Multimedia Tools and Applications (2020) 79:25921–25967
https://doi.org/10.1007/s11042-020-09262-1

Performance comparison of various watermarking techniques

Preeti Garg [1,2] · R. Rama Kishore [1]

Received: 13 August 2019 / Revised: 18 May 2020 / Accepted: 24 June 2020 /
Published online: 8 July 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
Digital watermarking is a method to provide authenticity and copyright ownership to digital content by embedding any presume content like audio, text, data or video into the original content. This embedding of data should not damage the quality of the original content and should fulfill its objective also. From a decade a number of researchers are working on watermarking for providing security, robustness and imperceptibility to the digital images. This paper describes the information about watermarking in terms of its characteristics, application areas, types and various attacks performed on it. A comparative study of various techniques used in the field of watermarking is provided here by measuring their performance in terms of various characteristics. A number of performance measures used by various researchers are also discussed here along with possible attacks. This paper can help researchers to find various techniques used in watermarking field and their performances against various attacks for further proceedings.

Keywords Digital watermarking · Robustness · Imperceptibility · DCT · DWT · SVD · CNN · NN

1 Introduction

Today all information is available in digital form on the internet. This availability of data on internet allows users to share and access all the data and information in digital form which infringes the law of copyright ownership. The information contained in watermarked content can be used for communication between sender and receiver and no one else will know its

✉ Preeti Garg
preeti.itgarg@gmail.com

R. Rama Kishore
ram_kish@yahoo.com

[1] University School of Information & Communication Technology, Guru Gobind Singh Indraprastha University, Dwarka, New Delhi, India

[2] Department of CSE, SGT University, Gurugram, India

existence in carrier content. [93]. Digital watermarking allows the user to add a design like a logo or image in some cover image to prove authenticity, copy control, fingerprinting and ownership. Digital watermarking has various applications like copyright protection, digital right management, fingerprinting, image and content authentication, tamper proofing and many more [81]. A watermarking algorithm should maintain the quality of the original image as well as it should embed watermark in such a way that watermarked image shows robustness against various attacks like Gaussian noise, JPEG compression or rotational attacks [128]. Watermarking can be done on any text, image, audio or video.

In this paper authors have focused on watermarking work done on digital images. Watermarking on images can be done in spatial and transform domain. In spatial pixel values are used for embedding while in transform domain, first the pixel values are converted into frequency coefficients and then these are used for embedding. There are various frequency domain techniques like DCT, DWT, DFT, RDWT, quaternion discrete Fourier transform (QDFT), LWT and many more. Ordered Hadamard Coefficient is used in [27] to convert original and watermark image into transform domain, and achieved shorter processing time. Researchers have used these techniques to convert images into transform domain. Each of these techniques has their own merits and demerits at particular condition which are explained in Section 4. In spatial domain Least Significant Bits (LSB) of images are used for embedding the watermark but these techniques are not very robust against various image processing attacks like rotation, cropping, clipping, JPEG compression and geometric attacks. So after seeing the work of authors in [18] most of the researchers have used transform domain techniques. Here authors have proposed a secure watermarking for multimedia contents which shows more robustness than spatial domain techniques. There are various characteristics of watermarking which are explained in Section 1.2. Most of the researchers have worked to find a stability between robustness and imperceptibility. Robustness is its capacity to handle any attack and imperceptibility is resemblance of original and watermarked image. These two characteristics are very important to achieve as these are inversely proportional to each other. Robustness is measured by the parameters like NC, BER, Bit Correct Ratio (BCR), CC (Correlation Coefficient), Tamper assessment function (TAF) metric while imperceptibility is measured by using PSNR, SSIM and MSE. Some of the performance measurement parameters are explained in Section 2. A large value of Peak Signal to Noise Ratio indicates that there is more similarity between watermarked and original image [106]. Commonly a watermarked image with PSNR value greater than 27 dB and NC value greater than 0.7 is found satisfactory [107].

Section 1.1 describes the procedure of watermarking and 1.2 shows its characteristics. Various types of watermarking are shown in 1.3 and types of attacks in watermarking field are explained in 1.4. Section 2 shows various performance measures used by various researchers. Section 3 gives a detail study of watermarking and Section 4 explained the summary of the research. Finally Section 5 concluded the work and shows its future directions.

1.1 Watermarking procedure

Watermarking hides the important information into the host image, audio, text or video. Basically two processes are involved in watermarking. First embedding and second is called extraction. Embedding is performed by owner of the content to add ownership to the content and extraction is performed at receiving end to proof the ownership. Watermark embedding and extraction process are opposite to each other but are related also, and embedding should be

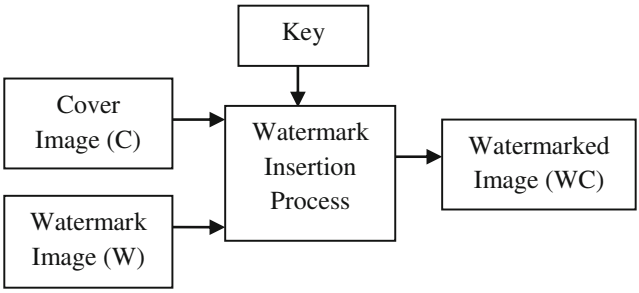


Fig. 1 Embedding process of watermark

done in a manner that extraction of it can be performed only by the authorized users. The watermark procedure can be explained in two steps.

A. **Watermark Embedding:** In watermark embedding first a watermark is inserted into cover/host image C using some embedding algorithm and a key generated by some procedure which is used at the time of extraction also. Now this watermarked image is available for the users. This watermarked image can be imposed to various image processing attacks and other attacks also which will change the watermarked image WC by WC′. The noise can be calculated by simply finding the difference between original watermarked image (WC) and extracted watermark (W′) using various measurement methods like NC, BER, CC. Figure 1 shows this complete procedure of embedding.

B. **Watermark Extraction:** Extraction is based on embedding process and it is a function of watermarked image, cover iamge,, key and test data [7]. The complete process of watermark extraction is shown in Fig. 2 which includes the extraction algorithm key and the watermarked image; in some cases it may also need the original image. The extraction process of watermarking is of three types.

(i) Non-Blind approach: This is the one in which cover image as well as the original watermark are required at the time of extraction. The equation of non blind approach is shown in Eq.1.

(ii) Semi-Blind Approach: In semi blind approach the original cover image is not required at the time of extraction but the key used for embedding, original watermark and the watermarked images are needed. The extraction process of semi-blind approach is shown in Eq.2.

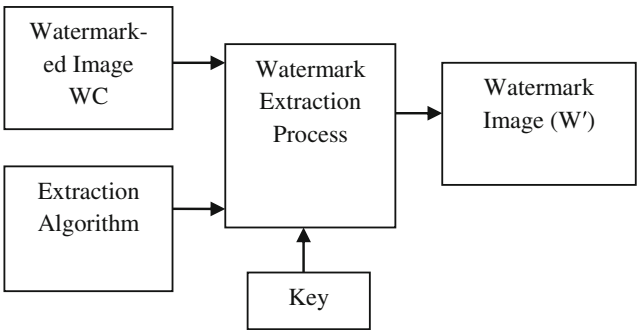


Fig. 2 Extraction Process of watermark

(iii) Blind- approach: A blind approach extracts the image on the basis of WC and key only and does not require cover image C or the original watermark. Blind approach is more secure than other two because in this the receiver of the image does not have any information about the original cover and embedded watermark image. A number of researchers have used neural network, Convolution Neural Network (CNN) and other techniques to make their algorithms blind or semi blind. The equation of it is shown in Eq. 3.

$$Extraction\ (Non{-}Blind)[K, C, W, WC] = W' \tag{1}$$

$$Extraction\ (Semi{-}Blind)[K, W, WC] = W' \tag{2}$$

$$Extraction\ (Blind)[K, WC] = W' \tag{3}$$

$$Where, K = Key\ used\ for\ embedding$$
$$C = Original\ Cover\ Image$$
$$W = Watermark\ Image$$
$$WC = Watermarked\ Image$$
$$W' = Extracted\ Watermark$$

1.2 Characteristics of watermarking

There are numerous types of characteristics which a watermark algorithm should acquire. These are explained below and shown in Fig. 3.

A. **Robustness:** Robustness shows how effective the watermarking is against various types of attacks. This characteristic is used to match the extracted watermark and the original watermark. The more similarity between these two the more robust the scheme is. Once the data is available over the internet a number of persons can use that data and modify it by performing various types of attacks on it, a watermark is called robust if it remains same before and after the attacks. Various types of attacks like image processing, geometric, Noise are explained in Section 1.4. One of the most used measurement parameter of robustness is Normalized correlation (NC) which determines the relation between extracted and original watermark. The value of the NC coefficient lies between o and 1, more the value closer to 1 higher is its robustness. If $W = W'$ then we say that scheme is robust and extracted watermark (W') is equals to the original one (W).

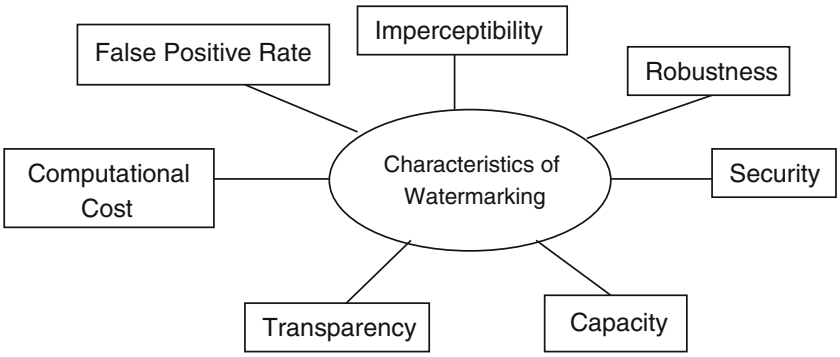


Fig. 3 Characteristics of Watermarking

B. **Imperceptibility:** Imperceptibility means the resemblance between the original and watermarked image [44]. Once a user uses any image available on the network, he should not be able to view the watermark embedded into image in case of invisible watermarking. This characteristic shows invisibility of the watermark content in watermarked image. One of the main problems of watermarking is to find a balance between imperceptibility and the robustness as these two are opposite to each other. Increasing the value of one decreases the other, so finding a trade-off between these two is a challenging task. A lot of researchers have worked in the field of image watermarking, some of them have worked only to provide one characteristics while others have provide schemes which provides balance between these two most important properties.

C. **Security:** One of the main characteristics of watermarking is security that is to resist the integrity and confidentiality of the watermark against various attacks performed by some unauthorized persons. An attacker should not be able to detect the watermark, which is called unauthorized detection, he should not be able to change it, called unauthorized modification or should not be able to embed some other data in the watermarked image, called unauthorized embedding. So security means to protect the watermarked image from unauthorized detection, modification and embedding of new content. The watermark should be robust and fragile or semi- fragile, fragile means authentication so there should not be any unauthorized access of watermark. Arnold transform is one of the techniques which provide security to the data by adding some secret key to the watermarked image. Many researchers have used Arnold transform to provide security like [97] have used Arnold technique to scramble the watermark by using secret key before embedding it to the cover image so if any unauthorized user became successful in extracting the watermark, he will not be able to understand it as it is a scrambled watermark and can only be detected by knowing the secret key. Some researchers have encrypted the watermark and then embedded it to the cover image using DES (Data Encryption Standard) encryption technique, or by using other encryption algorithms so that only an authorized user can decrypt the watermark after extraction of it.

D. **Capacity:** Capacity defines how much embedding can be done on cover image. It means that cover image should be able to handle the load of watermark image or in other words capacity means the quantity or volume of information a particular carrier data can handle. Capacity is also knows as payload means load capacity of the carrier content without losing its originality. Increasing the volume of the watermark data in cover image, will also make its imperceptibility poor and decreased robustness against various attacks. So there should be balance between capacity, robustness and imperceptibility [64].

E. **Transparency:** Once a watermark is embedded in the cover data, it should not affect the quality of it that is no loss of information should be there except some changes in its contrast or brightness etc. There should be transparency while embedding the watermark information carried by the cover content. Some of the researchers have used HVS (Human Visual System) [95] in consideration while embedding a watermark. HVS means how human visualize any image, the areas where users have less interest like low contrast pixels places can be used to embed the watermark.

F. **Computational Cost:** The scheme which is being used by researcher for embedding the watermark should not be very complex because it will increase its computational cost. The cost

of embedding and extraction of watermark should be according to the need of the owner of the image, the more complex algorithm is, the more will be its cost in terms of time taken to run that algorithm. So, the word computational cost is the cost or time taken by the algorithm to computer the watermarked image and to extract the embedded watermark.

G. **False Positive Rate:** False Positive Rate or FPR means detection of a watermark form watermarked image even though there was no watermark embedded in it [82]. Some attackers use the FPR property of the watermark to make it their own by detecting presence of their own watermark in the carrier image. Some Researchers have used SVD (Singular Value Decomposition) technique to embed the watermark but this particular technique is not able to remove the problem of false positive so hybrid techniques are used in combination with SVD.

1.3 Watermarking types

There are various categorizations of watermarking like on the basis of perceptibility, according to application on which watermarking is performed, according to domain and many more as shown in Fig. 4. These are as follows:

A. **According to perceptibility:** Perceptibility means the visibility of the watermark embedded in the carrier image. On the basis of perceptibility/ visibility watermarking can be of visible and invisible type.

(i) Visible Watermark: It means which a user can view embedded in the cover image like for example a logo of a company is added in background of some document or a TV news channel showing their news and have a logo of their channel on that particular news, an example of it is shown in Fig. 5(a). In this image we can see that a watermark logo image is embedding in a cover image called Lena which is very famous image in image processing field, the reason of adding a visible watermark is that any unauthorized user should know that this content belongs to some other person and it cannot be used for other's for their benefits.

(ii) Invisible Watermark: Invisible watermark is which a user cannot see embedded in some cover image it is also called imperceptible as it is embedded by some algorithm so that a person cannot see it easily. An example of invisible watermark is shown in Fig. 5(b). In this image we cannot see whether any watermark is embedded in it or not. A user can use this image but cannot extract the watermark embedded in it or modify it. This type of watermark embedding is done to prove the original owner of that particular content.

B. **According to accessibility:** Accessibility means who can access the watermark embedded in the watermarked image. According to accessibility a watermark is of two types private or public.

(i) Private: The word private means secret that is the presence of the watermark in a particular image is known to an authorized user only and these users can only see or

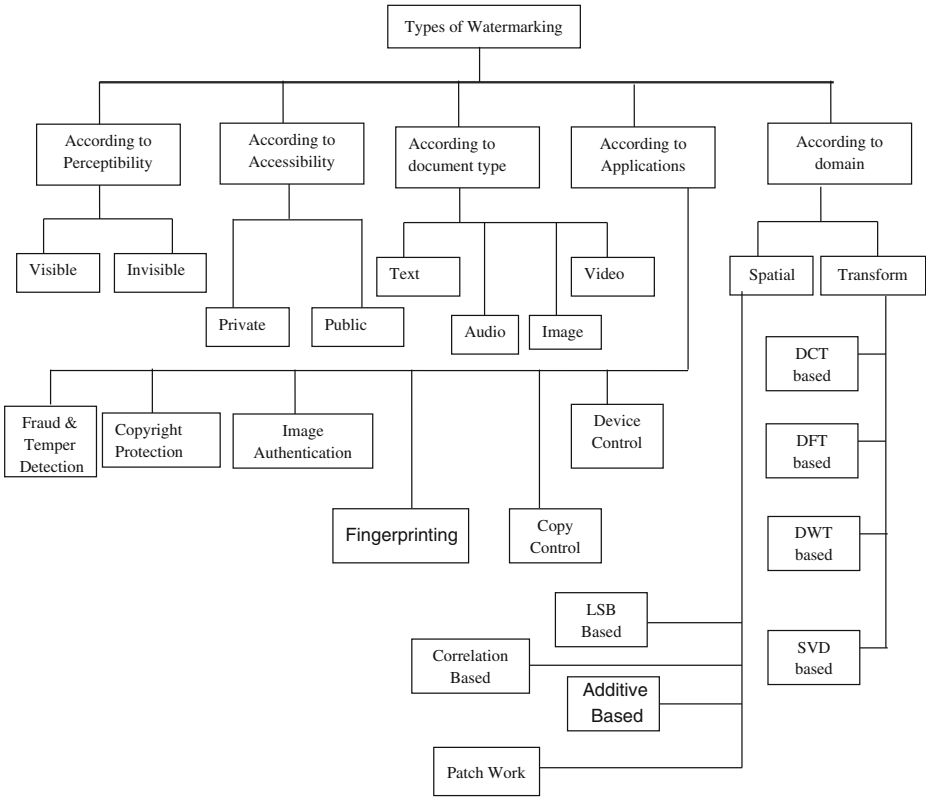


Fig. 4 Types of Watermarking

detect the watermark embedded in the carrier image. At embedding side some secret key is used to embed the watermark and only some authorized users know that secret key which they can use for extraction also.

(ii) Public: Public means which is known to everyone or some targeted audience. A public watermark is embedded in a location which is known to everyone and these users can extract or view the watermark embedded in the carrier image. Public watermarks are not secure and any person can modify these easily because they know the key used for embedding the watermark, so in general private watermark are more robust than public against various attacks.

C. **According to document:** According to the type of the document on which watermark is to perform it can be text, audio, image or video watermark.

(i) Text: Text watermark means a text is embedded in some carrier data like authorized person name or any id. These are easier to embed than image or video watermarks. Text watermarking is used to provide copyright protection for text document as well as it eliminates various problems like tempering of data, unauthorized access. Ref [84] has reviewed various methods like structural and linguistic approaches used for text watermarking and also addresses various applications of it.

(a) **(b)**

Fig. 5. **a** visible watermark and **b** invisible watermark

(ii) Audio: In audio watermarking a watermark is embedded in the audio signal to provide copyright protection to the audio content. Any unauthorized user can use bit by bit signal value to find the embedded watermark [10]. In case of audio the watermarking should be robust against various signal processing attacks like MPEG compression, filtering, sampling and others. [41] has reviewed various watermarking techniques which have been used in the field of audio watermarking in last 20 years.

(iii) Image Watermarking: A huge amount of digital images are available over the network to everyone, so there is a need to secure it from unauthorized access as well as to provide ownership of the data. Image watermarking is a technique in which a watermark is added in an image to provide these facilities. This paper has reviewed various techniques which have been used in the field of image watermarking. In a cover image, an image, text or both can be embedded as watermark like in medical applications along with image, data like owners ID or digital signatures are embedded so that its ownership and security can be maintained.

(iv) Video watermarking: In video watermarking a text, audio or image is embedded as watermark in a video frame so that its ownership and other features can be maintained. Video watermarking can be understood like images as a video is collection of various images used in a frame so techniques used in image watermarking with some advancement can be used for video as well but it is not just an extension of the still images, video watermarking is much more than the image watermarking [25]. One of the best uses of video watermarking is to differentiate an original movie from the pirated one. A watermark can be embedded in an original movie so that if someone makes a copy of it, a proof can be generated that this copy is a pirated one, and the original movie belongs to a particular person. Paper [11] reviews various techniques used in the field of video watermarking, it also covers the challenges faced in this.

D. **According to the applications:** Watermarking can be classified according of its applications for various purposes. Some of the applications of it are explained here.

(i) Copyright Protection: Watermarks are added to the carrier or original image to prove its originality and its rightful owner. Once a watermark is embedded in a digital image, it can

be extracted from the watermarked image by comparing it with the original image; this extracted watermark proves the copyright ownership of that image. In case of videos also it is very important to identify the original owner of it, so watermarks are added into particular frames which can be used to differentiate it from the pirated copies of it and shows the copyright owner of that particular video. In [101] DWT scheme is used to provide the content authentication and copyright protection of the original images.

(ii) Image Authentication: In real world any document is called authenticated if it has a signature of its owner. The word authentication means to verify the authentic user of that particular content either image, data or video. In digital world digital signatures are applied on any digital content to authenticate that data, for this owner uses some private key to generates his digital signature and embed it in the carrier content for its authentication. The receiver extracts this digital signature using his public key and verifies whether the content comes from a genuine person or not. So digital watermarking is used to authenticate any content available over the internet by adding some watermark into it which can only be detected by some authorized persons who have the key of its extraction. Authors in [61] have used biometric images as a watermark for providing confidentiality and authenticity of the digital content.

(iii) Fingerprinting: It is used to protect the unauthenticated distribution of the watermarked content [105]. Fingerprinting can be explained like a face recognition system or an iris detection machine, which is used to identify a particular person. Similarly to identify the identity of a particular content a fingerprint like owner's id or a unique number is added into the digital content to identify its owner and to differentiate between a pirated copy and the original one. Fingerprinting helps to prevent illegal copying of a particular content and its redistribution. The scheme used for adding watermark should be robust against various attacks like copying of data, forgery, rotation, clipping etc. so that the watermark extracted will be same as the embedded one and can be used to prove the owners identity.

(iv) Copy Control: The copy control scheme prevents multiple copying of the data by adding some watermark in digital content which gives some information about number of copies allowed for a particular content and when someone copies that content exceeding this limit, it will control it. One of the best applications of it is in movies. People use cameras within theatre to copy a film and then make a pirated copy of it. The solution of this problem can be implemented by embedding a watermark in the background of that movie which may includes theatre name, date and location information so that when someone makes a copy of it, authorized users can detect the watermark embedded in it and with the help of the extracted watermark the information about that theatre can be extracted which can control the further copying of the movie.

(v) Device Control: Watermarking is used to identify the authenticated device on which a particular audio, video or image should run. This type of watermarking scheme embeds a watermark which includes some code that can only be executed by any verified devices. In that device this code is first extracted and then that particular content can run on the device. An example of device control is like televisions where a particular video plays only a particular channel which can extract that secret code embedded in that video.

(vi) Fraud and temper detection: Watermarks are embedded on the original images to identify if someone has tempered it intentionally for his own benefits. Once a watermark is embedded in digital content an authorized user can extract it to check any unauthorized modifications, in the digital content. The watermark added should be robust against various attacks so that it can detect the frauds and tempering done in the original content. Many authors have used multiple

watermarking technique for authentication and temper recovery of the original content. Here, the term multiple watermarking is that an image is divided into multiple blocks and then different types of embedding techniques are used for different types of blocks to provide more security to the watermark.

Some other applications of watermarking are broadcast monitoring, medical applications, digital right management, electronic voting system, ID card security etc.

E. **According to the domain:** It can be of two types:

i. Spatial domain watermarking: In this watermark bits are added straight to the pixel values of cover image by changing its grey level pixel values to the pixel values of the watermark image. This technique has less complexity and is very easy to implement but the information inserted in pixel value can easily be detected by unauthorized persons. The watermarks embedded by this scheme provides more imperceptibility in comparison to the robustness because these schemes are very open to various types of attacks but spatial domain scheme are capable of hiding more capacity of the data. Some of the techniques are explained here which uses spatial domain for watermarking.

- LSB (Least Significant Bit): It is one of the simplest technique of spatial domain, in this image is converted into 8 bit plane and the LSB bit or 8th plane is used for embedding the watermark because LSB carries less information and it has less effect on the image. One of the benefits of LSB watermarking is that if the watermark size is very small then multiple watermarks can be added into the cover image so that if some of the watermarks are lost because of attacks then remaining watermarks can help in copyright protection of that content. This technique is less robust against various attacks, this is proved by applying various attacks like rotation, clipping, median filtering and mean filtering on watermarked image and then its performance is evaluated which shows that it does not work well against these attacks.
- Correlation Based technique: In this rather than embedding the watermark straight to the cover image, first watermark is transformed into some pseudo random noise sequence (PNS) and then a weight is multiplied into it and this weighted PNS is added into the cover image using following equation Eq. 4.

$$\begin{gathered} CW(i,j) = C(i,j) + k*W^{'}(i,j) \\ Where, CW(i,j) : Watermarked\ \ image\ at\ location\ i,j \end{gathered} \tag{4}$$

C (i, j): Cover image at i, j location.

k: Weight or Gain Factor.

Here, the value of k determines its robustness and imperceptibility, increasing the value of k increases the robustness but decreases its imperceptibility and vice versa.

- Additive Based technique: In additive method some pseudo random noise is added into the image on the basis of intensity of the pixel [52]. This noise is added to the original image using some key, which will be used at the time of its extraction to detect the watermark.
- Patchwork Technique: In this an image is divided into two patches X and Y where patch X is brightened by some factor alpha while patch Y is darkened by the same factor. Now watermark is embedded in these patched using some encoding technique and then extracted by using same factors.

ii. Transform/ Frequency domain watermarking: In this watermark is embedded in frequency transform of the host image which makes it more robust than spatial domain technique but these techniques are more complex than spatial domain. DCT, DWT, DFT are some of the transforms used to convert the image into frequency domain. Some frequency domain techniques used in watermarking are explained below.

- **Discrete Cosine Transformation (DCT):** DCT is used to convert an image from spatial domain to frequency domain by converting it into sum of cosine wave series at various frequencies. DCT can be done in various dimensions like 1D, 2D and 3D, in case of images 2D DCT is performed to convert it into cosine series. DCT transform can be applied on complete image or by dividing the image into various blocks of a particular size [85]. It converts an image into various bands and then watermark is embedded into these bands. The band selection is done on the basis of its information content so that robustness can be achieved against various noise attacks. If a high frequency coefficient is chosen for watermark embedding than a filter can remove it by filtering high frequency coefficients, so middle frequency components are chosen as embedding locations for the watermark which makes it more robust than spatial domain technique, selecting these embedding regions is one of the major concern of DCT technique. DCT is the most frequently applied linear orthogonal transformation in digital signal processing [126]. Many applications of DCT are like image processing, compression, watermarking and etc. [77]. 1D DCT and 2D DCT are represented using Eqs. 5 and 6. The results of applying DCT transform on Lena image is shown in Fig.6 and Fig. 6 (a) shows the Lena image taken as input and (b) shows results of 2D-DCT transform.

1D-DCT is shown as:

$$f(i) = F(u) \tag{5}$$

2D-DCT is given as [32]:

$$\mathrm{F(u,v)} = \alpha(u)\alpha(v)\sum_{i=0}^{M-1}\sum_{\mathrm{j}=0}^{\mathrm{M}-1} \mathrm{f(i,j)}\cos\left[\frac{(2\mathrm{i}+1)\mathrm{u}\pi}{2\mathrm{M}}\right]\cos\left[\frac{(2\mathrm{j}+1)\mathrm{v}\pi}{2\mathrm{M}}\right] \tag{6}$$

$$\textit{Where}, u, v = 0, 1, 2\ldots\ldots M-1, M \textit{ is size of sequence}$$
$$f(i,j)\textit{is image in spatial domain and } \mathrm{F(u,v)} \text{ is in frequency domain}$$
$$\alpha(u) = \begin{cases} \dfrac{1}{\sqrt{M}}, u = 0 \\ \sqrt{\dfrac{2}{M}}, u \neq 0 \end{cases}$$

Inverse DCT is given as,

$$\mathrm{f(i,j)} = \sum_{i=0}^{M-1}\sum_{\mathrm{j}=0}^{\mathrm{M}-1}\alpha(u)\alpha(v)\ F(u,v)\cos\left[\frac{(2\mathrm{i}+1)\mathrm{u}\pi}{2\mathrm{M}}\right]\cos\left[\frac{(2\mathrm{j}+1)\mathrm{v}\pi}{2\mathrm{M}}\right] \tag{7}$$

- **Discrete Fourier Transform (DFT):** Fourier transform means to convert an image into two transforms called magnitude and phase. DFT uses phase modulation instead of

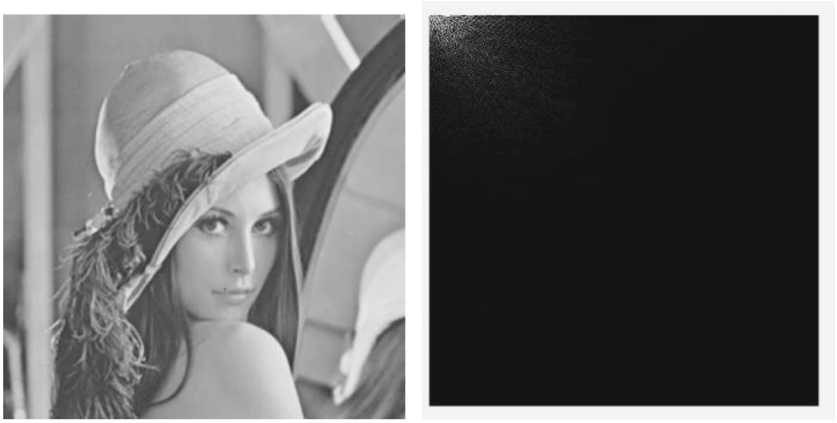


Fig. 6 **a** Original Lena image **b** 2D-DCT of Lena image

magnitude components to hide the message. DFT is used to covert an image into 4 sub bands HL,LH, HH and low frequency component LL [57]. To find DFT, calculations are performed by using Fast Fourier Transform (FFT). One property of DFT is transformation invariance [87] and there is an advantage of using DFT that it has less visual effect and is very robust against noise attacks on the message. DFT is represented by Eq. 8. The result of applying DFT on Lena image is shown in Fig.7 it shows the real and imaginary part of the DFT.

$$F(u,v) = \frac{1}{M*N}\sum_{i=o}^{M-1}\sum_{j=0}^{N-1} f(i,j)e^{-2\pi\left(\frac{ui}{M}+\frac{vj}{N}\right)j} \tag{8}$$

- **Discrete Wavelet Transform (DWT):** DWT is a fast and easy transformation approach which translates an image from spatial domain to frequency domain. DWT is a wavelet transform in which the wavelets are sampled in discrete manner [26]. DWT decompose an image into hierarchies by using mathematical tools [38]. This transform is based on wavelets rather than frequency, here the term wavelet means components with different scales. So it provides both details of an image that is frequency and spatial domain. It converts the signal into sequential order of its frequency in high to low order. High

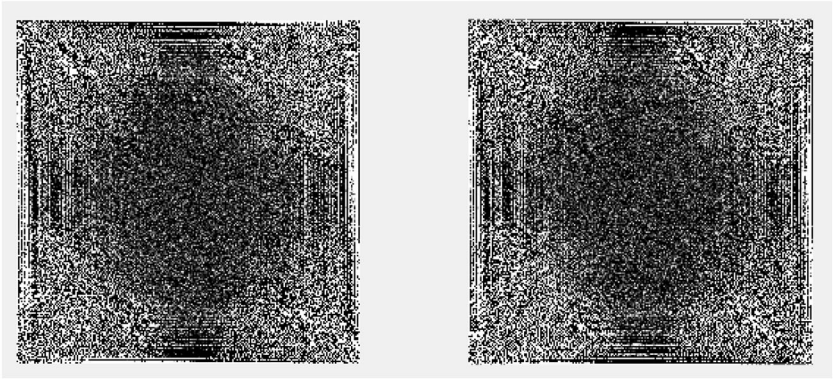


Fig. 7 Real and complex part of image after applying DFT

frequency components contain details of edges while the further decomposition is done for low frequency components. It converts the image into various sub bands called LL, LH, HL and HH, where LL represents low resolution, HL is for horizontal, LH is for vertical and HH is diagonal component of the image. There are various dimensions used for DWT like 1D, 2D, 3D these dimensions converts it into various levels of these sub bands. Here LL contains high components of the image, while HH has high frequency components. Most of the information of the image is contained in LL sub band.

DFT and DCT represent signal either in spatial domain or in frequency domain but DWT is able to represent signal in both spatial and frequency domain simultaneously. DWT is used in JPEG2000. The main concept of DFT is to segment an image into various blocks and then hide data into these blocks [23]. Most of the researchers have used DWT to convert the host image into various sub bands and then choose any band for the embedding. Mostly high frequency components are chosen for embedding to provide imperceptibility [63] but high frequency components are not robust against attacks as these are filtered out by various filters. One problem with DWT is that it has a problem of shift invariance which results into down sampling because of that many researchers have used RDWT(Redundant DWT), which removes the problem of shift invariance as well as it also increases the capacity of the watermarking. Figure 8(a) shows the results of applying 2D DWT on Lena image, in this 1st block shows LL sub band 2nd shows LH, 3rd shows HL and 4th shows HH sub band. Through this it can be seen that most of the information of image is stored in LL sub bands because of that most of the researchers have used LL sub band for watermarking. Figure 8(b) shows the plot of information content in every sub band.

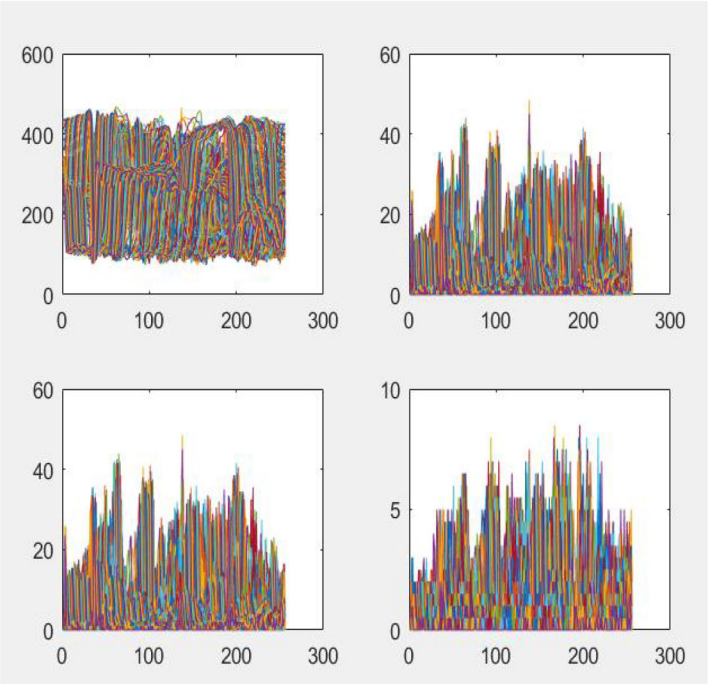
- Singular Value Decomposition (SVD): SVD is an efficient method to work on matrices and is used to process various types of images. While applying SVD on any image it converts it into 3 matrices [126]: A, U and A^T in which U matrix is called diagonal matrix while rest 2 are known as orthogonal matrices [77]. It is used in many fields like image compression, image processing and image watermarking. It is an effective tool which converts the metrics into singular values. SVD decomposition is shown by using Eq. 9, most of the researchers have used its diagonal component (U) for embedding as it has most of the information of the image but it suffers from the problem of false positive. False positive problem means any unauthorized user can use the watermarked image and can extract a watermark from it while there was no watermark added on it, by showing his own watermark he can prove his copyright on particular image because of this it is used in combination of DCT, DWT and DFT. One another solution to false positive problem is that rather than embedding watermark in U component, a principal component (A*S) can be used as watermark because principal component has a unique feature and can be used to remove false positive problem. The result of applying SVD on LL sub band achieved using DWT is shown in Fig. 9 here block 1st and block 3rd represents A and A^T information content while 2nd block represents information content in diagonal elements (U).

$$SVD(C) = A\ U\ A^T \tag{9}$$

1.4 Watermarking attacks

To identify the weaknesses and strength of watermarking techniques various attacks are performed on watermarked image. Some of the watermarking attacks are shown in Fig. 10

(a)



(b)

Fig. 8 **a** Result of applying 2D DWT on an image **b** Information content plot for every sub band

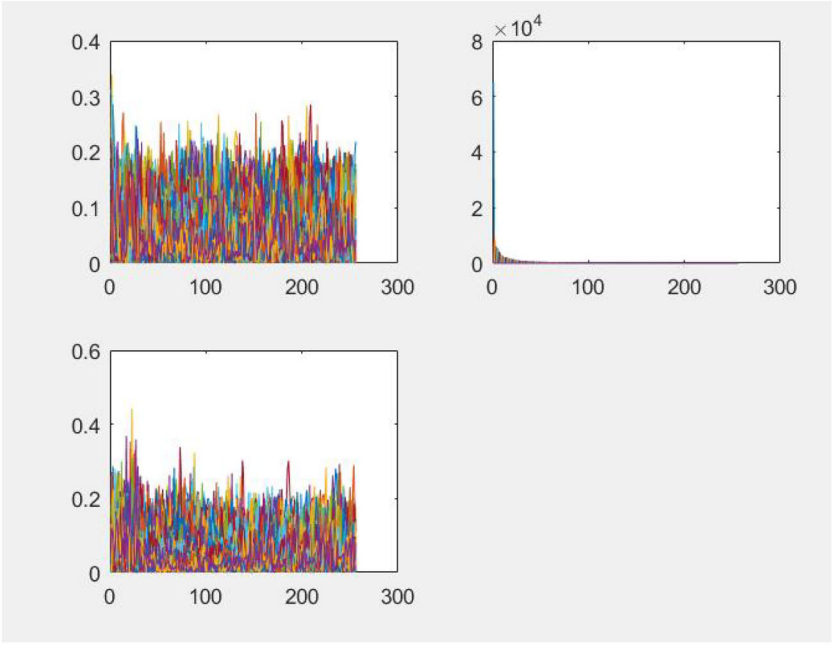


Fig. 9 Results of applying SVD on LL sub band of Lena image

and are described as follows [105]. Table 1 shows various types of attacks used by researchers and their abbreviations used.

A. **Image processing attacks:** It includes various attacks like filtering, JPEG compression and many more which are performed on images during its processing for filtering some frequencies to perform smoothening on the image.

- Attacks by filtering: In filtering first Fourier of image is calculated and then it is multiplied by the filter and after that inverse transform is calculated. A filter can be sharpening filter, smoothing filter, min filter, max filter, median filter or mean filter [22]. In median filter the median of neighboring pixels of the target pixel is calculated and then this value is assigned to the pixel at the center. Similarly in mean filter mean value of neighborhood pixels is calculated and then assigned to pixel under consideration [61]. To reduce the noise median filters are mostly used.
- Attack by JPEG-2000 compression: This technique is used for compressing an image so that image can be transferred easily over the network. This technique overcome the blocky effect problem of DCT based JPEG standard. JPEG-2000 can achieve high compression ratio and it removes blocky artifacts.

B. **Geometric attacks:** It includes image scaling, rotation and image clipping. Some of the geometric attacks are explained below

- Attacks by image scaling: Image scaling is when we scan an image and adjust its size for publishing like for example we reduce the length and width of an image into half and then up-sampled it to original size.

- Attacks by rotation: When we rotate watermarked image by some angle and some cropping is performed on it, this will not change the content of the image but makes watermark undetectable.
- Attacks by image clipping: In this an image is cropped from the watermarked image and to find the watermark from this image we will need the cover image as well to find the value of those portions which are not present in clipped image.

C. **Cryptographic attacks:** These attacks are used to hinder the security of the system by getting the key of embedding through some process. Once the key is found the attacker can rewrite the watermark or can add into cover image or attacker can try to guess the watermark from watermarked image.

D. **Protocol attack:** In this any unauthorized person first extract the watermark from watermarked image and then copy it to some other place in watermarked image by generating ambiguity in the protocol. Attacker does not destroy the watermark but use it for generating ambiguity, these types of attacks are also known as copy attack [109].

2 Performance measures

Performance measures or matrices are used to calculate the performance of any algorithm used for watermarking purpose. The performance can be in terms of its robustness against attacks, quality of the watermarked image called imperceptibility, capacity to handle the watermark, time taken by the algorithm to perform embedding and extraction and many other. Researchers have used a number of performance measures to prove the quality of their technique according to their needs. Some of the performance measures are explained here which are used in watermarking fields.

A. **Mean Square Error (MSE):** MSE is the average of the squared error and is used to find the error between original and watermarked image. Lower value of MSE depicts more similarity between host and embedded image while higher value of it shows dissimilarity between images. MSE is used to find the PSNR value of the watermarking scheme as is given by Eq. 10 for grayscale image and by Eq. 11 for color images

$$\mathrm{MSE} = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{\mathrm{N}}[\mathrm{C}(\mathrm{x},\mathrm{y})-\mathrm{WC}(\mathrm{x},\mathrm{y})]^2 \tag{10}$$

$$MSE(color) = \frac{\sum_{z=1}^{3}\sum_{x=1}^{\mathrm{M}}\sum_{y=1}^{\mathrm{N}}[\mathrm{C}(\mathrm{x},\mathrm{y})-\mathrm{WC}(\mathrm{x},\mathrm{y})]^2}{3*\mathrm{M}*\mathrm{N}} \tag{11}$$

Here, C(x,y): Host image at pixel x, y.
WC(x,y): Watermarked image at pixel x, y.
Z denotes number of planes in image.
M, N: Size of the host image

B. **Peak Signal to Noise Ratio (PSNR):** PSNR is one of the most common measure used to find the quality of the watermark image. It is ratio of the Peak value of the signal to the

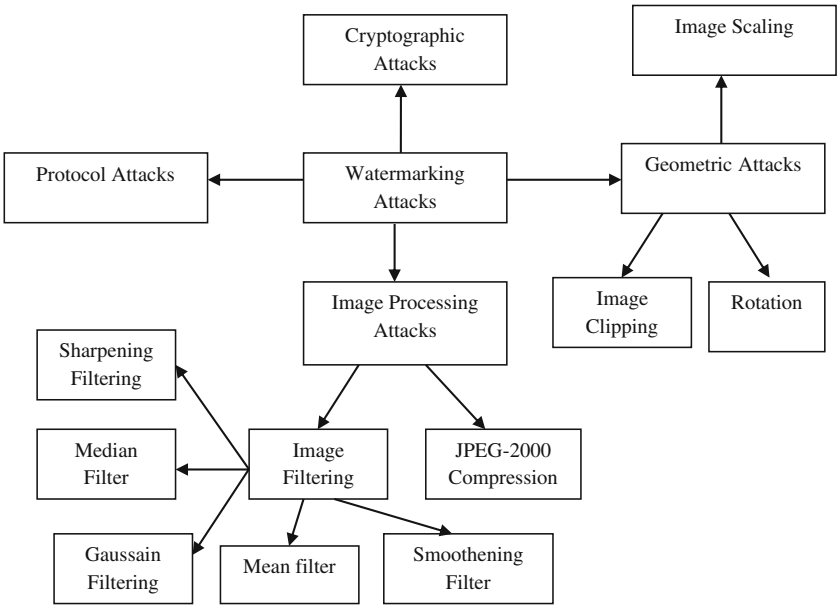


Fig. 10 Various watermarking attacks

power of noise. In watermarking field it is ratio of the original image and the watermarked image and is used to find the similarity between these two images. PSNR is used to measure the imperceptibility characteristics of any technique used for watermarking; it describes strength and weakness of the scheme. PSNR for gray scale image is given by Eq. 12 and for a color image it is same as for grayscale except the definition of MSE changes. Higher the value of PSNR the better will be its quality and imperceptibility. A PSNR value greater than 27 dB is acceptable [107].

$$PSNR = 10*log\frac{255^2}{MSE} \tag{12}$$

C. **Normalized Correlation (NC):** NC is measure of similarity and used to find the correlation between two vectors or images. In watermarking NC is used to find the correlation between original and the extracted watermark image. The value of NC lies

Table 1 Various attacks and abbreviations used

Abbr.	Attack	Abbr.	Attack	Abbr.	Attacks
S&P	Salt and Pepper	MF	Mean Filter	MPA	Mosaic Piece Attack
Rot	Rotation	Cr	Cropping	Dis	Distortion
LPF	Low Pass Filter	WF	Weiner Filter	BF	Butterworth Filter
GF	Gaussian Filter	SN	Speckle Noise	WC	Wavelet Compression
GN	Gaussian Noise	AF	Average Filter	GC	Gamma Correction
RS	Resize	SH	Sharpening	PN	Poisson Noise
JPEG	JPEG Compression	Sc	Scaling	HE	Histogram equalization
MDF	Median Filter	GA	Geometric Attack	CA	Contrast adjustment

between [0,1], a smaller value of NC shows the dissimilarity between two images while value closer to 1 indicates more relation between these two. NC is used to measure the robustness of the scheme after performing various types of attacks on the watermarked image. If the attack has no impact on the extracted watermark than a value near to 1 or 1 is achieved by NC and that scheme is called robust. Generally NC > 0.75 is acceptable for extraction scheme [88] and is calculated using Eq. 13

$$NC\left(W, W^{'}\right) = \frac{\sum_{x=0}^{M}\sum_{y=0}^{N}\left[W(x,y)W^{'}(x,y)\right]}{\sqrt{\sum_{x=0}^{M}\sum_{y=0}^{N}W(x,y)}\sqrt{\sum_{x=0}^{M}\sum_{y=0}^{N}W^{'}(x,y)}} \tag{13}$$

D. **Bit error ratio (BER):** The Bit Error Ratio (BER) defines the error rate occurs in the transmission system. In watermarking BER is the error rate between the original and extracted watermark image. The value of BER ranges between [0 100] for grey scale image represented using 8 bits and is represented by Eq. 14. Where number of errors is calculated by finding the bit difference between actual watermark and the extracted watermark.

$$BER\left(W, W^{'}\right) = \frac{Number\ of\ errors}{Total\ number\ of\ bits} \tag{14}$$

E. **Structural Similarity Index measures (SSIM):** It is used to measure the structural similarity between the original cover image C and the Embedded image WC. SSIM value near to 1 represents more similarity between these two images and shows that structure of the both the images are same. SSIM helps to prove imperceptibility characteristics of the watermarking scheme. It is calculated by using Eq. (15a) and for color images it is calculated by using Eq. (15b)

$$SSIM(C, WC) = \frac{\sum_{x=0}^{M}\sum_{y=0}^{N}C(x,y)WC(x,y)}{\sum_{x=0}^{M}\sum_{y=0}^{N}[C(x,y)]^2} \tag{15a}$$

$$SSIM(C, WC) = ld(CRGB, WCRGB)cd\left((CRGB, WCRGB)\ IC(CRGB, WCRGB)\right. \tag{15b}$$

Where, ld: luminance distortion between RGB component of original and watermarked image.
cd: contrast distortion between RGB component of original and watermarked image.
ic: loss of correlation between RGB component of original and watermarked image.

3 Study of various watermarking techniques

3.1 Spatial domain based watermarking techniques

An LSB based watermarking scheme is presented in [108], in this firstly watermark image is converted into double and then to 8 bit blocks now this watermark is embedded in LSB of the cover image bit by bit. This scheme gives a very good PSNR value but not good MSE and BER values because it is very easy to perform any attacks on it and any attacker can easily change the watermark algorithm. This spatial based technique provides very good

imperceptibility to the watermark image but is not robust against various image processing attacks.

An imperceptible watermarking technique based on pixel selection using shell is implemented in [73], in this first watermark is converted into binary image and then to a matrix then using shell based scheme pixel positions from the host image are selected for embedded the watermark. The reason of using shell scheme is that it gives sensitivity in data and provides temper detection. This scheme is evaluated against various attacks and its performance is measured using PSNR, NC and BER values.

An improved LSB based technique is implemented in [14] to provide better quality to the watermarked image. In this scheme watermarking is performed in 3rd and 4th LSB bits to provide the security because any unauthorized user will expect that watermark is embedded in 1st LSB bit. This scheme provides good imperceptibility results but does not work for the robustness. The scheme is evaluated against various existing works and shows good PSNR value.

A spatial domain technique is proposed in [4] to provide both characteristics robustness and imperceptibility by spreading the watermarking information to regions of pixels in the cover image. This watermarking scheme is implemented on color cover images and tested against various attacks to prove its robustness. Here watermarks are embedded in all regions of the image selected by using the SIRD technique and two embedding masks. In this scheme a new metric called Global Embedding Impact (GEI) is also used to measure its performance in terms of net variance a host image C(x, y) of size M*N will have in embedding process. It is given in Eq. 16.

$$\mathrm{GEI} = \frac{\sum_{z=1}^{3}\sum_{x=1}^{M}\sum_{y=1}^{N}(\mathrm{W}(x,y)-\mathrm{C}(x,y))}{3*M*N} \tag{16}$$

A watermarking method based on segmentation and region based chaotic watermark is proposed in [83]. Here firstly segmentation is performed in spatial domain to get information about image and then it is divided into regions, these regions are arranged according to some properties like their size and then watermark embedding is done on largest size region. Performance of this scheme is evaluated using FAR (False Acceptance Rate), NC and FRR (False Rejection Rate).

A blind watermarking scheme for color images is described in [113] which use blue components of RGB color space for embedding and rather than embedding complete watermark, four watermarks are embedded to host image four times in DC coefficients of the image to provide copyright protection. Here watermark is divided into 4 sub images and blue component of original image into 16 sub images and now watermark is embedded in these 16 blocks 4 times using a key which will be used at extraction side to make the scheme blind. Here MD5 algorithm is also used to permute the watermarks for embedding so that attacker cannot get the watermark until he will have the key to decrypt it. This scheme is blind so at the time of extraction, cover image is not required, which makes it a secure scheme.

Spatial domain watermarking for buyer authentication is proposed in [78]. A watermarking scheme to handle geometric attacks and for generating watermark dependent on images is presented in [90]. Watermark robustness against geometric attacks is also proposed in [2009 localized] by dividing images into 2 regions even and odd and then odd even quantization is performed to embed the watermark. This technique is tested against geometric attacks along with signal processing attacks. Again block based region selection is used in [59] to provide better quality of the watermarked image.

3.2 DCT based techniques

Digital watermarking using the concept of DCT and decision tree is used in [86]. Rather than embedding watermark at any place some blocks are selected using mining techniques for embedding. This proposed scheme is tested against various attacks and shows best results against JPEG compression and noise attacks. In this algorithm firstly blocks for embedding are selected by decision tree induction and then DCT is performed on these selected blocks. In this scheme watermarking is performed on color images and PSNR is used to measure the performance.

In [92] a non blind scheme using DCT is proposed along with Arnold transform and cross chaotic map. Firstly Arnold map is applied to encrypt the watermark image and then cross chaotic map is applied to provide more security to the watermarked image after this DCT is applied on cover image to convert it from spatial domain to frequency domain and then embedding is performed. Here PSNR and NC values are used for measuring the performance. Arnold map scramble the watermark image using some key so that if any attacker extracts the watermark, he cannot get any information from it because it is a scrambled one and cannot get the original until he knows the key used.

Along with DCT, SPIHT (listless set partitioning in hierarchical trees) technique is used in [102] to compress the image and provides more robustness. For security purpose Chinese remainder theorem is used which encrypts the watermark. Along with CRT, Arnold transform is also used to provide more security. This scheme is evaluated using PSNR, Temper Assessment Function (TAF), SSIM and NC values, it outperforms all the compared algorithms.

DCT along with Genetic algorithm is used in [96] [115]. Here in [96] genetic algorithm is used to select the DCT coefficients for embedding. DCT coefficients which have large frequency difference are chosen for embedding to guarantee better robustness as choosing higher frequency component will decrease its robustness. Genetic algorithm helps to find best locations to embed watermark by calculating a fitness value which gives better results in terms of robustness and imperceptibility. Fitness function is chosen in such a way that it provides the balance between these two characteristics.

Watermarking scheme for color images using combinations of DCT and DWT is proposed in [3]. Here Arnold transform along with DCT is performed on gray scale watermark image and DWT is applied on color cover image to convert it into sub bands. Firstly watermark is scrambled using Arnold transform and then DCT is applied to convert it into equal size blocks now these blocks are embedded in DWT sub bands of color cover image, which was applied on DCT components of the cover image. This scheme shows more robustness against linear and non linear attacks. In [37] authors have also proposed an algorithm using combination of DCT and DWT to improve its results.

In [35] DCT along with Quaternion wavelet Transform (QWT) are used to provide copyright protection. Here color cover image is converted in YIQ components and then QWT is applied on Y component to convert it into 4 sub bands then DCT is performed on these components and watermark is scrambled using Arnold transform and sine chaotic system before embedding it into DCT components. Along with common attacks, rotational attacks are also performed on the algorithm to prove its robustness against these attacks.

A blind scheme based on DCT and 2D linear discriminate analysis (2D LDA) has been implemented for color images by authors in [15]. Here color images are converted into YIQ space and then Q component is used for embedding by converting it into frequency domain

using DCT and two watermarks logo and reference are embedded in AC coefficient of DCT to provide digital archives and copy rights protection.

A DCT based scheme for forensic applications is used in [28]. The embedding is performed by finding the relation between DCT coefficient using Gabor filter and then according to this embedding is done. The scheme is tested against various attacks and proves its robustness and imperceptibility. Researchers in [53] have used Hamming code along with DCT for embedding in color images and for security watermark is encrypted using two encryption schemes Arnold and chaos. Here error correction code (ECC) is implemented to prove the robustness of the scheme and handling the errors. The color image is converted into YCbCr model and then embedding is done in HL1 sub band.

An embedding scheme is based on DCT and ZIP compression is implemented in [89] for X-ray images. Here embedding is performed in middle frequency components of DCT scheme and Zip compression is done for providing security. Rather than embedding watermark directly in DCT coefficient a pseudo random sequence is used to embed it and for its extraction. For compressing the images Huffman coding scheme is used because this scheme is easy to implement and is lossless.

A new scheme using differential evolution DCT and Kernel Extreme ML (KEML) has been proposed in [123]. Here block selection for embedding is done using KELM regression technique and optimized scaling factor is calculated using Differential Evolution (DE). This scheme is evaluated against [6] which is based on genetic algorithm based back propagation neural network and shows better results.

Multidimensional PSO along with DCT is applied in [56] to optimize the result in terms of robustness and imperceptibility. In [43] a blind watermarking technique using block based DCT is implemented. Here watermarking is done by finding the difference between DCT coefficients and then these coefficients are modified by water mark bits. Watermarking scheme for medical applications is implemented in [109] using DCT, error correction code along with Lifting Wavelet Transform (LWT). The reason for using LWT rather than DWT is that LWT requires less memory space than DWT and is faster than it.

From this study it can be concluded that DCT based applications are very imperceptible and robust but these requires huge calculations and takes more time which leads to difficulty in its implementation. These shows good robustness against various image processing attacks but are not good for scaling, rotation and cropping attacks. So many researchers are working in this field to make DCT based application robust against these attacks also.

3.3 DWT based techniques

A watermarking scheme for grayscale images based on DWT and Arnold transform is used in [67]. Here DWT is applied on cover image which converts it into 4 sub bands, in these sub bands HL sub band is used for embedding. Then Arnold is used for pre treating the watermark and gives a randomized image so that attacker will not be able to get the original watermark image. This scheme is non blind as it requires the host image at the time of the watermark extraction.

A watermarking scheme for copyright protection and data ownership is presented in [72], which uses HIS color space wavelet transform technique. Firstly image is converted into HIS color space and then DWT is performed to convert it into sub bands from which LL sub band is used for encryption. For embedding the watermark, the watermark is converted into 8*8 blocks and then scaled by a factor alpha, this value is then embedded into LL sub band of host

image. Similarly extraction of watermark is performed in opposite manner. The performance of the scheme is measured using PSNR and MSE parameters and evaluated against various existing works.

A different watermarking scheme based on 2D-DWT and encryption algorithm is proposed in [9] for copyright protection and content authentication of the digital content. Instead of embedding watermark directly an encryption algorithm is applied on it, which rotates the watermark by some secret key K so that if an attacker becomes successful in extracting the watermark, he will not be able to decrypt it without knowing this key value K. Both cover image and encrypted watermark goes under 2D-DWT to get relevant scaled image, now watermark image is embedded in the locations identified by using euclidian distance.

Another paper based on Haar Wavelet transform for color images is presented in [124]. This scheme has good robustness against compression and noise attacks. A color watermark in a color host image is embedded din this scheme using YIQ color space and then 1 scale 2D DWT is performed on watermark image and M scale 2D DWT on the cover image after this embedding is done.

A watermarking scheme using DWT and discrete time chaotic transmission is proposed in [36] to provide robustness and security to the watermark image. A modified Henon map encrypts the watermark image and then inserted into discrete time chaotic system. This encrypted watermark image is now embedded into DWT domain of the host image to provide security to the watermark. During extraction firstly DWT is performed on watermarked image and then it undergoes through same procedures used for encryption to decrypt it. The feasibility and robustness of the scheme is also evaluated and shows good results.

A 3 level DWT watermarking scheme for copyright protection in proposed in [58]. The low frequency sub bands are chosen for embedding the watermark as high frequency components can be filtered out easily during attacks. The proposed scheme is compared by 1-level and 2-level DWT schemes by PSNR and MSE performance matrices and it outperforms these two. Both watermark and host image undergoes through 3-level 2D DWT using daubecheis wavelet transform and then alpha bleending technique is used to embed watermark in host image after this 2 level 3D inverse DWT is performed to get the watermarked image. For extraction the original host image is also required which makes this scheme non blind.

Authors in [118] presented a watermarking scheme that embeds watermark in color channel of the host image by coefficient quantization method. A novel scheme for color channel selection is also used that selects HL4 and LH4 channels for embedding. This scheme provides the robustness and imperceptibility balance as well as gives strength to the watermark image. A key is used to encrypt the watermark before embedding and this key is generated at decryption side by Otsu's algorithm, so no key is shared in the communication channel for security purpose.

A blind watermarking scheme using redundant DWT (R-DWT) is presented in [121] that use Human Visual System (HVS) characteristics for embedding the watermark. The watermark is embedded in singular values of RDWT sub components of the cover image using some embedding factor, which is optimized using self adaptive differential evolution algorithm. As using SVD creates a problem of false positive, so here to remove this problem digital signature of the owner is also embedded. RDWT has more capacity handling feature than DWT which attracts authors to use RDWT instead of DWT.

An another scheme using RDWT is proposed in [19] that uses the concept of Principal Component Analysis as well as improved Grey Wolf Optimization algorithm to improve the performance in terms of robustness. The performance of the scheme is evaluated using NCC,

PSNR, MSE and SSIM and it is compared with various existing works. Result shows that the proposed work provides more robustness than the compared ones.

A hybrid watermarking scheme is proposed by [99] which is a combination of blind and non blind scheme. The watermark image is embedded in sub bands of the cover image converted by DWT using blind embedding scheme then this inner embedded image is again embedded into an outer cover image by suing SVD and DWT based on non blind scheme to get outer watermarked image. This complete combination is called hybrid watermarking scheme and shows good performance.

3.4 DFT based techniques

A DFT based technique is proposed in paper [91] to prove the image quality by embedding the watermark in magnitude of fourier transform of cover image. The scheme is evaluated on a dataset of 1000 images to shows its quality improvement and robustness against attacks. Firstly color image is converted into YCbCr space then low frequency components of luminance (Y) are moved to the center, this helps to find watermark frequencies to be embedded by controlling implementation radius. The scheme is compared with existing techniques and shows better results in terms of robustness.

A color image scheme is shown in [120] which use multidimensional fourier transform for watermarking. It proposes two vector watermarking techniques, in first technique color watermarks (Yellow and blue) are embedded in chromatic channels of cover image using Spatio Chromatic DFT technique (SDFT), in second method Quaternion FT (QFT) is used for embedding color cover image and watermark. These two algorithms are compared with other DCT based techniques and shows better performance. SDFT takes advantage of chromatic information of image which improves the imperceptibility but it ignores the Y component, because of that QDFT based technique is also proposed in it which improves robustness of the watermark image.

A 4D QDFT watermarking algorithm to improve the capacity, imperceptibility and robustness of the watermark is stated in [16]. It utilizes the benefits of 4D QDFT by maintain relationships between RGB color channels as well as QDFT components, which improves its performance against other QDFT based color schemes. It decreases the energy loss of watermark bits during embedding and improves the fidelity and robustness by using 4D QDFT.

A blind scheme for color images is proposed in [125] based on Fourier transform. There are two variations of this scheme. Firstly color image is converted into RGB channels and then different transforms are applied on these channels. Here different transform are like DFT, DWT, FFT and QDFT after this watermark is embedded into selected real parts of these coefficients then imaginary parts of the coefficients are combined with these parts and inverse transformations are applied again to get watermarked image.

Another blind color watermarking scheme using QDFT has been proposed in [39]. It has uses a number of schemes like Extreme pixel adjustment, mixed modulation, multi bit partly signed altered mean modulation (MPSAM) along with QDFT to provide blind watermarking technique. The results are optimized using swarm intelligence technique called PSO for better robustness. The combination of these techniques is called EMMQ here. MPSAM maps multiple bits within a single block while MM is used to embed the watermark so that better image quality and robustness can be achieved. This scheme is compared with other existing works and shows better results for a particular payload. The reason of using EMMQ based

technique with QDFT is that QDFT based techniques do not work good against JPEG compression and contrast enhancement attacks while using EMMQ provides good results of robustness against these attacks also.

A dual tree based complex wavelet transform technique is proposed in [13] to achieve the shift invariance and directionality features which are not provided by just using DWT or DFT. A color image is converted into YUV space and then watermarking is done in luminance levels as these provides more imperceptibility because of less perceptibility to HVS (Human Visual System). Low pass filters are also used to generate a perceptual masks which is used in both embedding and extraction process to provide better imperceptibility. DTCWT is a modified technique explained by [100] which remove shift invariance limitation of DWT, it is also less redundant to DWT. The luminance components (U and V) goes through 3 level DT-CWT transform after this low pass filter is used to create a mask for each channel. Then inverse DT-CWT is performed and other channels are merged to get watermarked image.

Another paper [71] has proposed watermarking algorithm using fractional fourier transform to provide authenticity of the digital data. To increase robustness of the scheme Butterworth filter has been applied on the host image which filters out the low frequency components of it and then FFT is applied on it to transform the cover image for embedding. Here watermark is not embedded directly for this a pixel position shuffling algorithm has been used which shuffles the watermark to provide security to it. The performance of this scheme is evaluated against various attacks and reasonable results are found for robustness.

A hybrid watermarking approach has been reported by [34] which uses a combination of DFT and DCT based techniques for security Arnold transform is also used. To improve the imperceptibility DFT coefficients are used while for robustness DCT is applied to these DFT coefficients. The medium frequency components of DCT are used for embedding. Watermark is embedded by using a key which is used at the time of extraction also; here a scrambled watermark is embedded in the host image to provide security. The experiments are performed on natural images and various attacks are also applied to show robustness. First host image is converted into magnitude and phase transformations using 2D DFT. Second 2D DCT is applied on magnitude coefficients where encrypted watermark is embedded using a key and a sequence. Third inverse 2D DCT is applied to get magnitude components, which is combined with phase components to reconstruct the image. At last 2D IDFT is applied to get watermarked image. Extraction process is reverse of the embedding process.

Authors in [98] provided a watermarking technique based on DMeyer DWT to increase the capacity characteristics of watermarking. Here equal sized host and watermark images are used to improve the capacity characteristics. Firstly DMeyer DWT is applied on host image to find coefficients having maximum information. Second DFT is used to find components which have sufficient information and third SVD is applied to get orthogonal matrix of transformed image. To measure the imperceptibility PSNR and SSIM measurements are used and robustness is measured against various image processing and noise attacks. The reason of using DMeyer DWT is that it ignores the staircase effects coming after watermark embedding in edges of the host image.

Again a hybrid technique is reported in [5] which uses a combination of DFT, DWT and SVD techniques for color images. First image is converted into YCbCr space to increase the correlation between host and watermarked image while DWT is used to find vertical and horizontal details, for removing its shift invariance problem DFT is used at last SVD is used for embedding. The scheme is tested against various attacks and shows robustness and good PSNR value. Here HL, LH components of DWT are used for embedding and embedding is done is diagonal matrix of SVD.

3.5 Combined approach of watermarking

A watermarking technique using the concept of lifting wavelet transform (LWT) and QR decomposition is presented in [74], which also uses Lagrangian support vector regression (LSVR) to provide robustness against attacks, in this low frequency bands are used for watermarking. In [41] authors have presented LWT and DCT based robust watermarking approach which can be used in medical applications. In [119] authors have used vector quantization approach for providing image integrity verification and authentication. They have calculated PSNR and normalized hamming similarity (NHS) to calculate its robustness. In [116] a robust watermarking technique using the concepts of multiple decompositions is proposed and is implemented on color images. Along with this Arnold transform is also used here which provides security to the watermark image. The given cover image is subjected to various types of transform like slantlet, contourlet discrete cosine transform and then the encrypted watermark is embedded in these transforms. In [94] DWT and SVD based digital image watermarking scheme is proposed which uses multi scale factor for embedding the watermark. The host image undergoes through 3-Level DWT to get the sub bands and then SVD is applied on these sub bands then embedding is done in singular values.

A combined approach of watermarking to provide a blind scheme for medical applications using a combination of DWT, SVD and Region of Interest approach is given in [117]. First DWT is applied on Region of interest of host image, which converts the image into 4 sub bands then LL frequency sub band is chosen for further processing. Second SVD is applied on LL coefficients to get singular matrices. Left singular matrix gives information about similar values which is used to embed the watermark using a threshold value. For authentication and identification of content 2 watermarks are embedded in this scheme, one is a logo and another one is electronic patient record which is a text data. To provide security to the watermark a blind scheme is proposed here and for host images various X Rays, mammography and CT scans images of patients are used. Hamming code is also applied on the text watermark so that Bit Error Rate can be reduced and recovery of watermark can be done efficiently.

Another approach to provide security is proposed in [111]. It is dual watermarking scheme in first LL sub band is chosen for watermarking and in second HH sub band. In this Scheme 2D DWT is applied on host image, it converts the image into 4 sub bands then LL and HH sub bands are converted into RGB color space. Now on these SVD is applied to get its singular values and watermark is embedded on these singular values. In this Scheme 2 watermarks, a logo and QR code are used for embedding. This is a non blind scheme as extraction of watermark requires the original cover image.

A blind watermarking technique which works against geometric attack is proposed in [66]. First n-level DWT is applied on host image; second SVD is applied on low frequency components of DWT. Now embedding is done on high value components of SVD. Zernike moments scheme is used to estimate the geometric attack parameters of the watermarked image. It is an improved scheme to estimate these components so that better robustness can be achieved against geometric attacks. To provide security, watermark image is encrypted using Arnold map before embedding. The scheme shows good robustness against various image processing attacks along with geometric attacks.

Multimedia security and copyright protections are main concern of [49] for these objectives DWT and SVD in lower upper decomposition are used. Here firstly DWT is applied on cover image which converts it into 4 sub bands then LU decomposition is applied on LL sub band which factorize it into L, D and U components then SVD is applied on D components.

Similarly SVD is applied on the watermark image, now singular values of the watermark image are embedded using a factor into singular values of the host. Then inverse DWT is applied to get the watermarked image. This scheme is evaluated against various attacks and shows good robustness against filtering and because watermark is not embedded directly so it also provides the security feature. Here reason of using LU decomposition is that it provides more robustness while combining with the DWT-SVD scheme.

Authors in [40] have explored a new combination of techniques called DCT, DWT and SVD to provide a multiple watermarking scheme. Here firstly 1-D DWT is applied on host image and then SVD is applied on LL sub band to get singular values now again 1-D DWT is applied on left and right singular values of SVD. For security Arnold transform is applied on the watermark and then progressive QIM scheme is used to quantize the host and watermark blocks after this inverse SVD and DWT are applied to get the watermarked image. In extraction cover image is not required so it is a blind scheme. Results show that the scheme gives excellent robustness against JPEG and JPEG-2000 compression.

Authors in [33] presented a semi blind scheme using cryptographic technique and DWT-SVD combination. In this a fast encryption scheme called Elliptive Curve Cryptography (ECC) is used to embed the watermark. The main use of ECC is that it encrypts the message with less number of bits in comparison to other encryption techniques. First host image is goes through entropy based HVS system in spatial domain, then DWT is applied on most appropriate blocks selected from HVS, last SVD is applied on DWT components. Authors have compared their work with other DWT-SVD based algorithms which do not have used encryption techniques and concluded that there results are better than these. This scheme is also implemented using HVS system implemented in DCT domain and shows good results with this also.

A multi optimized watermarking scheme is presented in [31], which uses DWT-SVD combination with entropy scheme. Here to provide security along with robustness and imperceptibility positions of the pixels are shuffled and then embedding is performed. Robustness of the scheme is shown after performing various attacks like rotation and JPEG compression. First DWT is applied on host image and then again DWT is applied but now on LL1 sub band only, these sub bands are rearranged according to increasing order of their entropy value. SVD is applied on LL2 sub bands and then embedding is done on these singular values. For security purpose watermark bits are shuffled using a predefined key which is used at extraction time also.

Authors in [60] have also used DWT-SVD combination for watermarking. A new technique has been used in [29] to provide improvements in robustness against geometric attacks. It uses the combination of DCT DWT and SVD for this purpose. First DWT is applied on host image then watermark is embedded in LH and HL sub band of it using hybrid technique. After performing DCT on these data replication and hamming code based error correction techniques are used to decrease the errors and to provide strong security against various attacks along with geometric attack.

Least square curve fitting along with chaotic map are used with DCT-DWT-SVD combination in [55]. DWT is applied on cover image, then LL sub band is divided into blocks after performing DCT on these and middle frequency components are taken out and SVD is performed on these selected blocks now watermark is embedded in singular values of it using an embedding strength factor. Embedding strength factor is calculated using least square curve fitting method and for security logistic map is used. Here watermarking is done in middle frequency components to provide the robustness.

In [30] authors have presented a watermarking scheme using the combination of Discrete Stationary Wavelet Transform (DSWT) along with DCT to optimize the results so that a balance between imperceptibility and robustness can be achieved. Now for security purpose SVD along with Arnold are also used. The proposed scheme has achieved a good PSNR value but the NC value is not up to the mark.

3.6 Optimized image watermarking techniques

Authors have worked a lot to optimize the results of digital watermarking. Watermarking should be done in a way that quality of the original image should not be decreased and it should resist against various types of attacks. To achieve these goals optimization is used so that improvement in robustness, imperceptibility, security and time taken by the algorithm can be achieved. The main motive of the optimization is to find a balance between various characteristics of watermarking as using only spatial or frequency domain techniques are not sufficient. Optimization cab be performed by using various algorithms like nature inspired algorithms, artificial intelligence based techniques, fuzzy logic and other algorithms. Nature inspired algorithms are inspired by the natural life of various birds or animals that how they are able to find their food and its source in an optimized manner. Many researchers have used various types of algorithms like Ant colony, Genetic algorithm (GA), Grey wolf optimization (GFO), Particle swarm optimization (PSO), Binary bat, Artificial bee colony (ABC), and Firefly optimization to get optimized results. Along with these various fuzzy logic inspired algorithms, machine learning techniques, Extreme machine learning (ELM) and deep learning techniques are also used to achieve these goals. The review of some of the techniques is shown here.

Authors in [45] stated an improved watermarking technique in terms of robustness, imperceptibility and capacity. Watermarking is done in LL sub band of the Integral Wavelet Transform (IWT) and embedding strength is optimized using ABC algorithm. A signature insertion algorithm is also implemented in this paper to provide authenticity and security to the watermark image. For signature generation firstly watermark image is converted into 2 matrices then from 2D array to a 1-D array. SHA-1 based hash function is applied on these 2 matrices to generate their hash function for signature, and then these two are XORed, the result is again XORed with first original hash matrix to get its 48 bit result as a signature. This generated signature is embedded in LL3 sub band of the host image in a most robust area so that signature can be retrieved after attacks to verify its authenticity. Here all the bands generated by IWT are used for embedding and then SVD is applied on these bands for imperceptibility and security purpose. The embedding is performed using an optimized embedding factor, provided by using ABC optimizer.

An adaptive watermarking technique for color watermark and color host image of equal size is proposed in [103]. RDWT is applied on the YCbCr color space of the host image to provide 4 sub bands on which SVD is applied, meanwhile watermark is also scrambled using Arnold chaotic map. The scrambled watermark is embedded in singular values of the host image using an optimized and adaptive embedding factor generated by ABC algorithm. To remove the problem of false positive, various security measures are also considered here and tested against rotation attacks suing SSIM, NC and PSNR measures.

Cuckoo search algorithm has been used in [8] for optimizing the embedding factor along with 2D DWT watermarking scheme. According to authors this work is the first experiment of cuckoo search algorithm in watermarking. First image is converted into 2D sub band then low

and high frequency sub bands that are LL and HH are selected for embedding the watermark image using optimized embedding factor generated by cuckoo search algorithm and then these blocks are coupled with remaining bands and inverse DWT is performed to get the watermarked image.

Authors in [47] have implemented watermarking technique using 2 bio inspired optimization algorithm Genetic and Cuckoo search. In first implementation a combination of SVD and GA has been used for embedding to provide maximum robustness and maintaining quality of the host image. For performance measurements correlation factor is used here. In second implementation a combination of RDWT, SVD and cuckoo search algorithm has been implemented. For optimization function NC value is used here, which helps the cuckoo search algorithm to find best optimum embedding factor. A number of attacks are performed on both the techniques and results show that a good PSNR, NC values are achieved here. A comparison between RDWT and RDWT-Cuckoo search is done to show the optimized results achieved through cuckoo search.

A swarm intelligence based optimization is used by combining the DWT-SVD based watermarking technique in [122]. A 2 level DWT is applied on host and then on middle frequency sub bands SVD is applied. For security purpose watermark is divided into 2 images padded with 0's to make both the divisions equal to size of original watermark and then these divided watermarks are embedded in singular values of both sub bands using optimized scaling factor generated by PSO algorithm after this inverse DWT is applied to get watermarked image.

A Guided Dynamic PSO (GDPSO) based watermarking technique is implemented in [70] for industry applications. The reason of using GDPSO instead of PSO is that PSO sometimes has a problem of premature convergence of swarm particles at a particular point while GDPSO does not have this problem as it distributed the information of fitness to other particles so that best global value can be achieved. The performance of GDPSO has been compared here with PSO to prove that it is better. The authors have used DWT-SVD based technique used in [110] for watermarking. Here singular values of watermark are embedded in host image to provide security. The strength factor is optimized using GDPSO to get better trade-off between imperceptibility and robustness.

In [2] authors have presented their work for Optimizing Robustness and imperceptibility. In this each watermark bits are embedded individually and results are optimized. A fitness function is proposed to best suit the optimization problem. The Bees algorithm is chosen as the optimization method and the proposed fitness function is applied to get optimized results. But this scheme does not work well against some of the attacks like salt and Pepper and Sharpening attacks.

Continuous Ant-Colony based optimization (CACO) is used in [50] for ECG steganography to provide security to the patient's information. Rather than using a single embedding strength, multiple embedding strength factors are used so that a balance between various characteristics can be achieved. For watermarking DWT and SVD techniques are used on MIH-BIH dataset.. CACO is used here to find out multiple embedding factor value for ECG steganography by embedding patient's information into it. Embedding is performed in HH sub band of ECG image after performing SVD on it. Here additive quantization method is used to embed singular values of watermark are embedded into host and then inverse operations are performed to get watermarked image. CACO continuously search for best solution given by particles using a fitness function based on correlation between watermark and extracted watermark as well as between host and embedded image so that a balance between robustness

and imperceptibility can be achieved. The results are also compared with performing same algorithm using single embedding factor.

A block selection based technique is proposed in [76] which uses distinct direct firefly algorithm (DDFA) to find the optimal blocks for embedding so that a balance between imperceptibility and robustness can be achieved. DDFA is an improvement of firefly algorithm, which works on distinct, discrete values to find the optimal blocks then Hadamard transform is applied on these blocks and then watermark is embedded in these coefficients. Along with this entropy values of the blocks are also used to find the optimal blocks. The optimization function used to find embedding factor (alpha) is a combination of PSNR, SSIM and NC values of various attacks, so it provides the value of alpha in such a way that a balance can be achieved easily.

A watermarking algorithm using Fuzzy Inference System (FIS) is proposed in [48] which uses blind procedure for extraction and considered Human Visual System (HVS) for embedding. They have used DCT, Fuzzy Inference System, Human Visual System to optimize robustness and imperceptibility but no work is done to make the scheme secure. Authors in [24] have also used the concept of fuzzy interference system.FIS is used here to find contrast and edge values of the images to optimize the value of embedding factor. Firstly DWT is applied on the host image and then entropy of the blocks are calculated, these blocks are rearranged in increasing order of their entropy value and then maximum entropy regions are selected for embedding because these are less sensitive towards various image processing attacks. The embedding factor is a function of contrast value and edge value, here contrast value is taken from the high contrast areas and edge values from higher edges of the host image because human eyes are less sensitive to these areas.

3.7 Machine learning based techniques

A back propagation based NN is applied in [128] for medical applications. In this scheme three watermarks are embedded in the host image for providing the authenticity to the patient's information. These three watermarks are lump image, doctor's signature and patient's information. For watermarking DCT-DWT-SVD combination has been used here and security to the watermark image is provided by using Arnold transform. For security of the text watermarks hamming error correction code and arithmetic compression techniques are used to encode the text watermark before embedding. BPNN is applied on the extracted watermark to minimize the effects of various types of attacks on it. This algorithm shows good results for healthcare applications so that identity of the patients can be secured against various attacks.

Authors have proposed a extreme machine learning (ELM) based fast neural network techniques for watermarking in [75]. ELM is a single layer network which makes its training process fast in just milliseconds and this is the reason why authors have used it instead of ML. For training the low frequency sub bands of the host image, generated by applying DCT on it are used here. In this 2 host images are embedded by using watermark sequence generated by ELM. ELM takes LL sub band of the host image at input layer and generates a sequence at output layer which is used as watermark. The performance of the scheme is evaluated by suing PSNR and SIM, the results show that good robustness and imperceptibility are achieved here.

A time efficient optimized watermarking technique is established in [1] which uses DCT transform for embedding the watermark. The results of the watermarking are optimized with the help of the Artificial Bee Colony (ABC) technique. Instead of using a general embedding factor K-Nearest Neighbor algorithm is used here which predicts the embedding factor. The

authors called this technique time efficient because here meta- heuristic techniques are not used which shows a delay in finding the optimal parameters. The watermark blocks are embedded by using the correlation between the neighboring pixels so that security can be achieved.

A General regression neural network (GRNN) based watermarking scheme is implemented in [20]. It is an adaptive watermarking technique which uses DWT and human visual system (HVS) for embedding the color image. The luminance component of YCbCr is used for embedding and embedding is done by training the GRNN. This scheme is blind as at extraction side GRNN helps to extract the watermark embedded. In this HVS is used to select the appropriate blocks for embedding and a scrambled watermark is embedded in these blocks. The performance of this scheme is also compared with other existing works and it shows good results.

A feature extraction based algorithm for providing robustness is given in [62]. The features are extracted using various techniques like DWT, IWT and SIFT. For embedding cascaded neural networks are used which is combination of two neural networks. The advantage of using cascaded NN is that these do not have problem of predictability and no information is leaked as these problems may occur in using the conventional NN. In this a dynamic pattern is generated by cascaded NN for embedding and embedding factor is optimized using PSO algorithm. The algorithm is evaluated using various parameters like PSNR, EC, DC and NC.

A Back Propagation NN (BPNN) based techniques for social applications is proposed in [127] to provide the security to the watermark image. For watermark embedding DWT-SVD combination is used and BPNN is used to reduce the effect of attacks on the watermarked image. Firstly image undergoes through 3- level DWT and then SVD is applied on both, LL3 sub band of host image and watermark image. Secondly the singular components of the watermark are embedded in S component of the host image. At last this modified S is combined with remaining U and V components and undergoes through inverse SVD and IDWT processes to get the watermarked image. The experiments show that this scheme outperforms other compared attacks but as embedding is done on some components only so any attacker can use the remaining part of the image for his benefits.

A blind watermarking scheme using BPNN is performed by authors in [42], the BPNN is trained to recover the watermark image from watermarked image. It uses wavelet domain of the image for embedding the scrambled watermark using HVS characteristics. For scrambling the watermark Arnold map is used which is shown in Eq. 16.

$$[a' \;\; b'] = [(1 \quad 1 \;\; 11) \;\; (a \;\; b)] \; mod \; X$$ where X is size of the watermark image Eq. 16.

BPNN is trained to learn the relationship between original and embedded image so that it can be used at extraction time. BPNN uses mean square error and Gradient Descent to find weights of the network. In this network 3 layers are used, one is input layer having 9 neurons, second is hidden layer having 18 neurons and last is output layer having one neuron. An optimized watermarking scheme based on BPNN is proposed in [114] along with Arnold transform. For security reasons multiple keys are used to scramble the watermark and multiple variables are used in Arnold transform. In this scheme the watermarked image is compressed using BPNN and then scrambled watermark obtained by using improved Arnold is embedded into it. Now image is decomposed again to get the watermarked image. The watermark extraction process is similar to the embedding process and it does not need the original image and original watermark which makes this scheme secure and blind.

Authors in [69] proposed a scheme which aims to provide feasibility, robustness, network capacity by using neural network. For copyright protection of the image NN based image

batch copyright protection scheme is used, by using it a copyright message bit stream can be extracted from each cover image while no modifications. A number of RGB images have been used to train the model. In [104] an enhanced time efficient secure watermarking scheme is proposed which uses ant colony optimization and light gradient boosting algorithm for optimization. In this Twenty four grayscale images, of size 512 × 512, are selected as training. To reduce the time taken by algorithm K-NN along with ant colony optimization algorithms have been used.

Most of the researches have using used machine learning techniques to make the watermarking scheme time efficient by training the model fast as these have less number of layers then deep learning networks. But a good balance between various characteristics of watermarking is not found using only ML based techniques in some of the papers.

3.8 Deep learning based techniques

Artificial Intelligence is the umbrella under which machine learning comes and deep learning comes under machine learning. Deep learning mimics the working of human brain and processes this data to make decisions. In deep learning Convolutional Neural Network (CNN) is used to train and test the model. Image recognition, image classification, object detection, Face recognition and watermarking are some of the areas where CNNs are widely used. In deep learning, model learns to do any computational tasks by directly learning from images or videos. Deep learning models are used to achieve a better accuracy which sometimes human brain cannot achieve. The reason of using neural network in watermarking is that it decreases the execution time when compared with other fuzzy based techniques.

In [80] a blind watermarking technique to achieve robustness is proposed which uses CNN technique. In this 4000 24-bit color images from the BOSSBase dataset are used for training the model and for learning model have taken 1 day. This learning process includes watermark embedding, simulation of various attacks on it and then updating the weights of the network. Most of the researchers have used Quantization Index Modulation (QIM) for making the networks o here authors have used Quaternion DFT (QFT) techniques and QIM combination for this purpose. A collection of ReLU and Fully connected layers are used here for creating the CNN model.

In [65] a blind CNN based watermarking for smart city applications has been proposed which uses Fast R-CNN technique to train the system. To ensure the security of the watermark image it is randomly scrambled before embedding so that it cannot be recognized by an illegal attacker. For watermark detection and extraction cooperative neural network is used here and for extraction host image is not required which makes this technique a blind one.

Authors in [12] have developed a framework for finding the appropriate embedding strength parameter so that a balance between robustness and imperceptibility can be achieved easily. For embedding DWT-DCT combinations are used and experiments are performed on COCO dataset available at [17]. Rather than using conventional CNN, Mask RCNN is used here because it is much faster than CNN and shows very good performance for semantic segmentation. The mask values of the host images are calculated by using mask RCNN. Here firstly, saliency detection algorithm is applied on the host image to find blocks having minimum saliency and then Mask RCNN is used to find the ROI areas by semantic segmentation. Then host image is divided into 128*128 blocks and blocks having lower ROI pixels are selected for embedding after this 2D DWT is applied to convert t into 4 sub bands. At last LH, HH and HL sub bands are divided into 8*8 blocks and DCT is applied on these sub blocks to embed the watermark bit wise. Similarly extraction is performed.

Authors in [21] proposed a watermarking scheme to maintain the intellectual property of the deep neural network, embeds the watermark and verifies the information of the owner. In this image set-5 is used as host image of size 512*512 and all the experiments are performed in Python. Here the use of DNN is to verify whether the extracted watermark is similar to the original one or not. It achieved an accuracy of 51.89% but in some cases this model gives inconsistent results. A two stage watermarking scheme for blind application is proposed in [68] which uses 2 stage separable deep learning (TDSL) network. The advantage of TDSL is that it is noise free network and has good training process because of this feature; it provides better stability, good results, fast performance and better robustness in presence of various attacks. In deep learning network encoder and decoders are used for embedding the watermark and to recover it. The experiments are performed on 1000 images of COCO dataset in which 996 images from CIFAR-10 dataset are used for training and testing the scheme.

In [79] authors have used Reinforcement machine Learning to find robust domain from attacks, this scheme is a blind one in which for watermark extraction there is no need of original cover image or watermark image. The authors have used image watermarking networks called WMNet using convolutional neural networks (CNNs) and for its training 4000 24-bit color images from the BOSSBase dataset have been used. The motive of this scheme is to find a balance between imperceptibility and robustness which is very difficult to achieve. It has proposed 2 methods for embedding, one using BPNN, SDT and another using auto encoder, where auto encoder is a feed forward network gradient. Eight different types of attacks are applied on these schemes to prove it robustness and Adam descent is used here rather than using Gradient descent because it has better loss reduction capacity.

A DWT based watermarking scheme along with Entropy and Neural network is explained in [46]. In this image is divided into 4 sub bands using DWT and then entropy of each block is calculated. Now blocks having largest entropy values are selected for embedding because these have less information. The regression NN is used to find the relationship between original and embedded image so that it can be used at extraction time. In this embedding is not performed in LL sub band because LL sub band is not good for embedding s these shows low entropy value which contains most of the information [112] and does not perform good against compression attacks. In [54] authors have proposed a non blind technique to achieve the feature of robustness and imperceptibility in transform domain. This technique is based on auto-encoder Convolutional Neural Network (CNN) and it is trained using standard gradient descent back propagation algorithm, the performance of the scheme is measured by NC and BER. Authors in [129] have also proposed a blind watermarking technique to achieve robustness, high capacity and security by using DWT, SVD and CNN. For showing the performance PSNR and NC parameters are used and compared with other schemes.

CNN based techniques provides a balance between imperceptibility and robustness of the watermarking scheme by training the model which can be used at extraction time also so that watermark can be extracted easily without using Cover image.

4 Summary and discussion

From the above study, it can be summarized that there are various applications of watermarking and a number of research is done in this field, some are in spatial domain while rest are in transform domain. Spatial domain techniques have less computational cost while transform domain have high computational cost but the robustness provided by spatial domain

is very less in comparison to the transform domain techniques. Spatial domain techniques provide very good imperceptibility and can be applied in data hiding or copyright applications but these do not resist against attacks because of that researchers move towards the transform domain techniques. Transform based techniques can be applied to provide imperceptibility, robustness and temper recognition applications. There are a number of methodologies which are used under this umbrella, and are explored in this paper and are shown in tabular form in Table 2. Each methodology has its own advantages and disadvantages like DCT based techniques are very imperceptible and robust but these do not work well against cropping and scaling attacks and these are difficult to implement. Most of the researchers have used middle frequency components of DCT to embed the watermark as embedding in low frequency components introduce distortions but provides good robustness while embedding in high components decreases the quality of the image and increases robustness. So embedding in these two frequency components does not provide a balance between robustness and imperceptibility. Similarly DWT based techniques provide very good imperceptibility but are not so much robust. In DWT mostly embedding is done in LL sub band which has most of the information of the image and provides more robustness. DFT has a problem of shift invariance because of that some researchers has used QDFT based scheme to provide more robustness against geometric attacks. SVD scheme shows good performance against cropping and geometric attacks but these have problem of false positive as explained earlier as well as these cannot be considered for rightful ownership. So a huge amount of research is done by combining these techniques and called it hybrid technique so that a balance between various characteristics can be achieved.

Some authors have used Region of Interest (ROI) based techniques, this is a good idea to embed the data only in interested regions of the image but these have a problem that these only embed data in some regions and leave other part of the image as it is without applying any security to that so any unauthorized user can take these parts to embed his watermark and claim for the image. Some authors have used entropy as a factor to select the blocks for embedding, in this embedding in high entropy areas is a good idea as these are most robust against image processing attacks and are low information areas. To calculate performance of the schemes MSE and PSNR are good measures and most of the researchers have used these two. From NC values it can easily be compared that which technique works well under what type of attacks. In watermark embedding the embedding factor often called α (alpha) plays a very important role [51] as a smaller value of α gives good PSNR but not robustness and its very high value gives robustness but not good imperceptibility. So a number of optimized techniques are used to find the best value of α to get a trade-off between these two. One of the optimization techniques is meta-heuristic but these takes more time for finding the optimal value of α because of that these can't be applied in real time applications. Some has used Back propagation Neural Network (BPNN) to embed the watermark, BPNN based schemes suffer from scaling attacks because these only remembers relationship between neighboring pixels are not good for big data analysis. Some has used k-NN (K-Nearest neighbor) algorithm to find relationship between neighboring pixels but these applications need for storage space. CNN based techniques provide a good balance between imperceptibility and robustness but are difficult to implement. So currently a huge amount of research is doing in deep learning and machine learning based watermarking techniques to achieve balance between various characteristics as well as making watermarking process blind so that security can be achieved. Table 2 provides a summary of various techniques used in field of image watermarking and compared these in terms of their performances. It shows the image size and image type used by

Table 2 Comparison of various techniques

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
LSB Watermarking [108]	Imperceptibility	Non-Blind	Grayscale Size = 512*512	PSNR = 51.147 MER = 0.50 BER = 0.50	No attacks are Applied	This Scheme is not robust and is only imperceptible.
Shell based scheme [73]	Imperceptibility Capacity Robustness	Non-Blind	Color,/ Gray	PSNR = 52.1513 BER = 3.9622 NC = 0.783 (For Cr attack)	GN, Cr, JPEG, SH,	This technique survives against some of the attacks but does not provide good robustness and error rate is also high
LSB Embedding in 3rd and 4th bit[[14]	Security, Imperceptibility	–	Grayscale, 512*512/ Bytes, 128 and 1023	PSNR = 52.7970 (Dock Image)	No attacks are applied	Provides an improved LSB based technique but no work for robustness is done.
Block SIRD based, Masks [4]	Imperceptibility and Robustness	Non-Blind	Color, 512*512/ Gray, 64*64	PSNR = 50.63 SSIM = 0.9934, GEI = 0.3333, NC > 0.9 For all attacks except Cropping	S&P, SN, AF, JPEG Compression, Cr, LSB reset, RS	Provides a balance between robustness and imperceptibility but relatively low value of NC for cropping attack
K-means Clustering, Region Approximation [83]	Robustness & Imperceptibility	–	Gray, 512*512/ Gray 128*128	SNR = 41.18, FAR = $5.9352*10^{-5}$, FRR = $1.2803*10^{-4}$	MF, GN, JPEG compression, Sc, Rot	In this clustering techniques are used to find regions of embedding where robustness will be high.
DC coefficients, MD-5 [113]	Robustness & Imperceptibility	Blind	Color, 512*512/ Grayscale, 32*32	PSNR = 49.9898 SSIM = 0.9872 NC = 1 (without attack)	JPEG, S&P, GN,MF, MAA, GA	The capacity of the scheme is very less and is not good for JPEG compression NC = 0.7673
DCT, Decison Tree, Arnold transform [86]	Robustness	–	Color & Gray scale Size = 512*512	PSNR = 50.37 (Gray)	No attacks are applied	Scheme is not robust
DCT, Arnold, Chaotic map [92]	Robustness, Security	–	Gray, 512*512/ Binary 64*64	PSNR = 41.52 NC = 1 (for no attack)	JPEG, Sc, GN,	A less number of attacks are applied on the scheme which does not proves its robustness against other attacks
DCT, Arnold, SPIHT [102]	Robustness, Imperceptibility	–	Grayscale, 512*512/ Binary 62*64	PSNR = 36 SSIM = 0.9750, NC = 0.9831 TAF = 1.36	Cr, Noise, SH, HE, auto contrast operation	More robust against compression attack but not good against cropping, noise and sharpening attacks. Low PSNR value is obtained.
DCT, Genetic Algorithm [96]	Imperceptibility and Robustness	Blind	Gray, 512*512/ Binary, 4096 sized sequence	PSNR = 49.74 NC = 0.97	S&P, GN,MF,MDF, SH	The algorithm shows good robustness against JPEG compression along with other attacks
DCT, DWT, Arnold [3]	Robustness & Imperceptibility	Non- Blind	Gray, 512*512/	PSNR = 47.1836, NC = 0.1936 for k = 10 scaling factor) (For baboon image)	Rot, Noise, Filtering, RS, JPEG, SH, Blurring	Embedding of parts of watermarks are done in DWT sub bands rather than complete watermark but no balance between PSNR and NC value is achieved.

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
QDWT, DCT, Arnold, iterated sine chaotic system [35]	Copyright Protection	Blind	Color, 512*512/ binary, 64*64	PSNR = 49.6142 NC > 0.9 (For most of the attacks)	GN, S&P, Sc, JPEG, Cr, Row deleting, image adjusting, Br, Rot	Watermark is embedded in middle frequency components of DCT and provide good robustness for some attacks.
DCT, 2D LDA [15]	Imperceptibility	Blind	Color, 512*512 / 32*25	PSNR = 44.49 BER = 0	Cr, Dis, Mosaic Blurring	The proposed scheme is simple to implement and need less processing power.
DCT, Arnold, Chaos, Hamming code, DWT [53]	Robustness, Imperceptibility, Security	Blind	Color, 1024*1024/ Gray 64*64	PSNR = 42.01 NC > 0.9	GN, S&P, SN, JPEG, MDF, Adaptive White GN, Sc	It Shows robustness against some of the attacks and error is reduced using error correction codes.
DCT, ZIP Compression [89]	Robustness, Imperceptibility	Non-Blind	Gray X-ray Images/ Patient Name, ID as watermark	CC = 0.93	No Attacks are performed	This scheme is applied on X-ray images and can also work for audio watermarking but no robustness proof is done against any attacks.
DCT, DE, KELM [123]	Imperceptibility, Robustness, Optimized scaling factor	Semi-Blind	Gray, 512*512/ Gray, 32*32	PSNR = 44.9 NC > 0.9 except Rot attack	MF, AF, RS, JPEG, Rot, HE, GN, WF, GF	It is not good against rotation attacks but works very good against other attacks in comparison to [6].
DWT, Arnold [67]	Robustness & Imperceptibility	Non-Blind	Gray, 512*512 / Binary	PSNR = 41.938 NC = 1 (for no Attacks) NC = 0.8429 (for Cr attack)	MF, WF, GN, S&P, WC, JPEG, CR	Provides robustness and imperceptibility against some attacks.
2D –DWT, Encryption [9]	Security, Imperceptibility, Robustness	Non-Blind	Color, 228*228 / Gray 90*90	PSNR = 54.96 MSE = 0.2047 CC = 0.9749	S&P, GA, Rot, JPEG	It is an Encryption based watermarking scheme, which shows robustness against compression attacks but not good for geometric attacks and have low capacity.
2 D-DWT in Multiple scale, similarity index [124]	Security	Non-Blind	Color, 256*256/ Color 64*64	Similarity = 75.74% Noise = 83.94% Filtering = 70.87%	Compression, Noise, Filtering	In this a color image is embedded in color host image using Haar transform to provide security to image information but only few number of attacks are performed.
DWT, Chaotic Discrete Time Transform [36]	Robustness, Security	Non-Blind	GrayScale 512*512 / No information	Cor = 0.9697	Statistical attacks	Its shows high security against statistical attacks but is very complex to implement for multimedia applications.
2D-3level DWT, Alpha blending technique [58]	Imperceptibility, Quality	Non-Blind	Gray, 256*256/ Gray, 256*256	PSNR = 45.72 MSE = 1.74	No Attacks are performed	It is a 3 level DWT scheme used to provide invisibility and quality to the watermarked image but with lower value of embedding

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
						factor watermark become visible and PSNR become low.
DWT, Optimal channel selection [118]	Robustness & Imperceptibility	Non-Blind	Color, 512*512 / Binary	PSNR = 46.05 BER = .232 (Rot attack), BER = 0 (no attack)	Sc, Cr, Rot, GN, S&P, AF, MDF, GF, Blur, SH, JPEG	It is a wavelet quantization based technique which shows good results but BER is not good against Rot attack.
RDWT, SVD, Self adaptive DE algorithm [121]	Security, Imperceptibility, Capacity	Blind	Grayscale 512*512	PSNR = 53.6117 Capacity = 4	S&P, GC, Rot, JPEG, Cut, translation	This scheme is not good against Rot attack and achieved PSNR = 8.9100 but shows good embedding capacity than compared works.
PCA, RDWT,IGWO [19]	Imperceptibility, Robustness	Blind	Grayscale	PSNR = 67.87 MSE = 0.0106 NCC = 0.995 SSIM = 0.9997	GN, Rot, Sc, Compression, RS, HE, MDF, Blur, SH	An improved optimized watermarking scheme for gray scale image is proposed using PSA algorithm. It can be improved to work for color images.
DWT, SVD, Block selection scheme [99]	Robustness, Security	Blind & Non--Blind	Color, 512*512 / Binary image 50*20	PSNR = 61.7524 SSIM = 0.9999 Cor = 1	GN, S&P, PN, SN, Rot, JPEG	It provides better robustness against geometric and other image processing attacks. It can be improved to provide minimum false positive rate and fidelity. It is not good for active attacks.
DFT [91]	Security	–	Bitmap 512*512	PSNR = 53.3	JPEG, Blurr, PS, PC	It is simple and device independent scheme which can be used for printing processes and it is a fast algorithm.
QDFT, Spatio chromatic DFT [120]	Imperceptibility	Non- Blind	Color, 512*480	PSNR = 30.1027	JPEG, RS, Rot, SH, Cr, HE, GN, Color to Gray conversion	It is a new approach which embeds watermark into luminance and chrominance components but there is no interaction between these two.
4D-QDFT, Arnold [16]	Capacity, Robustness, Fidelity	Blind	Color, 512*512, 128*128, 256*256 / Color, 32*32	PSNR = 37.025 NC > 0.8	Cr, Filtering, JPEG, Noise, GA, S&P	It is a 4D QFT scheme used to improve capacity of the watermark and decreases the energy loss by implementing relationships between QDFT and DFT channels.
QDFT, DFT, FFT [125]	Robustness, Imperceptibility	–	Color, 512*512 / 45,000 bit	PSNR = 39 MSE = 1 NPCR = 480,423 NPQ = 217,267 Capacity = 196,414	GN, HE, JPEG, Sc, Rot, Cr, MDF	It is a multi variant watermarking scheme and provides good PSNR value but capacity of the scheme is very less.
QDFT, MPSAN, PSO, MM, EPA [39]		Blind	Color 512*512/ Color 64*64	PSNR = 39.3 MSSIM = 0.966	PEG, Noise, Filters, Cr, Luminance	

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
	Robustness, Imperceptibility, Payload					It out performs various current methods in terms of quality and robustness for particular payload.
Dual Tree CWT [13]	Robustness, Imperceptibility	Non- Blind	Color 512*512 / Binary, 128*128	PSNR = 41.23 Cor = 0.91	No Attacks are performed	No attacks are performed to prove its robustness. This scheme can be used for data distributions.
FFT, Butter Worth Filter, Pixel shuffling [71]	Robustness, Imperceptibility, Security	Non- Blind	Gray	PSNR = 44.2823 BER = 0 NC = 1 (Without any attack)	S&P, SN, HE, Local variant	This scheme shows robustness and security but comparison of results are not performed to validate the results.
DFT, DCT, Arnold [34]	Imperceptibility, Robustness, Security	Blind	Gray 512*512, / Gray, 19*52, 64*64	PSNR = 61.28 NC > 0.9 (For most of the attacks) SSIM = 0.9998	Noise, Compression, HE, Filters	It is a combined technique used to provide robustness, imperceptibility and security. Here embedding is done in middle components so robustness is not up to the mark.
Demeyer DWT, DFT, SVD [98]	Robustness, Imperceptibility, Capacity	Non-Blind	Color, 512*512 / color, 512*512	PSNR = 26.5712 SSIM = 0.9604 (Pepper image)	GN, SN, S&P, Cr, Rot, JPEG	The scheme does not have a good balance between imperceptibility and robustness. PSNR<30 is achieved here which is not acceptable.
DWT, DFT, SVD, YCbCr space [5]	Robustness, Imperceptibility, Payload	Semi-Blind	Color / Grayscale	PSNR = 33.86 Cor > 0.9	Blur, Cr, GN, SH, AF, Rot, HE, GIC	In this scheme maximum efficiency of color space can be achieved using some other color space model instead of using YCbCr.
DWT, SVD, Hamming Code [117]	Robustness, Imperceptibility	Blind	Grayscale 1024*1024/ Gray 32*32, 367 characters	PSNR = 43 WPSNR = 52	Noise, Cr, Filtering, Rot, Check mark attack	This scheme is for medical applications. The performance of this scheme is good for medical applications in comparison to natural images.
DWT, SVD [111]	Robustness, Imperceptibility, Security	Non-Blind	Gray	PSNR = 27 (logo) 26 (QR code) CC = 0.9663 SNR = 21.4146	WF, MDF, Rot, S&P	In this scheme PSNR values are not good against various attacks.
DWT, SVD, Zernike moment [66]	Robustness,	Blind	Gray 512*512, / Gray, 32*32	PSNR = 42.0641 NC = 1 (Without attack)	Translations, Scaling, Rot, JPEG, Flipping	This scheme shows robustness against various image processing attacks along with Geometric attacks
DWT, SVD, LU decomposition [49]	Robustness, Imperceptibility, Security	Non-Blind	Gray, 512*512 / Gray, 256*256	PSNR = 38.82	Filtering, Sc, Rot, S&P	This algorithm can be applied on MM applications and for copyright protection of

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
						data but it gives low PSNR value for some attacks
DCT, DWT, SVD, Progressive QIM, Arnold [40]	Robustness, Imperceptibility, Security	Blind	Gray, 512*512 / Binary, 64*64	PSNR = 40.02	JPEG, JPEG-2000, GN, S&P, MDF, GF, Sc, Rot, RR, Darken	It is a blind multiple watermarking scheme and provides good robustness against JPEG and JPEG-2000 compression.
ECC, DWT-SVD, Entropy, HVS based model [33]	Robustness, Imperceptibility	Semi-Blind	Grayscale 512*512/ Gray 32*32	PSNR = 61.32 SSIM_index = 0.9989	MDF, Cr, GN, WN, JPEG	Elliptive Curve Cryptography provides good watermarking performance results in comparison to other works.
DWT, SVD, Entropy, Pixel position shuffling [31]	Robustness, Imperceptibility, Security	Non-Blind	Gray, 512*512/ Gray, 32*32	PSNR = 42.6369 NC = 1 (For no attacks)	MDF, AF, JPEG, Rot, GN, EF, GF, S&P	This algorithm provides very good results for robustness and imperceptibility but is not time efficient.
DCT, DWT, SVD [29]	Robustness, Imperceptibility		Gray 512*512, / Binary, 32*32	PSNR = 56.899 NC = 0.97	Translations, Flipping, Sc, Cr, Rot, JPEG, GN, S&P, AF, MDF	This scheme shows good robustness against geometric attacks along with other image processing attacks.
Least square curve fitting, DCT, DWT, SVD [55]	Robustness, Imperceptibility,	Non-Blind	Gray, 512*512 / Binary, 32*32	PSNR, BER	JPEG, GN, S&P, SN, MDF, AF, GF, HE, Sc, Cr, SH	In this scheme middle frequency sub bands are chosen for embedding but results of NC are not good for geometric attacks.
IWT, SVD, SHAI, ABC [45]	Robustness, Imperceptibility, Security, Capacity	Non-Blind	Gray, 512*512 / Gray, 256*256	PSNR = 43.1165 NCC = 0.9459	AF, Sc, GC, MF, SN, S&P, Cr, JPEG, CA, Translation, Blur	This scheme provides good imperceptibility, robustness, security and capacity to watermark using a new signature generation algorithm, but signature recovery is not good against geometric attacks.
DWT, SVD, ABC, Arnold Chaotic map [103]	Robustness, Imperceptibility, security, capacity	Semi-Blind	Color, 512*512/ color, 512*512	PSNR = 77.4875 NC > 0.9 (For most of the attacks) SSIM = 0.9940	AN, Filtering, GA, S&P, GN, SN, MDF, AF, WF, BF, JPEG, Rot, HE, cut, shear	This scheme has increased capacity to handle watermark image and provides security against various attacks. It outperformed other compared works in terms of PSNR and NC value
DWT, Cuckoo optimization [8]	Robustness, Imperceptibility,	Non-Blind	Gray, 256*256/ Binary logo, 128*182, 64*64	PSNR = 38.0358 NC = 0.8589	GC, MDF, Cr, Rot, HE, GN, JPEG, Blur, RS, SH	In this scheme no security measures are taken and it provides poor NC values against Rot attacks.
SVD, GA, RDWT, SVD, Cuckoo [47]	Robustness, Imperceptibility		Gray/ Gray	PSNR = 36.39	GC, Cr, MDF, Rot, Translation, HE, JPEG, GN, Flipping	This scheme provides copyright and ownership protection by using a variant of DWT called RDWT
DWT, SVD, PSO [122]		Non-Blind				

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
	Security, Robustness, Imperceptibility,		Gray, 512*512 / Gray, 128*128	PSNR = 62.0047 (For water image) NCC > 0.9 (For all attacks)	Rot, Cr, CA, GC, Noise attacks, Filtering, RS, HE	This scheme shows more robustness against filtering attacks.
DPSO, DWT, SVD [70]	Robustness, Imperceptibility		Color	PSNR = 39.792	GN, S&P, Rot, MDF, GC, BF	No measures are taken to prove robustness of the scheme. This scheme shows a comparison between PSO and GDPSO to prove that results of GDPSO are better.
DWT, SVD, CACO [50]	Robustness, Imperceptibility		Gray, 128*128/ Binary, 2.2 KB	PSNR = 45.12 BER = 0% PRD = 0.015 KL Distance = 0.68	No attacks are performed	This scheme is applied on ECG stegnography images but shows poor results with increasing size of watermark bits and no compression techniques are used to solve this problem.
Entropy, Hadamard transform, DDFA [76]	Robustness, Imperceptibility,	Blind	Gray, 512*512/ Gray, 64*64	PSNR = 47.984 NC = 0.9942	MDF, GF, AF, GC, Noise, Cr, Sc, Rot, JPEG, AF	It provides poor robustness against mean filter while works good against other attacks.
ELM, DCT, Coax Method [75]	Robustness, Imperceptibility, fast	Blind	Gray/ Gray	PSNR = 60.40434 SIM = 20.4956 RMSE = 0.0166	No attacks are performed	It is a fast neural network technique of watermarking. No work is done to show robustness.
DCT, DWT, SVD, Arnold, Hamming code, lossless Arithmetic compression, BPNN [129]	Robustness, Imperceptibility, Security	Non-Blind	CT-Scan images, 512*512 Gray, 256*256 / text, 90 char	PSNR = 43.88 NC = 0.9888 BER = 0.2174	JPEG, S&P, GN, Filtering, Rot, Cr, RS	It is a multilevel watermarking scheme to secure patient's information. For high gain factor the quality of watermarked image is poor.
DCT, ML, ABC, K-NN [1]	Robustness, Imperceptibility	Blind	Gray, 512*512/ Gary 64*64	PSNR = 40.583 (Barbara image)	JPEG, MDF, S&P, HE, GC, GF, AF, MF, Cr, Rot	This scheme shows very good results but because of using K-NN large memory is required.
4D-DWT, YCbCr color space, GRNN, HVS system [20]	Robustness, Imperceptibility, Security	Blind	Color 512*512/ Binary 64*64	PSNR = 42.83 WAR = 100% (without attack)	Scaling, GN, JPEG, S&P, MDF	It shows good WAR % against various types of attacks and compared their work with BPNN network based so shows its importance.
DCT, DWT, Cascaded NN, SIFT [62]	Robustness, Imperceptibility,	Non-Blind	Coral Image Dataset	PSNR = 95.4271 NC = 0.87451	No attacks are performed	It shows better performance than NN and SFIT based techniques but there is a problem of accuracy of fitness function because of PSO.
DWT, SVD, BPNN [127]	Robustness, Imperceptibility, Security	Non-Blind	Color, 512*512/ Color, 64*64	PSNR = 36.26 NC = 0.98	RS, Cr, S&P, JPEG	This scheme can be applied for social applications and is complex in terms of computations.
DWT, Arnold, BPNN [42]		Blind		PSNR = 45.55	Filtering, Sc, Cr, S&P, JPEG	

Table 2 (continued)

Technique used	Purpose	Scheme Type	Cover Image /Watermark Details	Results (For Lena Image)	Attacks	Remarks
	Robustness, Imperceptibility, Security		Grayscale 256*256/ Grayscale 25*25	NC = 1 (without attack), NC < 0.9 at low pass filter		PSNR<30 is achieved at median filtering attack and no balance between robustness and imperceptibility is achieved.
Arnold Transform, BPNN [114]	Robustness, Imperceptibility, Security	Blind	Gray, 512*512/ Binary 64	PSNR = 51.6799 (For cameraman image) BER = 0.0061 NC = 0.9982	HE, GN, S&P, MDF, JPEG, GA, Rot	The experiments are performed on USC-CIPI dataset. For some attacks PSNR value is very poor and less than 20.
CNN, QFT, QIM [80]	Robustness	Blind	Color 512*512BossBase Dataset	PSNR	Affline transform, Cr, JPEG, Noise, GF, MDF, Rot, Sc	It is a robust watermarking scheme using CNN and has 1 day training time.
Fast RCNN, DCT, DWT [65]	Robustness, Transparency, Security	Non-Blind	Image Dataset	PSNR = 50.12 (For Baboon image) Execution time = 1.1962	No attacks are performed	It shows a classification accuracy of 93.75% and used fast RCNN to increase the speed.
DWT, DCT, Mask RCNN [12]	Robustness, Imperceptibility	Blind	COCO Dataset/4*4	PSNR = 49.1052 SSIM = 0.9985 NC = 1	GN, JPEG, MDF, HE, S&P	It is a ROI based blind watermarking scheme and provides redundancy improvement by embedding watermark bit 15 times.
DNN [21]	Intellectual property, Ownership Identification		Image set −5, Gray 512*512	Accuracy = 51.89%	No Attacks are performed	This model has achieved an accuracy of 51.89%, but in some cases it gives inconsistent results.
TDSL, YUV Space [68]	Security Privacy, COCO dataset	Blind	–	PSNR = 63.4	JPEG, GF, Cr	Satisfactory results are found for watermarking.
Reinforcement ML, WMnet [79]	Imperceptibility and Robustness	Blind	BossBase Dataset, color, 512*512	PSNR = 40, NC = 1	JPEG, Cr, Rot, RS, GN, S&P, GC	The results of this scheme are compared with QIM and QDFT based techniques. It shows better performance than these.
DWT, Entropy, GRNN, Moving average filer [46]	Robustness & Imperceptibility	Blind	Gray, 512*512/ Gray 512*512	PSNR = 56.7584, NC = 0.9900 MSE = 56.7584 (for no attack)	GN, Cr, MDF, Rot	It shows good results except for compression attack. NC value is smaller by 2–9% from compared works.

Table 3 Various Techniques used for watermarking

Technique	Abbreviation	References
Ant Colony Optimization	AC	[56]
Arnold Transform	AT	[53] [67] [86] [92] [102] [3] [35] [16] [34] [40] [129] [114]
Artificial Bee Colony	ABC Optimization	[45] [1] [103]
Chaotic map	Chaotic map	[92] [35] [103]
Continuous Wavelet Transform	CWT	[13]
Convolution Neural Network	CNN	[80] [65] [12]
Cuckoo Search Optimization	CSO	[8] [47]
Decision Tree	Decision Tree	[86]
Discrete Cosine Transform	DCT	[86] [92] [102] [96] [3] [35] [15] [53] [89] [123] [35] [34] [40] [29] [55] [75] [129] [1] [62] [65] [12]
Discrete Fourier Transform	DFT	[91] [125] [34] [98] [5]
Discrete Wavelet Transform	DWT	[3] [9] [124] [36] [58] [118] [99] [98] [5] [117] [11] [66] [49] [40] [33] [31] [29] [55] [103] [8] [122] [70] [50] [129] [20] [62] [127] [65] [12] [46]
Elliptive Curve Cryptography	ECC	[33]
Entropy	Entropy	[33] [31] [76] [46]
Extreme Machine Learning	ELM	[75]
Fast Fourier Transform	FFT	[71] [125]
Genetic Algorithm	GA	[96] [47]
Hamming Code	Hamming Code	[117] [129]
Integer wavelet Transform	IWT	[45]
Least Significant Bit	LSB	[108] [14] [73] [14]
Machine Learning	ML	[1] [79]
Message Digest-5	MD-5	[113]
Neural Network	NN	[129] [20] [62] [127] [21] [114] [46]
Particle Swarm optimization	PSO Optimization	[39] [122] [70]
Pixel Shuffling	Pixel Shuffling	[71] [125] [31]
Principle Component Analysis	PCA	[19]
Quantization Index Modulation	QIM	[40] [80]
Quaternion DFT	QDFT	[120] [16] [125] [39] [80]
Quaternion DWT	QDWT	[35] [67]
Redundant DWT	RDWT	[121] [19] [47]
Singular Value Decomposition	SVD	[121] [99] [98] [5] [117] [111] [66] [49] [40] [33] [31] [29] [55] [45] [103] [47] [122] [70] [50] [129] [127]
Two dimension Linear Discriminate Analysis	2 D LDA	[15]
ZIP Compression	ZIP	[89]

various authors as well as a number of attacks used by them to compare these. Table 3 has listed various techniques used by the authors and their reference numbers along with abbreviations used for particular technique.

5 Conclusion and future work

The concept of digital watermarking gives the users freedom to provide their content online to other users while maintaining its authenticity and copyright protection. Digital watermarking provides the copyright protection, temper proofing and fingerprinting to various types of content like audio, video or images. Watermarking can be performed in spatial frequency domain. In spatial domain watermark bit is directly embedded into the pixels of the cover image. Least Significant Bit (LSB), patch work are some of the methods used under spatial domain watermarking. But these methods are not secure and it also degrades the quality of the cover image, so frequency domain watermarking is more useful. In frequency domain watermarking bits are spread throughout the image so no one can easily detect the watermark image. In frequency domain DCT, DWT, DFT, LWR and SVD techniques are used. This paper has reviewed various researches done in this field and shows a summary of these shown in Table 2. Some provides only imperceptibility while other provides imperceptibility and robustness both. Some has also worked to provide security to the watermark image by any encryption algorithm, scrambling or by Arnold transform. Now a number of machine learning and deep learning techniques are being used in the field of watermarking to increase balance between robustness and imperceptibility and to make algorithm time efficient.

In future work can be extended for other types of data used for watermarking like audio or video and some schemes can be developed to provide a good balance between imperceptibility, robustness and security.

Compliance with ethical standards

Conflict of interest The Authors declare that they have no conflict of interest.

References

1. Abdelhakim A, Abdelhakim M (2018) A time-efficient optimization for robust image watermarking using machine learning. Expert Syst Appl 100:1–35
2. Abdelhakim A, Saleh H, Nassar A (2016) Quality metric-based fitness function for robust watermarking optimisation with. Bees algorithm IET Image Processing 10(3):247–252
3. Abdulrahman A, Ozturk S (2019). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimedia Tools and Applications:1–23.
4. Abraham J, Paul V (2016) An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University - Computer and Information Sciences 1-10:31–133. https://doi.org/10.1016/j.jksuci.2016.12.004
5. Advith J, Varun K, Manikantan K (2016). Novel digital image watermarking using DWT-DFT-SVD in YCbCr color space. IEEE: 1–6.
6. Agarwal C, Mishra A, Sharma A (2013) Gray-scale image watermarking using GA-BPN hybrid network. J Vis Commun Image Represent 24(7):1135–1146
7. Agarwal N, Singh A, Singh P (2019). Survey of robust and imperceptible watermarking. Multimedia Tools Application Springer: 1–31
8. Ali M, Ahn W (2014) An optimal image watermarking approach through cuckoo search algorithm in wavelet domain. Int J Syst Assur Eng Manag 9:1–10
9. Ambadekar P, Jain J, Khanapuri J. (2019). Digital image watermarking through encryption and DWT for copyright protection. https://doi.org/10.1007/978-981-10-8863-6_19
10. Arnold M (2000) Audio watermarking: features, applications and algorithms. Proceedings of IEEE International Conference on Multimedia & Expo, New York, pp 1013–1016. https://doi.org/10.1109/ICME.2000.871531

11. Asikuzzaman M, Pickering M (2017) An Overview of Digital Video Watermarking. IEEE Transactions on Circuits and Systems for Video Technology 28:1–23. https://doi.org/10.1109/TCSVT.2017.2712162
12. Bagheri M, Mohrekesh M, Karimi N, Samavi S (2020). Adaptive control of embedding strength for image watermarking using neural networks: 1–4
13. Balakrishnan A (2020). Digital Watermarking Technique using Dual Tree Complex Wavelet Transform. First International Conference on Power, Control and Computing Technologies (ICPC2T) IEEE:62–67.
14. Bamatraf A, Ibrahim R, Salleh M (2011). Digital watermarking algorithm using LSB. International Conference on Computer Applications and Industrial Electronics (ICCAIE) IEEE Xplore: 155–159.
15. Chang T, Pan I, Huang P, Hu C (2018) A robust DCT-2DLDA watermark for color images. Multimed Tools Appl 78:1–23
16. Chen B, Coatrieux G, Chen G, Xingming S, Coatrieux J, Shu H (2014) Full 4-D quaternion discrete Fourier transform based watermarking for color images. Digital Signal Processing 28:106–119
17. COCO n.d.. Dataset available online at- http:// cocodataset.org.
18. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Transaction Image Processing 6(12):1673–1687
19. D Rajani, P Rajesh (2020). An optimized blind watermarking scheme based on principal component analysis in redundant discrete wavelet domain. Signal Processing: 1–15
20. Dang H, Kinsner W (2012). An intelligent digital colour image watermarking approach based on wavelets and general regression neural networks. Proceedings of the 11th IEEE international conference on cognitive informatics and cognitive computing ICCI*CC: 115–123
21. Deeba F, She K, Dharejo F, Memon H (2020) Digital Watermarking Using Deep Neural Network. International Journal of Machine Learning and Computing 10(2):277–282
22. Deguillaume F, Voloshynovskiy S, Pun T (2003) Secure hybrid robust watermarking resistant against tampering and copy attack. Signal Process 83:2133–2170
23. Dehghan H, Safavi S (2010). Robust image watermarking in the wavelet domain for copyright protection. ICEE Conference ArXiv: 1–4
24. Dhar J, Islam M, Ullah M (2019). A fuzzy logic based contrast and edge sensitive digital image watermarking technique. SN applied sciences: 1-9
25. Doërr G, Dugelay J (2003) A guide tour of video watermarking. In: Signal Processing: Image Communication: 263–282. https://doi.org/10.1016/S0923-5965(02)00144-3
26. Dubolia R , Singh R, Bhadoria S , Gupta R (2011). Digital Image watermarking By Using Discrete Wavelet Transform And Discrete Cosine Transform And Comparison Based On PSNR. IEEE International Conference on Communication Systems and Network Technologies:593–596
27. Mansoori G, Soltani SS (2016) A new semi-blind watermarking algorithm using ordered Hadamard transform. The Imaging Science Journal 64(4):204–214
28. Fang H, Zhou H, Ma Z, Zhang W, Yu, N (2018). A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization. Multimedia Tools and Applications:1–15
29. Fazli S, Moeini M (2015). A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik - International Journal for Light and Electron Optics:1–9
30. Garg P, Dodeja L, Dave P, Dave M (2018). Hybrid color image watermarking algorithm based on DSWT-DCT-SVD and Arnold transform. Advances in signal processing and communication springer: 327-336
31. Garg P, Kishore R (2020) Secured and multi optimized image watermarking using SVD and entropy and prearranged embedding locations in transform domain. J Discret Math Sci Cryptogr 23(1):73–82
32. Gonge S, Bakal J (2013) Robust digital watermarking techniques by using DCT and spread Spectrum. International Journal of Electrical Electronics and Data Communication 1(2):27–32
33. Gupta R, Mishra A, Jain S (2017). A semi-blind HVS based image watermarking scheme using elliptic curve cryptography. Multimedia Tools and Applications:1–26
34. Hamidi M, Haziti M, Cherifi H, EL H Mohammed (2018). Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimedia Tools and Applications: 1–34
35. Han S, Yang J, Wang R, Jia G (2018) A robust color image watermarking algorithm against rotation attacks. Optoelectron Lett 14:61–66
36. Hannoun K, Hamiche H, Lahdir M, Laghrouche M, Kassim S (2018) A novel DWT domain watermarking scheme based on a discrete-time chaotic system. IFAC-PapersOnline 51:50–55. https://doi.org/10.1016/j.ifacol.2018.12.089
37. Hazvini M, Hachrood E, Mirzadi M (2017) An improved image watermarking method in frequency domain. Journal of Applied Security Research 12(2):260–275
38. Hong W, Hang M (2006). Robust Digital Watermarking Scheme for Copy Right Protection. IEEE Trans. Signal Process l2: 1–8

39. Hsu L, Hu H (2020) Blind watermarking for color images using EMMQ based on QDFT. Expert Syst Appl 149:1–54
40. Hu H, Hsu L (2014) Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. Comput Electr Eng 41:1–12
41. Hua G, Huang J, Shi Y, Goh J, Thing V (2016) Twenty years of digital audio watermarking – a comprehensive review. Signal Process 128:222–242. https://doi.org/10.1016/j.sigpro
42. Huang S, Zhang W, Feng W, Yang H (2008). Blind Watermarking Scheme Based on Neural Network. Proceedings of the 7th World Congress on Intelligent Control and Automation China: 5985–5989
43. Hung K, Cheng T, Gwoboa H, Shiuh W (2019) Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. Inf Sci:1–33
44. Ingemar MLM, Cox J, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking and steganography. Morgan Kaufmann Publishers
45. Irshad A, Millie P, Chang A (2017). Secured and optimized robust image watermarking scheme. Arabian journal for science and engineering: 1-20
46. Islam M, Ullah M, Jitu D (2019) An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network. Karbala International Journal of Modern Science 5(1):1–11
47. Issa M (2018) Digital image watermarking performance improvement using bio-inspired algorithms. Advances in Soft Computing and Machine Learning in Image Processing, Studies in Computational Intelligence 730:683–698
48. Jagadeesh B, Kumar PR, Reddy PC (2015) Fuzzy inference system based robust digital image watermarking technique using discrete cosine transform. Procedia Computer Science 46:1618–1625
49. Jane O, Elbaşı E (2013) A new approach in non-blind watermarking method based on DWT and SVD via LU decomposition. Turk J Electr Eng Comput Sci 22:1354–1366
50. Jero E, Ramu P, Swaminathan R (2015) Imperceptibility – robustness tradeoff studies for ECG steganography using continuous ant Colony optimization. Expert Syst Appl 49:123–135
51. Jiang M (2012) A new adaptive visible watermarking algorithm for document images. Inf Technol J 11: 1322–1326
52. Chitra K, Venkatesan V (2016) Spatial domain watermarking technique: an introspective study. Proceedings of the International Conference on Informatics and Analytics ICIA-16:1–6. https://doi.org/10.1145/2980258.2980363
53. Kalra G, Talwar R, Sadawarti H (2014) Adaptive digital image watermarking for color images in frequency domain. Multimed Tools Appl 74:1–21
54. Kandi H, Mishra D, Gorthi SR (2017) Exploring the learning capabilities of convolutional neural networks for robust image watermarking. Computer & Security Elsevier Science Direct 65:247–268
55. Kang X, Fan Z, Guangfeng L, Chen Y (2017) A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength. Multimed Tools Appl:1–28
56. Kang, X, Chen Y, Fan Z, Guangfeng L (2019). Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain. Soft Computing:1–24 https://doi.org/10.1007/s00500-019-04563-6
57. Kansal M, Singh G, Kranthi B (2012). DWT, DCT and SVD based Digital Image Watermarking. IEEE International Conference on Computing Sciences:77–81
58. Kashyap, Nikita and Sinha, Professor G. (2012). Image watermarking using 3-level discrete wavelet transform (DWT). International Journal of Modern Education and Computer Science. 4. https://doi.org/10.5815/ijmecs.2012.03.07
59. Kimpan S, Lasakul A, Chitwong S (2004) Variable block size based adaptive watermarking in spatial domain. IEEE International Symposium on Communications and Information Technology ISCIT 1:374–377. https://doi.org/10.1109/ISCIT.2004.1412871
60. Kumar A, Maruturi H, Bindu H (2014) Novel image watermarking algorithm with DWT-SVD. Int J Comput Appl 106:13–17
61. Kumar D, Dontoju T, Sykam RNS (2017) An efficient watermarking technique for biometric images. 7th International Conference on Advances in Computing & Communications. ICACC, Cochin, pp 423–430
62. Kumar P, Sharma A (2019) A robust image watermarking technique using feature optimization and cascaded neural network. International journal of computer science and information security (IJCSIS) 18(8):36–45
63. Kundur D, Hatzinakos D (1998) Digital watermarking using multiresolution wavelet decomposition. International conference on acoustics. Speech, and Signal Processing 5:2969–2972
64. Mohammad LA, Zeki A, Chebil J, Gunawan T (2013) Properties of digital image watermarking. Proceedings - 2013 IEEE 9th International Colloquium on Signal Processing and its Applications. CSPA, pp 235–240. https://doi.org/10.1109/CSPA.2013.6530048

65. Li D, Deng L, Gupta BB , Wang H , Choi C (2018). A novel CNN based security guaranteed image watermarking generation scenario for Smart City applications. Information Sciences, Elsevier: 1–25
66. Li J, Zhu Y (2010) A geometric robust image watermarking scheme based on DWT-SVD and Zernike moments. IEEE, pp 367–371
67. Li N, Zheng X, Zhao Y, Wu H, Li S (2008) Robust algorithm of digital image watermarking based on discrete wavelet transform. In: International symposium on electronic commerce and security IEEE, pp 942–945
68. Liu Y, Guo M, Zhang J, Zhu Y, Xie X (2019). A novel two-stage separable deep learning framework for practical blind watermarking. MM '19 France: 1509-1517. https://doi.org/10.1145/3343031.3351025.
69. Lu H , Gong D , Liu F , Liu H, Qu J (2019). A batch copyright scheme for digital image based on deep neural network. Mathematical Bioscience & Engineering: 6121-6133
70. Luo A, Zou W (2018) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimed Tools Appl 78:1–17
71. Malik S, Kishore R (2018) Fractional Fourier transform and position shuffling based digital image watermarking scheme and its performance analysis. International Journal of Advanced Studies of Scientific Research 4(1):1–7
72. Maruturi H, Bindu H, Swamy K (2016) A Secure & Invisible Image Watermarking Scheme Based on wavelet transform in HSI color space. Procedia Computer Science 93:462–468
73. Mathur S, Dhingra A, Prabukumar M, Loganathan A, Muralibabu K (2016) An efficient spatial domain based image watermarking using shell based pixel selection. International Conference on Advances in Computing, Communications and Informatics IEEE, pp 2696–2702
74. Mehta R, Rajpal N, Vishwakarma V (2016) LWT- QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR. Multimedia Tools and Applications 75(7):4129–4150
75. Mishra A, Goel A, Singh R, Chetty G, Singh L (2012) A novel image watermarking scheme using extreme learning machine. IEEE World Congress on Computational Intelligence IJCNN:1–6. https://doi.org/10.1109/IJCNN.2012.6252363
76. Moeinaddini E (2018) Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm. Soft Comput 23:1–15
77. Moosazadeh M, Gholamhossein Ekbatanifard (2017). An improved robust image watermarking method using DCT and YCoCg-R Color Space. International Journal for Light and Electron Optics: 1–32. https://doi.org/10.1016/j.ijleo.2017.05.01
78. Mukherjee D, Maitra S, Acton S (2004) Spatial domain digital watermarking of multimedia objects for buyer authentication. IEEE Transactions on Multimedia 6:1–15. https://doi.org/10.1109/TMM.2003.819759
79. Mun S, Nam S, Jand H, Kim D, Lee H (2019) Finding robust domain from attacks: a learning framework for blind watermarking. Neurocomputing Elsevier 337:191–202
80. Mun S, Nam S, Jang H, Kim D, Lee H (2017). A robust blind watermarking using convolutional neural network: 1–5
81. Nasr A, Ahmed S, Roslizah A,Wan A, Wan A, Rahman (2016). A state-of-the-art in techniques of text digital watermarking: challenges and limitations. J. Comput. Sci.: 62–80
82. Nematollahi, Ali M, Vorakulpipat, Chalee, Rosales, Gamboa H (2017). Digital watermarking techniques and trends. Springer Singapore. https://doi.org/10.1007/978-981-10-2095-7
83. Nikolaidis A, Pitas I (2001). Region-based image watermarking. IEEE transactions on image processing. A publication of the IEEE Signal Processing Society: 1726–1740
84. Nurul K, Kamsin A, Yee P, Hameedur R (2018) A review of text watermarking: theory. Methods and Applications IEEE Access 6:1–20. https://doi.org/10.1109/ACCESS.2018.2796585
85. Parah S, Sheikh J, Loan N, Bhat G (2016). Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digital signal Process Elsevier: 1–25
86. Patel S, Mehta T, Pradhan S (2011) A unified technique for robust digital watermarking of colour images using data mining and DCT. Int J of Internet Technology and Secured Transactions 3:81–96
87. Pereira S, Pun T (2000) Robust template matching for affine resistant image watermarks. IEEE Trans Image Process 9(6):1123–1129
88. Perwej Y, Parwej F, Perwej A (2012) An adaptive watermarking technique for the copyright of digital images and digital image protection. International Journal of Multimedia & Its Applications 4(2):21–38. https://doi.org/10.5121/ijma.2012.4202
89. Phade R et al (2013) Digital image watermarking using DCT and ZIP compression technique. Global Journal of Computer Science and Technology Graphics & Vision 13(3):1–5
90. Pitas I (1998) Robust image watermarking in spatial domain. Signal Process 66:385–403. https://doi.org/10.1016/S0165-1684(98)00017-6

91. Poljicak A, MandićL AD (2011) Discrete Fourier transform-based watermarking method with an optimal implementation radius. Journal of Electronic Imaging - J ELECTRON IMAGING 20:1–9
92. Pradhan C, Saxena V, Bisoi A (2012). Non blind digital watermarking technique using DCT and cross chaos map. International conference on Communications, Devices and Intelligent Systems (CODIS) IEEE: 274–277
93. Priya S, Santhi B, Swaminathan P, Raja Mohan J (2017). Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. Optik - international journal for light and Electron optics: 1–36
94. Purwar R, Jain A (2017) An evolutionary algorithm based multiscale digital image watermarking technique using discrete wavelet transform and singular value decomposition. International Journal of Tomography and Simulation 30:53–62
95. Qingtang Su (2017). Color Image watermarking Algorithms and Technologies. Berlin ; Boston : De Gruyter ; [Beijing] : Tsinghua University Press
96. Rafigh M, Ebrahimi M (2010). A robust evolutionary based digital image watermarking technique in DCT domain. Seventh International Conference on Computer Graphics, Imaging and Visualization IEE Xplore: 105–109.
97. Saikrishna N, Resmipriya MG (2016) An invisible logo watermarking using Arnold transform. Procedia Computer Science 93:808–815
98. Savakar D, Ghuli A (2017) Non-blind digital watermarking with enhanced image embedding capacity using DMeyer wavelet decomposition, SVD, and DFT. Pattern Recognition and Image Analysis 27:511–517
99. Savakar D, Ghuli A (2019) Robust invisible digital image watermarking using hybrid scheme. Arab J Sci Eng 44:1–14
100. Selesnick I, Baraniuk R, Kingsbury N (2005) The dual-tree complex wavelet transform. IEEE Signal Process Mag 22(6):123–151
101. Selvi C, Sudhakar RB, Priyadharshini G (2016). DWT based watermarking approach for medical image authentication:1–5. https://doi.org/10.1109/ISCO.2016.7726895
102. Senapati R (2017) Robust image embedded watermarking using DCT and listless SPIHT. Future Internet 9:1–16
103. Sharma H, Sharma J (2019) An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. Appl Soft Comput 84:1–18
104. Sharma V, NaazMir R (2019). An enhanced time efficient technique for image watermarking using ant colony optimization and light gradient boosting algorithm. Journal of King Saud University - computer and information sciences science direct: 1-12
105. Shih F (2017) Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis Group CRC Press
106. Singh A (2015). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimedia tools application springer: 1-18
107. Singh A, Dave M, Mohan A (2014). Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools Application Springer: 1–21
108. Singh A, Sharma N, Dave M, Mohan A (2012). A novel technique for digital image watermarking in spatial domain. Proceedings of 2012 2nd IEEE international conference on parallel, Distributed and Grid Computing, PDGC: 497–501
109. Singh AK (2019). Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. Multimedia Tools Application, Springer: 1–11.
110. Singh D, Singh SK (2017) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection [J]. Multimed Tools Appl 76(11):13001–13024
111. Singh R, Shaw D, Jha S, Kumar M (2017) A DWT-SVD based multiple watermarking scheme for image based data security. J Inf Optim Sci 39:1–16
112. Specht D (1991) A general regression neural network. IEEE transactions on neural networks / a publication of the IEEE Neural Networks Council 2:568–576
113. Su Q, Chen B (2017) Robust color image watermarking technique in the spatial domain. Soft Comput 1–16:22–106. https://doi.org/10.1007/s00500-017-2489-7
114. Sun L, Xu J, Liu S, Zhang S, Li Y, Shen C (2017) A robust image watermarking scheme using Arnold transform and BP neural network. Neural Comput & Applic:1–16
115. Tech M, Saxena A (2017) Image watermarking using discrete cosine transform [DCT] and genetic algorithm [Ga]. International Journal of Innovation In Engineering Research & Management 4(3):1–13
116. Thajeel S (2018). A new color image watermarking technique using multiple decompositions. J Theor Appl Inf Technol: 2324–2327

117. Thakkar F, Srivastava V (2016) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76:1–29
118. Thien H, Oresti B, Sungyoung L, Yongik Y, Thuong T (2016) Improving digital image watermarking by means of Optimal Channel selection. Expert Syst Appl:1–36
119. Tiwari A, Sharma M, Tamrakar R (2017). Watermarking based image authentication and tamper detection algorithm using vector quantization approach. AEU-Int J Electron C: 114–123
120. Tsui T, Zhang X, Androutsos D (2008) Color image watermarking using multidimensional Fourier transforms. IEEE Transactions on Information Forensics and Security 3:16–28
121. Vali M, Aghagolzadeh A,Baleghi Y (2018). Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. Expert Systems with Applications:1–43
122. Verma V, Srivastava V, Thakkar F (2016). DWT-SVD based digital image watermarking using swarm intelligence. International Conference on Electrical, Electronics, and Optimization Techniques IEEE: 3198–3203
123. Vishwakarma V, Sisaudia V (2018) Gray-scale image watermarking based on DE-KELM in DCT domain. Procedia Computer Science 132:1012–1020
124. Wang J, Du Z (2019) A method of processing color image watermarking based on the Haar wavelet. J Vis Commun Image R 64:102627–102634
125. Wang X, Wang C, Yang H, Niu P (2013) A robust blind color image watermarking in quaternion Fourier transform domain. J Syst Softw 86:255–277
126. Xu H, Kang X, Wang Y, Wang Y (2018) Exploring robust and blind watermarking approach of colour images in DWT-DCT-SVD domain for copyright protection. Inderscience Int. J Electronic Security and Digital Forensics 10(1):79–96
127. Zear A, Singh A (2017) Robust watermarking technique using back propagation neural network: a security protection mechanism for social applications. Int J Inf Comput Secur 9:20–35
128. Zear A, Singh A, Pardeep Kumar, (2016). A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools Application. https://doi.org/10.1007/s11042-016-3862-8
129. Zheng W , et al (2018) Robust and High Capacity Watermarking for Image Based on DWT-SVD and CNN. 13th IEEE Conference on Industrial Electronics and Applications (ICIEA). Wuhan, p 1233–1237

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.