed a chaotic, solution to the watermarking of medical images. Using non-sample contourlet transformations (NSCT), redundant and discreet wavelet transformations (RDWT), and singular value decomposition, the approach is used to significantly increase perception and power (SVD). The solution is ensured by the application of chaotic medical photographs with watercolor, encryption of 2-D logistics maps. The experimental evaluation, when attacked, shows that the solution is stable, imperceptible, safe, and suited for medical usage with NSCT, RDWT, SVD, and disorderly encryption.

## 3.2 Watermarking Attacks

Attacks are the factors or processes which degrade the strength of the digital watermark. there are so many new attacks continuously developed by hackers to affect the watermarking algorithms and watermark. These main broad definitions may be used to classify attacks [48]. According to the extensive literature on various watermarking techniques, extracting or altering hidden watermark data is not a difficult task for anyone, as information passes through the communication channel.However, a critical characteristic is that the watermarking system should be sufficiently robust against attacks. Any processing that results in the harmful detection of the watermark or impairment of the communication conveyed by the watermark is referred to as an attack in a watermarking system. Then, the watermark data that has been processed is identified as attacked data. Passive and active attacks, geometric attacks, removal attacks, protocol attacks, cryptographic attacks, blind attacks, informed attacks, tampering attacks, simple attacks, attacks based on key estimation, destruction attacks, and synchronization attacks are all intentional or unintentional attacks that can affect the watermarked image in various ways. Some of the known image watermarking attacks are listed in this section.[31]

a. **Active Attacks:** An active attack occurs when a hacker discovers and destroys the watermark itself. An image watermarking technique frequently implemented involves utilizing elimination, collusion, masking, distortion, forgery, duplication, mistranslation, and scamming. With an elimination attack, the watermark image cannot be detected, but in a copy attack, a copy with no watermark is produced [49].
b. **Passive attacks:** A passive attack happens when an attacker searches for a watermark and does not mind if the watermark is erased. To obtain the information associated to the watermarking resources, the attacker does not attempt to modify them. As different levels of passive attacks are considered for various important communication goals, different levels of these attacks can be used to meet various objectives.[50,51].
c. **Removal Attacks:** Such attacks damage the watermark so that it can erase or almost remove watermark data in its entirety. The denoising, measurement (e.g.

for compression), modulation and collusion attacks are examples of these attacks [52].

d. **Geometric Attacks:** Such assaults can target the pixels of the image. Like shifting pixels, image scaling, image rotating without further visual adjustments. Such attacks aim to weaken the watermark quality [24].
e. **Cryptographic Attacks:** In such attacks, they locate the gaps in the key built-in algorithm and delete watermark information. Examples include the assault by (brute force and oracle) attack. However, if the embedding algorithm is complicated, the attacks will easily be constrained [53].
f. **Protocol Attacks:** These attacks are carried out deliberately by attackers to modify or erase the copyright of the watermarked image. Copy attacks and watermark changes are an example of these attacks. Any active attacks are malicious and others do not. The image enhancement or image degradation techniques may also carry out active attacks. Geometric attacks, particularly the projective, are a very destructive form of active attacks. The projective type adjusts the image content angle and parallels while the affine attack type maintains parallel and angle values[54].

As show in Fig. (10) the classification of watermarking attacks with subfields.

## 3.3 Image Watermarking Performances

### A. Security

Different encryption methods may confirm safety under which security levels are determined by the key. Several approaches, such as chaos-based, DCT (Discrete Cosine Transform), and mapping logistics, guarantee the protection and confidentiality of the embedded watermark [56]. The security of functional magnetic resonance imaging (fMRI) images in connection with brain activities is critical. To guarantee the integrity and accuracy of fMRI images, a watermarking scheme has been proposed which introduces a fragile reversible watermark scheme to characterize images of fMRI which are free of any formats. The system does not depend on external metadata [57]. The watermark is encoded and the safety of the watermarking algorithm is increased before embedding in binary pseudo-random sequences. The protective conditions may be met by telemedicine, visual imaging, messaging, multimedia data, etc. [58].

### B. Capacity

Capabilities Watermark (also referred to as payload) assesses the sum of information embedded into the host image based on the original data scale [59]. After inserting the watermark image the capability of

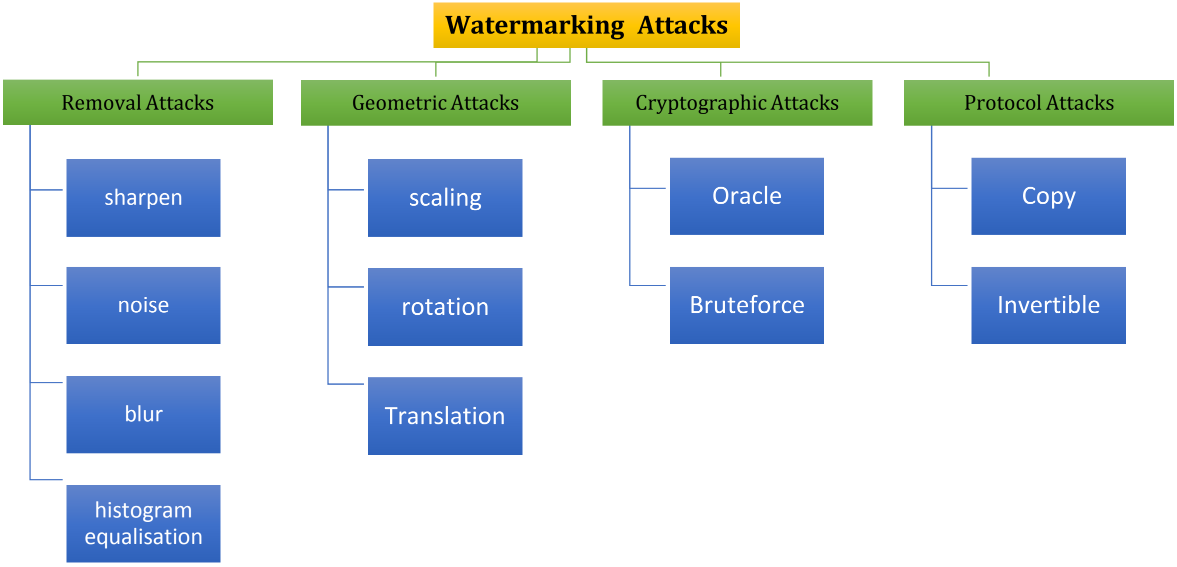

**Fig. 10. Classification of watermark attacks [55]**

each host image is calculated by the number of bits. More specifics on watermarks that need a pre-condition dependent on realistic applications are challenging, though [60].

In other terms, capability defines the limits of watermarking knowledge and thereby satisfies the robustness and imperceptibility of watermarking. The capabilities of watermarking are based on details present in the cover image to attackers, encoders, decoders, distortion restrictions, and the mathematical model. Various methods are used to test problems during assaults with watermarking. This involves Gaussian (PGC) theoretical and parallel channels [61].

Only when the channel capacity is higher than the number of bits that are embedded in the host image, the watermark extraction is successful. The capacity for watermarking was determined by the detection probability, the probability of false alarm, and the mean square error. More watermark data is seen in the host image as more data is added. In military and medical uses, though, distortion is not tolerable. Hence the implementation of watermarking techniques to minimize distortion by lower capacity in data embedding. A mixture of IWT, the bit plane technique, and the Fast Response code (QR), where the watermark can be transformed into QR-code, has been suggested. In this regard. This limits the embedding capacity by the proposed process [62].

### C. Robustness

The requirement for robustness is that after some conventional signal processing operations in digital watermark schemes, a watermark may be detected. These requirements include spatial filtering, color mapping, scanning, and printing. Other activities include optical analog (A/D), digital and digital (D/A), improving images, cutting, etc. There are many popular techniques to obtaining a high level of robustness including redundant incorporation, spectrum spreading, and watermarking. A successful digital image watermarking system should also be resilient against many attacks to prevent unauthorized distributors from deleting or excluding watermarking data. Not all watermarking algorithms may be stable at the same level, depending on the application. Others are resistant to various image processing processes, whereas others are vulnerable to additional attacks. [63]

## 4. IMAGE AUTHENTICATION BASED ON WATERMARKING

To ensure the image authentication with the watermarking approach with an appropriate level of security, the safer and more diverse use of authentication is provided. There are several common approaches to achieving high durability, including over-embedding, diffusion, and watermarks. A successful digital photo watermarking system also needs to be resilient against many attacks to prevent unauthorized distributors from deleting or excluding watermark data. Not all watermark algorithms may be stable at the same level, depending on the application. Others are resistant to various image processing operations, while others are vulnerable to additional attacks. Therefore, robustness can be classified into robust, fragile, and semi-fragile [63].

a. **Robust:** A robust robust watermark helps to prevent the data from several noisy assaults, geometrically and non-geometrically. And after many assaults, the watermark stays stable and the watermark is allowed to be detected. In various uses, including copyright and broadcast management, copy control, and fingerprinting, this watermark has used This watermark. [29]. Robust watermarking approach for the color of images is proposed by (A. K. Abdulrahman and S. Ozturk [64]), that dependent on the (DCT) and (DWT). With this approach, several image processing procedures on the watermarked images, including spin, redimension, filter, jpeg compression, or inclusion of noise, have shown the robustness of the proposed color image watermark. Experimental results show that the method suggested resists linear and nonlinear attacks and preserves the transparency of watermarked images. Moreover, A. K. Singh [65], suggested a robust watermarking method focusing on (LWT) and in telehealth applications (DCT). The medical picture of the host is 'signature watermark' and 'Patient Reports' are '64 to 64' to '80' in height. In addition, a message-digest (MD5) encodes the watermark signature, and the BCH error fixes the patient record with the error correction code before inserting it into the host image. Experimental demonstrations demonstrate the robustness and security of the procedure against multiple threats without significant cover and watermark distortions.

b. **Fragile:** Fragile watermarks are often used to validate the accuracy of multimedia data that may include signature details and content authentication. This watermark checks whether the image was manipulated or not. Normally, it is simple to execute a delicate method than a robust one. Binary authentication information was inserted into the image of the host where suspect tampering and localization by a fragile pixel watermarking technique was used. This led to a visually good result [66].

Extensive research on fragile watermark as follow;

A. Shehab et al. [67], proposed a new fragile method for medical applications, IA, and self-recovery watermarking. In the suggested system the distortion of the image is identified and the image is taken out. The host image is divided into 4 blocks, and the single SVD values are broken down to decide the transformation of the original image. In the image pixels, the block-by-button SVD is placed in a minor bit (LSB). The transformation to Arnold calculates the integration of self-recovery bits which, even after high disruptions, restore the original images. SVD-based watermark information improves IA and enables multiple attacks to be detected in the watermarked picture area. The exact position handling and the PSNR of the image retrieved are substantially enhanced by the scheme proposed.

J. J. Shen & et al. [68], proposed a fragile IA self-embedding approach focused on the decomposition of the singular value (SVD). The original image was divided into non-overlapping blocks first, and every block was subsequently divided into two sections: top and bottom. Using SVD, the upper and low sections of a block are authenticated, then concatenated for authentication code development after the block split. The assaulting experiments on the original picture were carried out to assess the robustness of the suggested technique. In a multitude of attacks, the experimental conclusions proved to be quite imperceptible. The suggested method precisely defined image manipulation and, after intensive manipulation, was able to obtain the managed image of high quality.

N. E. H. Goléa and K. E. Melkemi [69], Proposed the fragile watermarking medical image tamper detection area of interest (ROI) based. The proposed approach is focused on network propagation, which partitions the message into packets and provides redundant information for the processing of errors. One of the main instruments to monitor digital communications is the Cyclic Redundancy Check Code (CRC). The region to be covered is thus considered to be an error-free post. Therefore, the CRC code focuses on a common CRC-32 polynomial generator with certain mathematical properties that are used to generate a watermark that is located in each packet's space domain. For anomalies, at the end of the receipt, the watermark is extracted. The test results show the validity in terms of imperceptibility and performance of the proposed approach to secure and robust assaults.

B. Bolourian Haghighi & et al. [70], proposes a novel watermarking technique focused on (LWT) and (FNN) to detect and restore manipulation by hiding half-fragile data. The proposed approach outperforms similar works in terms of dominance, performance, and efficacy for applications including tamper detection and recovery.

c. **Semi-fragile:** This type of watermark does not work correctly in the presence of malicious transformations, but resists such transformations. A half-fragile watermark can be used for IA. A bi-orthogonal transform (APBT) and a single-value decomposition (SVD) algorithm are recommended to boost the robustness and imperceptibility of the watermarking method. In a neighborhood decided by selected applicant feature points, the block-based APBT algorithm is used. To construct a coefficient matrix for SVD, the APBT coefficients are used. To increase imperceptibility and robustness, it was suggested for the insert of the watermarked imagery to be focused on the Discreet wavelet transformation (DWT), all-phase discrete cosine-biorthogonal transform (APDCBT), and SVD, which use high-frequency sub-band (LH and HL) direct current (DC) coefficients. This technique is resistant to a variety of signal processing operations. [71,72]

More research on watermark have been conducted by the following researchers. These include;

Jobin Abraham & et al. [43], used Spatial domain techniques to produce high-quality watermarked images to incorporate watermark content. Spatial domain approaches are popular for delicate watermarks that sometimes store two or three minor picture bits of recovery information. Spatial domain approaches are explored via a robust copyright scheme. The algorithm is evaluated with various accuracy tests and the elimination of watermarks. The results show the imperceptible watermarking of the model and high strength to attack.

Swaraja K [73], optimized a novel robust hybrid for multiple watermarking schemes with the fusion of DWT and Schur, along with the training of the optimized FA, rather than the individual application of DWT, Schur, and FA or the DWT-Schur/DCTSchur group. The simultaneous insertion in a simultaneous test picture of multiple watermarks (text and image) provides extra security with standard ruggedness and imperceptibility efficiency. The watermarked image quality is also enhanced with the aid of Schur and FA, besides the robustness of the proposed algorithm. The projected approach uses two strong watermarks to endorse the actual case accounts and the hospital emblem in support of the root of the image for genuineness. The algorithm proposed also focussed more on enhancing the payload capacity, without compromising the imperceptibility and robustness of the algorithm even after different types of attack. The approach is robust in contrast to all calculated attacks that achieve a fair payload capability with the standards visual consistency of the medical watermarked image.

S. Koley [74], proposed the process embeds two watermarks into the host picture concurrently. The proposed scheme is extremely robust against geometric, signal processing, and hybrid assaults. Additionally, owing to the inclusion of the delicate watermark, it is capable of detecting and localizing picture tampering with extreme precision.

## 5. ASSESSMENTS AND RECOMMENDATIONS

Through the literature review of IA techniques presented in this paper, the concept of image content authentication, and the standards required for an effective watermark-based authentication system. The watermark framework has two important processes, embedding, and extraction. Watermarking schematics can be categorized into two main groups: spatial domain and transform frequency domain based on the field of work and each has its own set of pros and cons. The current image watermarking schematics based on both areas are discussed in the following subsections.

Spatial domain techniques apply directly to the original image by manipulating the pixel value during the embedding process based on the LSB technique, it is less complex, easy to implement, more capacitive but it has poor robustness. suggested several advancements in LSB for ensuring the accuracy of images and demonstrate a strong level of resistance to attacks such as [35–37,75].

While the frequency domain is found to be more powerful with the embedding process than the spatial domain, the image with watermark has good properties such as masking the invisible watermark bits, and the strength of some kinds of attacks, moreover, it can define tamper zone. On the other hand, it can be found that DWT is better for embedding as compared to DCT or DFT due to its effective multi-resolution properties of DWT. The watermarked photo under the transformation field is imperceptible and robust than digital watermarked photos [45–47].

Several watermarking schemes have been suggested. In the spatial domain, the watermark is embedded by changing the pixel values of the original image. In the frequency domain, the watermark is embedded by changing the values of its conversion coefficients. The frequency domain is more powerful and less sensitive when compared to spatial field methods. While the implanted technique in the spatial domain is simple, and it needs few requirements, but the frequency domain technique has more mathematical requirements, and some types are very complex.

Attack robustness is an important watermark parameter. It can be difficult to attain reach absolute against all and their variations of potential threats. Thus, the functional requirement is for an effective attack to affect the host data such that its economic importance is greatly reduced until it deteriorates to such an extent that it cannot be recovered. Power, durability, payload, and safety were achieved with DWT, RONI, and DWT-Schur technologies. But the most important DCT, DWT, and SVD technologies are used with hybrid methods for more image security. It should be noted that the robustness of data rates and imperceptibility also needs to be handled and that the optimal swap will depend on the application[43,64,68–70,73].

## 6. CONCLUSION AND FUTURE WORK

At the moment, due to the interactive and digital communication of multimedia data, information can be easily duplicated. As a result of this issue, digital image watermarking has become a significant area of research. Watermarking digital images with a variety of techniques has become a critical tool for image authentication, integrity verification, tamper detection, copyright protection, and digital security. We reviewed the most prevalent state-of-the-art watermarking techniques in this study. Due to the multi-resolution characteristics of DWT, DCT, DFT, and SVD, it can be concluded that they are a high-quality and robust technique for image watermarking. The essential requirements for designing an efficient watermarking system are robustness, imperceptibility, and capacity. However, meeting all of these requirements concurrently is nearly impossible. As a result, an appropriate trade-off must be maintained between these three requirements. However, security remains a significant issue in digital image watermarking technologies and researchers face a challenge in integrating IoT and blockchain-based authentication schemes. In the field of informatics and communications, authentication is the method by which it is possible to verify the authenticity of the identity of a person or entity, as it is claimed, to prevent impersonation. The digital watermark is a popular digital data security technique. Digital watermark deals with the merging of categorized data, digital watermark techniques have been divided into three main categories based on the field of work, the format of the document (text, image, music, or video), human perception, and algorithms. This paper reviewed summarize researchers' suggestions for watermarking images that help in promoting and protecting private data. Thus, future work can be expanded by combining different techniques from diverse domains to satisfy the three critical requirements outlined above. Additionally, to enhance robustness and security, researchers should concentrate on developing novel, advanced techniques.

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES

1. Sreenivas K, Kamkshi Prasad V. “Fragile watermarking schemes for image authentication: A survey,” Int. J. Mach. Learn. Cybern. 2018;9(7):1193–1218.
   DOI: 10.1007/s13042-017-0641-4.
2. Mohammed Munir Al-Naima F, Yousif Ameen S, Al-Naima F, Ameen SY, Al-Saad AF. “Destroying Steganography Content in Image Files Development of Optical Network Models for Quantum Cryptography View project AES Cryptosystem Development Using Neural Networks View project Destroying Steganography Content in Image Files,”; 2006.
   Accessed: May 09, 2021. [Online].
   Available:https://www.researchgate.net/publication/267369380.
3. Barni M, Bartolini F, Fridrich J, Goljan M, Piva A. “Digital watermarking for the authentication of AVS data,” Eur. Signal Process. Conf.; 2000.
4. Wang H, Eds AP, Goos G. Digital Forensics and Watermarking; 2019.
5. Mohsin Abdulazeez A, Zeebaree D, Zebari D, Hajy DM, Zeebaree DQ, Zebari A. “Structure of a typical research project View project Gait recognition with wavelet transform View project Robust watermarking scheme based LWT and SVD using artificial bee colony optimization,” Indones. J. Electr. Eng. Comput. Sci. 2021;21(2):1218–1229.
   DOI: 10.11591/ijeecs.v21.i2.pp1218-1229.
6. Ur-Rehman O, Zivic N. “Digital watermarking for image authentication,” Signals Commun. Technol. 2018;33–37.
   DOI: 10.1007/978-3-319-78942-2_4.
7. M. Azimpourkivi, “FIU Digital Commons Image-based Authentication,”; 2019.
8. Abdulrahman AK, Ozturk S. “A novel hybrid DCT and DWT based robust watermarking algorithm for color images,” Multimed. Tools Appl. 2019;78(12):17027–17049.
   DOI: 10.1007/s11042-018-7085-z.
9. Quiring E, Arp D, Rieck K. “Forgotten Siblings: Unifying Attacks on Machine Learning and Digital Watermarking,” Proc. - 3rd IEEE Eur. Symp. Secur. Privacy, EURO S P. 2018;488–502.
   DOI: 10.1109/EuroSP.2018.00041.
10. El Bakrawy LM, Ghali NI, Ella Hassanien A. “Intelligent Machine Learning in Image

Authentication,”. J. Signal Process. Syst. 2015;78(2):223–237.
DOI: 10.1007/s11265-013-0817-4.

11. Hassan O, et al. “Hiding image by using contourlet transform a review on region of interest segmentation based on clustering techniques for breast cancer ultrasound images view project knowledge exchange, view project hiding image by using contourlet transform.” ; 2021.
Accessed: Apr. 20, 2021. [Online].
Available:https://www.researchgate.net/publication/342397936.
12. Hilal M, Ameen SY, Al-Badrany MR. “Optimal image steganography content destruction techniques,”; 2018.
Accessed: May 09, 2021. [Online].
Available:https://www.researchgate.net/publication/328450232.
13. A. Mahmud, B. Esakki, and S. Seshathiri, “Quantification of groundnut leaf defects using image processing algorithms,” in Advances in Intelligent Systems and Computing, 2021, vol. 1309, pp. 649–658, doi: 10.1007/978-981-33-4673-4_53.
14. Mohammed Munir Al-Naima F, Yousif Ameen S, Al-Naima F, Ameen SY, Al-Saad AF. “Destroying steganography content in image files neural network-based stream image encryption view project encoder and decoder view project destroying steganography content in image files,”; 2006.
Accessed: Apr. 20, 2021. [Online].
Available:https://www.researchgate.net/publication/267369380.
15. Brifcani AMA, Al-Bamerny JN. “Image compression analysis using multistage vector quantization based on discrete wavelet transform,” in Proceedings of 2010 International Conference on Methods and Models in Computer Science, ICM2CS-2010. 2010;46–53.
DOI: 10.1109/ICM2CS.2010.5706717.
16. Hilal M, Ameen SY, Al-Badrany MR. “Optimal image steganography content destruction techniques,”; 2018.
Accessed: Apr. 20, 2021. [Online].
Available:https://www.researchgate.net/publication/328450232.
17. Shah P. “Image based Authentication System,” no. December. 2018;0–4,
18. Jabbar K. Kadhim. “Image Authentication Subject Review,” Int. J. Eng. Res. Adv. Technol., 2018;4(12):13–18.
DOI: 10.31695/ijerat.2018.3352.
19. Mushtaq S, Mir AH. “Digital image forgeries and passive image authentication techniques: A Survey.” Int. J. Adv. Sci. Technol. 2014;73:15–32.
DOI: 10.14257/ijast.2014.73.02.
20. Srinivas TAS, Ramasubbareddy S, Govinda K, Manivannan SS, “Web image authentication using embedding invisible watermarking.” Springer, Singapore. 2020;207–218.
21. Khurana M, Singh H. “Two level phase retrieval in fractional Hartley domain for secure image encryption and authentication using digital signatures,” Multimed. Tools Appl. 2020;79(19–20):13967–13986.
DOI: 10.1007/s11042-020-08658-3.
22. Salah E, Amine K, Redouane K, Fares K. “A Fourier transform based audio watermarking algorithm,” Appl. Acoust. 2021;172:107652,
DOI: 10.1016/j.apacoust.2020.107652.
23. Sudha MS, Thanuja TC. “Digital Image Authentication ( Dia ) - a Survey,” no. March 2014. 2014;73–78,
24. Singh P, Agarwal A, Gupta J. “Image watermark attacks: Classification and Implementation,” Int. J. Electron. Commun. Technol. 2013;4(2):95–100.
25. Shrivastava V. “Analysis of Attacks on Hybrid DWT-DCT Algorithm for Digital Image Watermarking With MATLAB,”. 2014;2(3):123–126,
26. Zebari DA, Zeebaree DQ, Saeed JN, Zebari NA, Al-Zebari A. “Image Steganography Based on Swarm Intelligence Algorithms: A Survey.”; 2015.
27. Kakkad V, Patel M, Shah M. “Biometric authentication and image encryption for image security in cloud framework,” Multiscale Multidiscip. Model. Exp. Des. 2019;2(4):233–248.
DOI: 10.1007/s41939-019-00049-y.
28. Kalligeros E, Karousos N, Karybali IG. “Oracle-based Logic Locking Attacks: Protect the Oracle Not only the Netlist,” in Proceedings of the 2020 Design, Automation and Test in Europe Conference and Exhibition, DATE 2020. 2020;939–944.
DOI:
10.23919/DATE48585.2020.9116463.
29. Ahmadi SBB, Zhang G, Wei S. “Robust and hybrid SVD-based image watermarking schemes:: A survey,” Multimed. Tools Appl. 2020;79(1–2):1075–1117.
DOI: 10.1007/s11042-019-08197-6.

30. Lee CF, Shen JJ, Chen ZR. "A survey of watermarking-based authentication for digital image," 2018 3rd Int. Conf. Comput. Commun. Syst. ICCCS. 2018;239–243. DOI: 10.1109/CCOMS.2018.8463259.
31. Begum M, Uddin MS. "Digital image watermarking techniques: A review," Inf. 2020;11(2). DOI: 10.3390/info11020110.
32. MPR, Khanapuri JV. "A Study on Image Authentication Methods," pp. 1719–1721, 2018.
33. Al-ghadi MQ. "Watermarking approaches for images authentication in applications with time constraints To cite this version: HAL Id : tel-01967625 A pproches de tatouage pour l ' authentification de l ' image dans des,"; 2019.
34. Soualmi A, Alti A, Laouamer L, Benyoucef M. A blind fragile based medical image authentication using schur decomposition,. Springer International Publishing. 2020;921.
35. Das S, Sunaniya AK, Maity R, Maity NP. "Efficient FPGA implementation of corrected reversible contrast mapping algorithm for video watermarking," Microprocess. Microsyst. 2020;76:103092. DOI: 10.1016/j.micpro.2020.103092.
36. Arun Kumar C, Sooraj MP, Ramakrishnan S. "A comparative performance evaluation of supervised feature selection algorithms on microarray datasets," Procedia Comput. Sci. 2017;115:209–217. DOI: 10.1016/j.procs.2017.09.127.
37. Pearson K. " LIII. On lines and planes of closest fit to systems of points in space ," London, Edinburgh, Dublin Philos. Mag. J. Sci. 1901;2(11):559–572. DOI: 10.1080/14786440109462720.
38. Tarmal TA, Saha C, Hossain MF, Rahman S. "Integer wavelet transform based medical image watermarking for tamper detection," 2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE. 2019;7–9. DOI: 10.1109/ECACE.2019.8679152.
39. Prajwalasimha SN, Chethan SS, Mohan CS. "Performance analysis of DCT and successive division based digital image watermarking scheme," Indones. J. Electr. Eng. Comput. Sci. 2019;15(2):750–757. DOI: 10.11591/ijeecs.v15.i2.pp750-757.
40. Sankaran KS, Abhi Rayna H, Mangu V, Prakash VR, Vasudevan N. "Image water marking using DWT to encapsulate data in medical image," Proc. 2019 IEEE Int. Conf. Commun. Signal Process. ICCSP. 2019;568–571. DOI: 10.1109/ICCSP.2019.8698057.
41. Rakhmawati L, Wirawan W, Suwadi S. "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," Eurasip J. Image Video Process. 2019;2019(1). DOI: 10.1186/s13640-019-0462-3.
42. Mohsin Abdulazeez A, Zeebaree D, Zeebaree DQ, Abdulqader DM. "Wavelet applications in medical images: A review,"; 2021. Accessed: Apr. 20, 2021. [Online]. Available: https://www.researchgate.net/publication/341977072.
43. U. 004 932, Ruban I, Bolohova N, Martovytskyi V, Koptsev O. "Methods of information systems protection," Сучасні інформаційні системи. 2021;5(1). DOI: 10.20998/2522-9052.2021.1.16.
44. Singh RK, Shaw DK, Jha SK, Kumar M. "A DWT-SVD based multiple watermarking scheme for image based data security," J. Inf. Optim. Sci. 2018;39(1):67–81. DOI: 10.1080/02522667.2017.1372153.
45. Soualmi A, Alti A, Laouamer L. "A novel blind watermarking approach for medical image authentication using MinEigen value features," Multimed. Tools Appl. 2021;80(2):2279–2293. DOI: 10.1007/s11042-020-09614-x.
46. Kahlessenane F, Khaldi A, Kafi R, Euschi S. "A DWT based watermarking approach for medical image protection," J. Ambient Intell. Humaniz. Comput., no. 0123456789; 2020. DOI: 10.1007/s12652-020-02450-9.
47. Soualmi A, Alti A, L L-M, T. and Applications and undefined, "A novel blind watermarking approach for medical image authentication using MinEigen value features," Springer; 2020. Accessed: Apr. 04, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s11042-020-09614-x.
48. Sharma N, Saroha K. "A novel dimensionality reduction method for cancer dataset using PCA and Feature Ranking," 2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI. 2015;2261–2264. DOI: 10.1109/ICACCI.2015.7275954.
49. Zeebaree DQ, Abdulazeez AM, Mohammed O, Hassan S. "Hiding image by using contourlet transform,".

2020;16979–16990.

50. SMA Shefa A Dawwd Laith M. Fawzi, Siddeeq Y. Ameen, “Embedded Real-Time Video Surveillance System based.-Google Scholar.”; 2021.
Available:https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Embedded+Real-Time+Video+Surveillance+System+based+on+Multi-Sensor+and+Visual+Tracking&btnG=
(accessed May 29, 2021).

51. LM Fawzi SA, Ameen SY. “Fawzi: Embedded real-time video surveillance system... - Google Scholar.”; 2021.
Available:https://scholar.google.com/scholar?cluster=1331130053108737341&hl=en&oi=scholarr
(accessed May 29, 2021).

52. Su Z, Yao L, Mei J, Zhou L, Li W. “Learning to hash for personalized image authentication,” IEEE Trans. Circuits Syst. Video Technol. 2020;1–1.
DOI: 10.1109/tcsvt.2020.3002146.

53. Kadian P, Arora SM, Arora N. “Robust digital watermarking techniques for copyright protection of digital data: A survey,” Wireless Personal Communications. Springer; 2021.
DOI: 10.1007/s11277-021-08177-w.

54. Sherekar S, Thakare V, Jain S, Ashwini T, Tijare P, Deshpande M. “Attacks and countermeasures on digital watermarks: Classification, implications, benchmarks,” Int. J. Comput. Sci. Appl. 2011;4(2):32–45.

55. Mohanarathinam A, Kamalraj S, Prasanna Venkatesan GKD, Ravi RV, Manikandababu CS. “Digital watermarking techniques for image security: a review,” J. Ambient Intell. Humaniz. Comput. 2020;11(8):3221–3229.
DOI: 10.1007/s12652-019-01500-1.

56. Wang H, Jing X, Niu B. “A discrete bacterial algorithm for feature selection in classification of microarray gene expression cancer data,” Knowledge-Based Syst. 2017;126:8–19.
DOI: 10.1016/j.knosys.2017.04.004.

57. Chand Bansal J, Nagar AK. “Algorithms for intelligent systems series editors,”; 2019.[Online].
Available:
http://www.springer.com/series/16171.

58. Vora S, Yang H. “A comprehensive study of eleven feature selection algorithms and their impact on text classification,” Proc. Comput. Conf. 2017;2018:440–449.
DOI: 10.1109/SAI.2017.8252136.

59. Lee SJ, Xu Z, Li T, Yang Y. “A novel bagging C4.5 algorithm based on wrapper feature selection for supporting wise clinical decision making,” J. Biomed. Inform. 2018;78:144–155.
DOI: 10.1016/j.jbi.2017.11.005.

60. Verma G, Liao M, Lu D, He W, Peng X. “A novel optical two-factor face authentication scheme,” Opt. Lasers Eng. 2019;123:28–36.
DOI: 10.1016/j.optlaseng.2019.06.028.

61. Garg P, Kishore RR. “Performance comparison of various watermarking techniques,” Multimed. Tools Appl; 2020.
DOI: 10.1007/s11042-020-09262-1.

62. Tenenbaum JB, De Silva V, Langford JC. “A global geometric framework for nonlinear dimensionality reduction,” Science (80-.). 2000;290(5500):2319–2323.
DOI: 10.1126/science.290.5500.2319.

63. Laouamer L, Tayan O. “Performance evaluation of a document image watermarking approach with enhanced tamper localization and recovery,” IEEE Access. 2018;6:26144–26166.
DOI: 10.1109/ACCESS.2018.2831599.

64. Taleby Ahvanooey M, Li Q, Shim HJ, Huang Y. “A comparative analysis of information hiding techniques for copyright protection of text documents,” Security and Communication Networks, 2018. Hindawi Limited. 2018;1–22.
DOI: 10.1155/2018/5325040.

65. Singh AK. “Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image,” Multimed. Tools Appl. 2019;78(21):30523–30533.
DOI: 10.1007/s11042-018-7115-x.

66. Singhal S, Ranga V. “Passive authentication image forgery detection using multilayer cnn,” in Lecture Notes in Networks and Systems. 2021;140:237–249.
DOI: 10.1007/978-981-15-7130-5_18.

67. Shehab A, et al. “Secure and robust fragile watermarking scheme for medical images,” IEEE Access. 2018;6(c):10269–10278.
DOI: 10.1109/ACCESS.2018.2799240.

68. Shen JJ, Lee CF, Hsu FW, Agrawal S. “A self-embedding fragile image authentication based on singular value decomposition,” Multimed. Tools Appl; 2020.
DOI: 10.1007/s11042-020-09254-1.

69. Goléa NEH, Melkemi KE. “ROI-based fragile watermarking for medical image tamper detection,” Int. J. High Perform. Comput. Netw. 2019;13(2):199. DOI: 10.1504/ijhpcn.2019.097508.

70. Bolourian Haghighi B, Taherinia AH, Monsefi R. “An effective semi-fragile watermarking method for image authentication based on lifting wavelet transform and feed-forward neural network,” Cognit. Comput. 2020;12(4):863–890. DOI: 10.1007/s12559-019-09700-9.

71. Feng B, Li X, Jie Y, Guo C, Fu H. “A novel semi-fragile digital watermarking scheme for scrambled image authentication and restoration,” Mob. Networks Appl. 2020;25(1):82–94. DOI: 10.1007/s11036-018-1186-9.

72. Sivasubramanian N, Konganathan G. “A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT,” Computing. 2020;102(6):1365–1384. DOI: 10.1007/s00607-020-00797-7.

73. Swaraja K. Medical image region based watermarking for secured telemedicine. 2018;77(21).

74. Koley S. “Visual attention model based dual watermarking for simultaneous image copyright protection and authentication,” Multimed. Tools Appl; 2020. DOI: 10.1007/s11042-020-09918-y.

75. Boujemaa N, Aissaoui Abdelaziz E, Yousef EM, Rachid L, Aziz BM. “Fragile watermarking of medical image for content authentication and security,” IJCSN Int. J. Comput. Sci. Netw. 2016;5(5):2277–5420. [Online]. Available: www.IJCSN.org.

*Peer-review history:*
*The peer review history for this paper can be accessed here:*
*http://www.sdiarticle4.com/review-history/69033*