Digital Watermarking: A Potential Solution for Multimedia Authentication

Kaiser J. Giri and Rumaan Bashir

Abstract The digitization has resulted in knowledge explosion in the modern technology-driven world and has led to the encouragement and motivation for digitization of the intellectual artifact. The combining, replication, and distribution facility of the digital media such as text, images, audio, and video easier and faster has no doubt revolutionized the world. However, the unauthorized use and maldistribution of information by online pirates is the sole threat that refrains the information proprietors to share their digital property. It is therefore imperative to come up with standard means to protect the intellectual property rights (IRP) of the multimedia data, thereby developing the effective multimedia authentication techniques to discourage the illegitimate distribution of information content. Digital watermarking, which is believed to be the potential means among the various possible approaches, to encourage the content providers to secure their digital property while maintaining its availability, has been entreated as a potential mechanism to protect IRP of multimedia contents.

Keywords Multimedia authentication · Digital watermarking · Copyright protection · Intellectual property rights · Discrete wavelet transformation

1 Introduction

The realm of computer science and information technology has revolutionized the entire world. In particular, computer science is the scientific and practical approach to computation and information technology is the application of computers, the ever-evolving fields in human history. Both of these aspire on giving vast solutions

K.J. Giri (✉) · R. Bashir
Department of Computer Science, Islamic University of Science and Technology,
Awantipora, Pulwama, J&K 192122, India
e-mail: kaiser.giri@islamicuniversity.edu.in

R. Bashir
e-mail: rumaan.bashir@islamicuniversity.edu.in

N. Dey and V. Santhi (eds.), *Intelligent Techniques in Signal Processing for Multimedia Security*, Studies in Computational Intelligence 660,
DOI 10.1007/978-3-319-44790-2_5

to day-to-day problems with the focus to save time and effort. These have become an integral part of our lives, shaping virtually everything from the way we live to the way we work. The exponential growth in these high-speed computer networks and World Wide Web has converged the whole world into a very small place and have explored means of new scientific, economic, business, entertainment, and societal opportunities in the shape of data sharing, collaboration among computers, instant information delivery, electronic distribution and advertising, business transaction processing, product ordering, digital libraries and repositories, network video and audio, individual communication, and a lot more.

The panorama of economic feasibility together with recent advances in computing and communication technology has revolutionized the world. The cost-effectiveness of vending software by communication over World Wide Web in the form of digital images and video clips is significantly enhanced due to the advancement in technology. Of many technological advances, the digital media invasion in nearly every aspect of routine life was one of the biggest technological accomplishments. Digital media has several advantages over its analog counterpart. The key attribute of digital data is that it can be stored efficiently with very high quality, manipulated easily using computers by accessing its discrete locations, communicated in a fast and economical way through networks without losing quality [1]. Editing is simple because of access to the exact discrete locations that are required to be modified. The copying of digital data is easy without loss of reliability. The digital media duplicate is identical to the original; pursuant to which, a serious concern has emerged due to which proprietors refrain to share digital content in view of threats posed by the online pirates and to maintain intellectual property rights.

Consequently, as an interesting challenge, digital information protection schemes, multimedia authentication in the form of information security, have gained so much of attention. Since copyright enforcement and content verification are challenging issues for digital data, one solution would be to restrict access to the data by using encryption tools and techniques. However, encryption does not provide overall protection of the whole data as it can be freely distributed or manipulated once the encrypted data is decrypted. Unauthorized use of data creates several problems. The subject of multimedia authentication is becoming more and more important. The prevention of any illegal duplication to the data is of more concern to copyright owners [2]. Therefore, concrete measures are required in order to maintain the availability of multimedia information but, in the meantime, standard procedures/methods must be designed to protect intellectual property of creators, distributors, or owners. This is an interesting challenge and has led to the development of various multimedia authentication schemes over the past few decades.

Of the many possible approaches to protect visual data, digital watermarking is probably the one that has received most interest. Digital watermarking is the process of embedding information into a noise-tolerant digital signal such as image or audio data [3]. Information is embedded in such a manner that it is difficult to be removed due to which the relevant information is not easily identified, thus serving different purposes such as copyright ownership of the media, source tracking, and piracy deterrence.

2 Digital Watermarking

The concept of hiding or concealing some additional information (watermark) in the host data such as images, audio, video, text, or combination of these to establish the ownership rights is known as watermarking [4]. In digital watermarking, an invisible signal (message) generally known as watermark is embedded into digital media (host) such as in text, image, audio, or video. The watermark embedding is further integrating in an inseparable form from the host digital content [2]. While embedding the watermark information into the host media, the imperceptibility and robustness properties have to be taken into consideration so that the quality of watermarked data may not degrade and can replace the original unwatermarked data for all practical purposes. Besides, the embedding process has to be carried in such a manner so that the watermark data remains inseparable from watermarked data and can even be extracted later to make an assertion of the digital data. The authentication and copyright protection of the digital content are the two prime objective of the watermarking. Watermark embedding/extraction is primarily carried either in spatial domain or in frequency (transform) domain. In spatial domain, the host data pixels under consideration are directly modified with respect to the watermark pixels, whereas in transform domain, some reversible transformation is initially applied to host data and the resulting transformed coefficients are then modified with watermark pixels. Digital watermarking offers two principle advantages for authentication: firstly, the watermark is integrated as an inherent part of the host image avoiding the appended signature of cryptology, and secondly, the watermark will experience the similar transformations as that of the data due to the fact that it is concealed within the data [5, 6]. These transformations can be undone by observing the transformed watermark.

A generic watermarking model is presented in Fig. 1.

The idea of watermarking can be dated back to the Late Middle Ages. The earliest use has been to record the manufacturer trademark on the products so that authenticity could be easily established. The term “digital watermark” was first coined in 1992 by Andrew Tirkel and Charles Osborne. Actually, the term used by Andrew Tirkel and Charles Osborne was originally used in Japan—from the Japanese—“denshisukashi”—literally, an “electronic watermark” [7, 8]. The idea of watermarking has been used for several centuries, in the form of watermarks found initially on plain paper. However, the field of digital watermarking flourished during the last two decades, and it is now being used for many different applications. Therefore, a digital watermark is a message that is embedded in the digital media (audio, video, text, or image) which needs to be extracted later. These embedded messages carry the ownership information of the content. The procedure

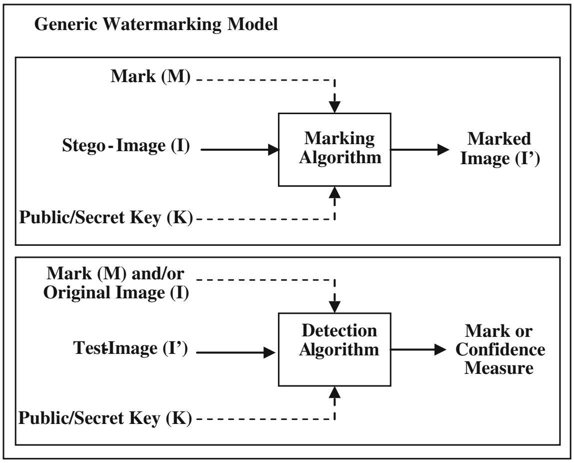

Fig. 1 Generic watermarking model

of embedding copyright information in the form of a digital watermark into digital media is called digital watermarking.

The idea of watermarking and steganography are closely related to each other in the sense that both of them hide a message inside the digital media. However, the difference lies in their objectives. In case of watermarking, the message that is embedded is related to the actual content of the digital signal, whereas in steganography the message being concealed has no relation to the digital signal. The technique of steganography embeds data inside a signal, either host or cover, in an unnoticeable manner. Various types of digital data that can be used as a cover medium for information hiding include text, images, audio, and video. The invisible inks that one could make use of to send a secret message to others was one of the simplest and oldest ways of steganography. Numerous types of invisible inks were available to conceal the messages such as lemon juice, onion juice, milk, and urine to name a few. For hiding a message, one would write it using these inks on a sheet of paper. Since the ink is invisible, nothing would appear on the paper. On reception, this paper was placed over flame in order to recover the message.

For securing the transmission of data, a technique known as cryptography, which converts information into an unintelligible form, is often used. Here a "key" is used for performing encryption, which disguises the original data. On reception, the encrypted message is decoded to retrieve the original message with the help of either same or different key. Hence, the objective of cryptography is to protect the contents of the message. However, once the data is decrypted, it is available to the intruder. Therefore, cryptography is a scrambling message so that it is not comprehensible to the unapproved user whereas in watermarking, neither the cover medium nor the copyright data is converted to an unintelligible form. Instead, the copyright data is concealed in order to provide the ownership information of the signal in which it is hidden.

Digital signatures are similar to written signatures and are mainly used to provide message authentication. It is an electronic signature which can authenticate the identity of the sender/signatory of a message during its transmission. They are transportable, non-imitable, and automatically time-stamped. It possesses the property of non-repudiation, which ensures that the original signed message has arrived. A digital signature is separately placed in the protected message and is vulnerable to distortions, whereas a digital watermark lies within the protected message and has to tolerate a certain level of distortion. Watermarking and digital signature both protect integrity and authenticity of a message.

Therefore, digital watermarking is the addition of "ownership" information in a signal in order to prove its authenticity [9]. This technique embeds data, an unperceivable digital value, the watermark, carrying information about the copyrights of the message being protected. Constant efforts are being made to devise effective and efficient watermarking techniques which are robust enough to all potential attacks [10]. An attacker tries to remove the watermark in order to violate copyrights. An attacker can cast the same watermark in the message after altering it in order to forge the proof of authenticity.

3 Characteristics of Watermarking

Watermarking provides an assortment of vast solutions to a variety of data. The technique of watermarking should possess a set of properties which make it a potential solution [2, 9–11]. An effective watermarking system should exhibit the following characteristics:

1. Imperceptibility
   The imperceptibility property signifies that the host medium should be minimally altered, once the watermark data is embedded within it. The cover medium being protected should not be affected by the presence of the watermark data. If a watermarking system does not uphold this property, post-insertion of a watermark data in a cover medium, the image quality may get reduced.
2. Robustness
   The robustness property of the watermark data indicates that the watermark data should not be destroyed if common operations and malicious attacks are performed on the message. Robustness is a primary requirement of watermarking, but it depends upon the application areas under consideration.
3. Fragility
   The fragility property indicates that the copyright data is altered or modified within a certain limit when on applying common manipulations and malicious attacks on the host media. Application areas such as tamper detection require a fragile watermark in order to detect any tampering with the host media. Other applications may require semi-fragility which indicates that the embedded watermark comprises of a fragile as well as robust components.

4. Resilient to Common Signal Processing
   The resilience property implies that the watermark should be retrievable even when common signal processing manipulations such as analog-to-digital and digital-to-analog, image contrast, brightness and color adjustment, conversion, audio bass and treble adjustment, high-pass and low-pass filtering, histogram equalization, format conversion, dithering and recompression, resampling, and requantization are applied to the host media.
5. Resilient to Common Geometric Distortions
   The watermarking scheme except for audio watermarking should embed watermarks which are resilient to geometric image operations. These operations include translation, rotation, cropping, and scaling.
6. Robust to Subterfuge Attacks (Collusion and Forgery)
   The watermark embedded should be robust to collusion attack which implies that multiple individuals possessing a copy of the watermarked data may destroy the watermark presence by colluding the watermark copies in order to create the duplicate of the original copy.
7. Unambiguousness
   After retrieving the watermark, the identity of the owner should be unambiguously identifiable. In addition, if the watermarked data is subjected to some attack, the owner identification should not degrade beyond an established threshold.

4 Digital Watermarks Techniques

Watermarking techniques can be classified on various parameters in view of the variety of digital media types and application requirements [2, 9] as shown in Fig. 2.

1. Embedding/Extraction Domain
   There are two types of watermarking schemes depending upon the embedding/extraction domain:

   - Spatial Domain-based Watermarking Schemes: The watermarking is carried out by directly modifying the host data pixels according to the watermark pixels. Number of schemes haven been developed by researches over the period of time in the spatial domain.
   - Transform Domain-based Watermarking Schemes: The watermarking embedding/extraction is performed by applying some reversible transformation to the host data and modifying transform domain coefficients with watermark data. The watermark data is later obtained by applying the inverse transformation. The transform-domain-based watermarking systems are more robust as compared to spatial domain watermarking systems. They are robust against simple image processing operations such as low-pass filtering,

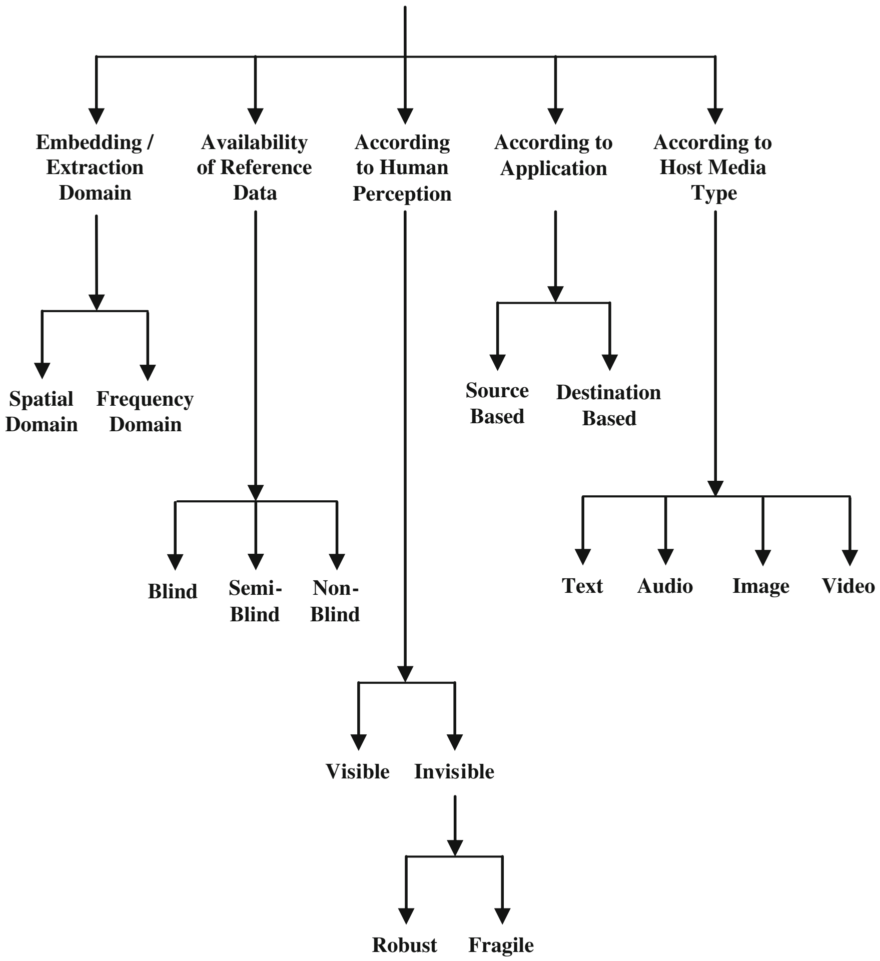

Fig. 2 Watermarking techniques

brightness and contrast adjustment, and blurring. However, they are difficult to implement and computationally more expensive. We can use either discrete cosine transform (DCT), discrete Fourier transform (DFT), or discrete wavelet transform (DWT) [12–15]; however, DCT is the most exploited one.

2. Availability of Reference Data
   As per the availability of reference data, the watermarking techniques can be of three types as follows:

   - Blind: The original unwatermarked data is not required for extraction of watermark [16–20]. Blind watermarking scheme is also known as public watermarking scheme. This is the most challenging type of watermarking system as it requires neither the cover (original) data, I, nor the embedded watermark, W. These systems extract n bits of the watermark data from the watermarked data (i.e., the watermarking image) and using key K recover/reconstruct the watermark. I × K → W, where K is the key.

- Non-Blind: The original unwatermarked data is required for extraction of watermark [21]. This scheme is also known as private watermarking scheme. This system requires at least the cover (original data) for detection.
- Semi-Blind: Some features derived from original unwatermarked data are required for extraction of watermark [22]. This scheme is also known as semi-private watermarking scheme. This system does not require the cover (original image) for detection.

3. According to Human Perception
   According to human perception, watermarking can be of the following two types:

   - Visible: The embedded watermark inlaid in the host data is transparent [23]. Visible watermarks can be seen by the user; logo and the owner details are identified by person. These technique changes the original signal.
   - Invisible: The embedded watermark inlaid in the host data is hidden and can be extracted only by an authorized user. Invisible watermarks cannot be seen by other party, and output signal does not change when compared to the original signal.

     – Fragile: The embedded watermark is destroyable by any kind of modification to the host data [24]. These techniques are more sensitive than other and can be easily destroyed with small modification.
     – Robust: The embedded watermark is resilient to image processing attacks. These methods are used for copyright protection because this type of watermark cannot be broken easily.

4. According to Application
   From application point of view, the watermark can be of two types, i.e. source based or destination based.

   - Source Based: To detect the host data tampering, source-based watermarks are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with.
   - Destination Based: To embed the watermark for copyright protection, the watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination-based watermark could be used to trace the buyer in the case of illegal reselling.

5. According to Host Media
   According to the host media, the watermarking can be of four types:
   - Text Watermarking: Most of the paper documents such as those from digital libraries, banks, journals, books contain more valuable information than other types of multimedia. In order to trace illegally copied, altered, forged, or distributed text documents, watermarking is being used as a tool to provide copyright information. Documents on which text watermarking can be applied have to be properly formatted unlike the text in raw form like source code. Unformatted text cannot be watermarked because of lack of "perceptual headroom" for the watermark to be placed.
   - Image Watermarking: As there are multiple sources of digital images such as photographs, medical scans, satellite images, or computer-generated images, watermarking is therefore one of the commonly used watermarking schemes. Watermarks for images usually modify pixel values or transform coefficients. However, other features like edges or textures could also be modified to include the watermark. An image may be subjected to certain geometric transformations such as filtering, cropping, compression, and other hostile attacks; therefore, imperceptibility and robustness properties are usually the most desirous properties in case of image watermarking. In context of image compression such as JPEG, watermarking in the transform or wavelet domain is usually exploited.
   - Video Watermarking: Video watermarking is the application of watermarking, wherein the sequence of moving still images are watermarked; hence, various image watermarking techniques have been used for the digital video [25, 26]. Contrary to simple images, digital video requires large bandwidth which implies that larger messages can be embedded within the video. As digital video is mostly stored and distributed in compressed form like MPEG, therefore, it is required that the watermarked video should not take more bandwidth as compared to its counterpart.
   - Audio Watermarking: In case of audio files, digital audio watermarking is used to protect them from illegal copying. Keeping in view the ease with which the audio files can be downloaded and copied, audio watermarking is becoming necessary. Audio watermarks embedded into the digital audio are special signals. Audio watermarking techniques exploit the imperfection of the human auditory system. These techniques are difficult to design because of the inherent abilities of the complex human auditory system. Thus, good audio watermarking schemes are difficult to design.
6. Spatial Versus Transform Domain
   Watermarking operations are mainly performed in either spatial domain or in the transform domain [9, 27]. In order to achieve improved performance in terms of robustness and perceptual transparency, a thorough understanding of the embedding/extraction domain is essential. Accordingly, a comparative analysis in terms of the computational cost, time, resources, complexity, robustness, capacity, and quality is given in Table 1.

Table 1 Comparative analysis of spatial domain and transform domain

S. No.	Factors	Spatial domain	Transform domain
1.	Technique	Simple technique to use by modifying pixel values	Complex to use by modifying transform coefficients
2.	Computation cost	Computation cost involved is low	Computation cost involved is high
3.	Robustness	Fragile, less robust, incompetent in dealing with various attacks	More robust against various attacks
4.	Perceptual quality	High control	Low control
5.	Computational complexity	Low	High
6.	Computational time	Less	More
7.	Capacity	Limited capacity to hold the watermark	High capacity to hold the watermark
8.	Example of application	Mainly authentication	Copy rights

5 Applications of Digital Watermarking

The field of watermarking has witnessed a great deal of research over the last few decades [9]. Due to the important applications of watermarking for copyright protection and management, the research is increasing day by day. A watermark can be applied for a variety of purposes. The following are a few noted applications of watermarking:

1. Copyright Protection
   Watermarking is chiefly used in an organization in order to assert its "ownership" of copyright with regards to the digital items [10, 28]. This watermarking application is the main focus of institutions which are vending objects of digital information (news/photograph) and to "big media" organizations. Here, a tiny amount of data (watermark) needs to be embedded which requires a high level of resistance to signal alteration. When digital data is broadcasted, it demands strong watermarking as any intruder can use it without paying the IPR charges to its owner.
2. Copy Protection
   In order to prevent illegal copying of digital data, watermarking is used as a highly potential tool. A system or software trying to copy an audio compact disc cannot do so if a watermark has been embedded in it. Additionally, if copying is done still the watermark will not get copied to the new duplicate compact disc. Hence, the replica compact disc can be recognized easily due to the absence of the watermark. Digital recording devices can be controlled by

the information stored in a watermark for copy protection purpose [29]. Here, the watermark detectors in the recording device decide whether the recording can take place or not. This is made possible by the presence of a copy-prohibited watermark which in the simplest form is a single bit that indicates whether the content is copyrighted or not. This copy protection bit cannot be removed easily as it is strongly tied to the content and when removed the digital content would get seriously affected.

3. Tamper Detection
   Tamper detection is used to ascertain the origin of a data object and to prove its integrity [30]. The classical example of tamper detection is presentation of photographic forensic information as evidence in the legal matters. Since digital media can be manipulated with great ease, there may be an obligation to prove the fact that a media (image/video) has not been altered. In such cases, a camera can be equipped with the capability for tamper detection, by a watermarking system which is embedded in digital cameras [31]. Here as an example, while proving charges of an over speeding driver in a legal court, the driver may claim that the video taken by the police department is tampered. Such a watermark would get destroyed when one would try to tamper the data.
4. Broadcast Monitoring
   A need to monitor the broadcasts of certain individual and institutions for their interests is an important application of watermarking. Here as an example, the exact airtimes purchased from the broadcasting firms received by the advertisers who want to advertise can be ensured. Similarly, celebrities like actors want to calculate their accurate royalty payments of their performances when broadcasted. In addition, the copyright owners do not want that their digital properties illegally rebroadcasted by pirate stations. Such incidents have been seen all over the globe. In Japan, advertisers were paying hefty amounts for commercials that were never broadcasted [32]. The said case had been undetected for nearly 20 years as there was no system to monitor the real broadcast of advertisements. This broadcast can be monitored by using a unique watermark in each video signal or audio clip prior to the broadcast. The broadcasts can be monitored by automated stations to check for the unique watermarks.
5. Fingerprinting
   If the same watermark is placed in all the copies of a single item, it might be a problem for monitoring and owner identification. If one of the legal users of the common digital item sells it illegally, it would be difficult to identify the culprit. Therefore, each copy of the digital data distributed is customized for each legal user. This method embeds a unique watermark to each individual copy. The owner can easily identify the user who is illegally vending the digital media by checking the watermarks. This application of watermarking is called fingerprinting [2]. The fingerprinting serves two purposes: It acts as prevention to illegal use and as an aid to technical investigation.

6. Annotation Applications
   Here, the watermarks express the information specific to the digital item such as "feature tags" or "captions" or "titles" to users of the item. As an example, identification of the patient can be embedded into medical media-like images. There exists no need to protect such digital items against intentional tampering. They require comparatively large quantities of embedded data. Such digital items might be susceptible to transformations such as image cropping or scaling; therefore, the watermarking technique resistant to those types of modifications must be employed.
7. Image Authentication and Data Integrity
   Image authentication is another application of watermarking. As an example, the authenticity of images/photographs used for surveillance in the military must be established. Digital images are exploited by image processing packages using seamless modifications. Digital images produced before courts as evidences may be modified or altered beforehand. Watermarking can enable the user to detect the imperative modifications of the images under consideration. The watermarks used for such verification purposes need to be fragile so that any alteration to the original image will obliterate or noticeably alter the watermark [33]. Fragile watermarks indicate whether the data has been changed. Further, they also provide information as to where the data was changed.
8. Indexing and Image Labeling
   Comments and markers can be embedded in the video content for the purpose of indexing of video mail, news items, and movies that can be used by search engines. This feature is usually used by the digital video disc recordings in order to let the user select certain scenes or episodes without rewinding or forwarding which is otherwise necessary with a video cassette recording (VCR). When the information about the image content is embedded as a watermark, the application is called as image labeling. Such embedding methods are required for proving extra information to the viewer or for image retrieval from a database.
9. Medical Safety
   A safety measure similar to fingerprinting could be used to embed the date and the name of the patient in medical images or a music recording with the owner/user information [34]. This application is becoming more important in view of tele-medicine. The watermarks could be used to authenticate the claims made by various bodies regarding the serious health condition of an important personality.
10. Data Hiding
    The transmission of secret private messages can exploit watermarking techniques. Using tools such as invisible ink, microscopic writing, or hiding code words within sentences of a message, data hiding or steganography is a method of hiding the existence of a message [35]. Here, the communication using often enciphered messages without attracting the attention of a third party is performed. Here, the important and mandatory properties of the watermark are the

invisibility and capacity while robustness requirement is low for steganography. Users may hide their messages due to the fact that various governments are restricting the use of encryption services, in other data.

6 Recent Advances: Wavelet Domain Image Watermarking

Watermarking techniques are usually applied either in the spatial domain or in the transform domain. Spatial domain techniques directly modify the pixels of an image or a subset of them with respect to the watermark pixels values. These methods when subjected to normal media operations are not more reliable. In the transform domain techniques, the image is subject to some kind of reversible transformation [36–39] such as discrete fourier transformation (DFT), discrete cosine transformation (DCT), discrete wavelet transformation (DWT) [13, 15] and then the watermarking is being carried on transform coefficients. Transform domain techniques provide higher image perceptibility and are more robust against various image processing attacks. However, the time/frequency decomposition characteristics of DWT which are very similar to human visual system (HVS) have made them more suitable for watermarking. Earlier, the work carried out in the field of watermarking was mainly focused on monochrome and grayscale media; however, due to widespread use of multimedia applications and keeping in view the fact that most of the organizations and business concerns nowadays mainly use color data especially images (labels, logs, etc.), the need for design and development watermarking schemes for color images has accordingly increased.

Discrete wavelet transformation (DWT) [40] is more appropriate for performing watermarking in transform domain, for it hierarchically decomposes an image [41]. The application of wavelet transform is more suitable so far as the processing of non-stationary signals is concerned. The whole concept of wavelet transform is based on small waves of limited duration called as wavelets having the property of multiresolution analysis [42]. Dissimilar to that of the conventional Fourier transform, the wavelet transform provides a multiresolution description of an image both in spatial as well as in frequency domain and further retains the temporal information also. The high- and low-frequency components are separated from a signal using DWT. The high-frequency components mainly contain the information related to edges, whereas the low-frequency components related to sharp details are further split into low- and high-frequency parts. The high-frequency components are mostly used for watermark embedding/extraction for they are less sensitive toward human visual system (HVS) in comparison with their low-frequency counterparts. The low-frequency components, however, are more robust to image distortions that have low-pass characteristics. These distortions include lossy compression, filtering, and geometric manipulations. So far as gamma correction, contrast/brightness adjustment, and cropping are concerned, low frequencies are

Table 2 Comparative analysis of important digital watermarking methods

S. No.	Algorithm	Advantages	Disadvantages
1.	LSB	It is easy to implement and understand. Image quality is not highly degraded and it possesses high perceptual transparency	It lacks basic robustness and is vulnerable to noise, scaling, and cropping
2.	Correlation	Gain factor can be increased which results in improved robustness	Very high increase in gain factor causes the image quality to deteriorate
3.	Patchwork	It displays high level of robustness against various attacks	It can conceal a diminutive amount of information
4.	Texture mapping	It conceals data within the continuous random texture patterns of a picture	It is only suitable for those areas with large number of arbitrary texture images
5.	DCT	The watermark is embedded into the coefficients of the center frequency, so the visibility of image is not affected. The watermark will not be removed by any kind of attack	Blockwise DCT destroys the invariance properties of the system. Some higher frequency components tend to be suppressed while quantizing
6.	DFT	It is rotation, scaling, and translation invariant therefore can recover from geometric distortions	It has complex implementation. The cost of computing may be higher
7.	DWT	It allows superior localization both in time and spatial frequency domain. It provides higher compression ratio which is pertinent to human perception	Cost of computing is somewhat higher. Time required for compression is more. Noise is present near edges of images or video frames

less robust. The watermark data inserted into middle- and high-frequency components on the other hand is typically less robust to lossy compression, low-pass filtering, and small geometric deformations of the image. The wavelet-based watermarking algorithms and schemes presented so far have been implemented using different wavelet filter banks and by using different decomposition levels. The type of wavelet to be used mainly depends on two important parameters, i.e. symmetry and perfect reconstruction. It has been observed that the appropriate selection of embedding subspace, wavelet filter bank, and decomposition level have sound bearing as far as the robustness and transparency properties are concerned.

A comparative analysis of some of the important digital watermarking methods in spatial domain as well as in transform domain is provided in the following table. From the table, it is evident that spatial domain techniques though simple in implementation are not so resistant to noise and other image processing attacks as compared to the transform domain counterparts (Table 2).

From the available literature, it has been observed that the work done by various researchers over the period of time for watermarking color images using discrete wavelet transformation has been carried in the following directions:

1. Types of Wavelet Filters and Level of Decomposition: Symmetry and perfect reconstruction are two important aspects to decide the type of wavelet being used. As the human visual system is less sensitive to symmetry, the wavelet used should be symmetric. Moreover, to preserve the image quality and imperceptibility, the decomposed image should be perfectly reconstructed. The different types of wavelet filters that have been used for watermarking are Haar wavelet, Daubechies wavelet, bi-orthogonal wavelets, complex wavelets, wavelet packets, balanced multiwavelets, stationary wavelets, morphological wavelets, non-tensor wavelets, and Berkeley wavelets.
2. Color Space Used: In the pervasive multimedia applications, color images are considered to be the basic and pivotal component of all the multimedia systems. The visual perception of these color images has a significant impact even if very small color changes are made. The representing models that can be used as candidates for color image watermarking are RGB, HSV, HSL, CMYK, CIE Lab, and CIE XYZ. RGB images to any other color spaces and then processing these images give good results.
3. Optimization Techniques Used: Optimizations being one of the important parameters to improve the efficiency and effectiveness of any algorithm, wavelet-based watermarking algorithms for color images have been optimized using number of techniques [43–45] such as singular value decomposition (SVD) [46], ant colony optimization (ACO), independent component analysis (ICA), differential evolution (DE), support vector machine (SVM), genetic algorithm (GA), fuzzy logic, cat swarm optimization (CSO), particle swarm optimization (PSO) [47], firefly algorithm (FA), bees algorithm (BA), and cuckoo search (CS).

7 Watermarking Attacks

The most common watermarking attacks [48–50] reported in the literature can be categorized into following four classes:

1. Removal Attacks:

   These attacks are being performed to completely remove the ownership information embedded as watermark data from the watermarked data without compromising on the security of the watermarking scheme under consideration. Some of the attacks included in this category are quantization, denoising, collusion, and remodulation. Though none of these methods significantly damage the watermark information; however, some of the methods come very close to complete removal of watermark information. In order to recover the embedded watermark as realistically as possible, while maintaining the quality of data being attacked, some sophisticated removal attacks go for optimization of operations such as quantization or denoising.

2. Geometric Attacks:
   These attacks intend to change watermark detector synchronization with the embedded watermark information instead of removing the embedded watermark itself [51]. On regaining the perfect synchronization, the embedded watermark information could be recovered by the detector. The amount of complexity involved in the required synchronization process, however, might be too high to be practical. In case of image watermarking, most of the commonly known benchmarking tools normally integrate a variety of geometric attacks. However, by using special synchronization techniques most of the recent watermarking methods withstand against these attacks.
3. Cryptographic Attacks:
   These attacks are intended to crack the security of the watermarking schemes being used and thus finding a way to either remove the embedded watermark information or to embed misleading watermark information. The techniques included in this category are oracle attack, where a non-watermarked signal is being created once watermark detector device becomes available and brute-force search for the embedded secret information. However, the computational complexity involved restricts the application of these attacks.
4. Protocol Attacks:
   These attacks are being performed with the objective of attacking the concept of the watermarking application as a whole. The concept of invertible watermarks forms the basis of one of the attacks in this category, wherein the attacker claims to be the owner of watermarked data after subtracting his own watermark information from the watermarked data. The idea behind this type of attack is to create ambiguity so far as the true owner of the data is concerned. Another form of protocol attack is the copy attack, wherein the objective is neither to destroy the watermark nor to impair its detection; instead, the watermark data is copied to some other data known as target data. This is usually done after analyzing the watermarked data and estimating the presence of watermark in it. To satisfy the imperceptibility property, the adoption of estimated watermark to the local features of the target data is considered (Fig. 3).

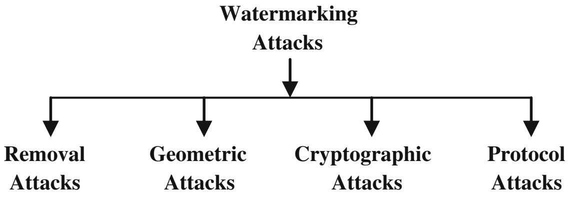

Fig. 3 Watermarking attacks

It has been observed that despite of having a clear separation between different attacks as presented in the above classification, an attacker most often applies these attacks in combination instead of using a particular attack in isolation.

8 Future Scope

The extensive creation and dissemination of multimedia content have attracted researchers from computer science and other allied fields to work in the area of digital watermarking to ensure the genuineness of the multimedia content, besides protection of the owner copyrights. Accordingly, lot of research work has been done in this area over the past few decades. Keeping in view the exponential growth of the multimedia data, there is a tremendous potential of further research in this field. Further studies may be conducted to evaluate the attack impacts on multimedia data and then watermarking schemes to be developed so that those impacts could be minimized before the start of watermarking so that a better recovery of the copyright data could be performed. Keeping in view the huge financial implications and aspects of the watermarking application areas, more characteristics against some attacks such as forgery attack or multiple watermarking can be embedded. More wavelet transforms should be examined for embedding of the watermark data and robustness against JPEG2000 format conversion. A watermarking scheme may have some relationship with the image on which it is going to apply. Performance of the watermarking scheme or selection of the watermarking scheme or at least few input parameters of the watermarking scheme must be related to image characteristics. The provision of embedding nested watermarks could be explored in future studies for improved security of the watermark under consideration from the pirates.

9 Conclusion

Digital watermarking is an evolving field of research in computer science and information technology besides many other fields which include signal processing, information security, cryptology, and communications. The diverse nature of this field with respect to multimedia has made research more exciting and challenging. Digital watermarking is still evolving and is an open problem for future researchers.

Acknowledgments We thank our parents for their unflagging belief and encouragement.

References

1. Singh N, Sharma D (2015) A review on watermarking & image encoding. Int J Comput Sci Mobile Comput 4(6):632–636
2. Giri KJ, Peer MA, Nagabhushan P (2014) A channel wise color image watermarking scheme based on discrete wavelet transformation. In: Proceedings of IEEE international conference on computing for sustainable global environment trans, pp 758–762
3. Nin J, Ricciardi S (2013) Digital watermarking techniques and security issues in the information and communication society. In: International conference on advanced information networking and applications, pp 1553–1558
4. Sequeira A, Kundur D (2001) Communications and information theory in watermarking: a survey. In: Proceedings of SPIE multimedia systems and application IV, vol 4518, pp 216–227
5. Cox IJ, Miller ML (2001) Electronic watermarking. In: IEEE fourth workshop on multimedia signal processing, pp 225–230
6. Cox IJ, Miller ML, Bloom JA, Friedrich J, Kalker T (2008) Digital watermarking and steganography, 2nd edn. Morgan Kaufman, San Francisco
7. Schyndel RGV, Tirkel AZ, Osborne CF (1994) A digital watermark. In: Proceedings of IEEE international conference on image processing, vol 2, pp 86–90
8. Tirkel AZ, Rankin GA, Van Schyndel RM, Ho WJ, Mee NRA, Osborne CF (1993) Electronic water mark. DICTA, Macquarie University, pp 666–673
9. Kaiser J, Giri M, Nagabhushan P (2015) A robust color image watermarking scheme using discrete wavelet transformation. Int J Image Graph Signal Process 1:47–52
10. Giri KJ, Peer MA, Nagabhushan P (2013) Copyrirght protection of color images using novel wavelet based watermarking algorithm. In: Press: 2nd IEEE international conference on image information processing, JUIT, Shimla, India
11. Kutter M, Petitcolas F (1999) A fair benchmark for image watermarking systems. In: Electronic imaging 199: security and watermarking of multimedia content, vol 3657 of SPIE Proceedings, San Jose, California USA, 25–27 January 1999
12. Jithin VM, Gupta KK (2013) Robust invisible QR code image watermarking in DWT domain. Int J Electron Commun Eng Technol (IJECET) 4(7):190–195
13. Zhao M, Dang Y (2008) Color image copyright protection digital watermarking algorithm based on DWT & DCT. IEEE, pp 1–4
14. Anuradha RPS (2006) DWT based watermarking algorithm using haar wavelet. Int J Electron Comput Sci Eng 1:1–6
15. Zhang Y, Wang J, Chen X (2012) Watermarking technique based on wavelet transform for color images. In: 24th Chinese Control and Decision Conference (CCDC), pp 1909–1913
16. Dey N, Biswas S, Das P, Das A, Chaudhuri SS (2012) Lifting wavelet transformation based blind watermarking technique of photoplethysmographic signals in wireless telecardiology. In: 2012 World Congress on Information and Communication Technologies (WICT). IEEE, pp 230–235
17. Dey N, Mukhopadhyay S, Das A, Chaudhuri SS (2012) Analysis of P-QRS-T components modified by blind watermarking technique within the electrocardiogram signal for authentication in wireless telecardiology using DWT. Int J Image Graph Signal Process 4 (7):33
18. Dey N, Das P, Chaudhuri SS, Das A (2012) Feature analysis for the blind-watermarked electroencephalogram signal in wireless telemonitoring using Alattar's method. In: Proceedings of the fifth international conference on security of information and networks. ACM, pp 87–94
19. Dey N, Biswas D, Roy AB, Das A, Chaudhuri SS (2012) DWT-DCT-SVD based blind watermarking technique of gray image in electrooculogram signal. In: 2012 12th international conference on intelligent systems design and applications (ISDA). IEEE, pp 680–685
20. Dey N, Roy AB, Das A, Chaudhuri SS (2012) Stationary wavelet transformation based self-recovery of blind-watermark from electrocardiogram signal in wireless telecardiology. In:

Recent trends in computer networks and distributed systems security. Springer, Berlin, pp 347–357

21. Khalifa A, Hamad S (2012) A robust non-blind algorithm for watermarking color images using multi-resolution wavelet decomposition. Int J Comput Appl 37(8):0975–8887
22. Elbasi E, Eskicioglu AM (2006) A semi-blind watermarking scheme for color images. Int J Technol Eng Syst (IJTES) 2(3):276–281
23. Craver S, Memon N, Yeo B, Young M (1997) On the invertibility of invisible watermarking techniques. In: Proceedings of the IEEE International Conference on Image Processing, vol 1, pp 540–543
24. Hua Y, Wu B, Wu G (2010) A color image fragile watermarking algorithm based on DWT-DCT. In: Chinese control and decision conference, pp 2840–2845
25. Hartung F, Girod B (1997) Digital watermarking of raw and compressed video. In: Proceedings of SPIE 2952: digital compression technologies and systems for video communication, pp 205–213
26. Hartung F, Girod B (1998) Watermarking of uncompressed and compressed video. Signal Process 66:283–301
27. Chavan SK, Shah R, Poojary R, Jose J, George G (2010) A novel robust colour watermarking scheme for colour watermark images in frequency domain. In: International conference on advances in recent technologies in communication and computing, pp 96–100
28. Brassil J, Low S, Maxemchuk N, O'Gorman L (1994) Electronic marking and identification techniques to discourse document copying. Proc INFOCOM 13(8):1495–1504
29. Langelaar GC, Lagendijk RL, Biemond J (1998) Real-time labeling of MPEG-2 compressed video. J Vis Commun Image Represent 9(4):256–270
30. Dey N, Dey M, Mahata SK, Das A, Chaudhuri SS (2015) Tamper detection of electrocardiographic signal using watermarked bio–hash code in wireless cardiology. Int J Signal Imaging Syst Eng 8(1–2):46–58
31. Friedman G (1993) The trustworthy digital camera. IEEE Trans Consum Electron 39(4):93–103
32. Cox IJ, Miller M, Bloom J (2001) Digital watermarking: principles and practice. Morgan Kaufmann 10:1558607145
33. Wolfgang RB, Delp EJ (1999) Fragile watermarking using the VW2D watermark. Proc Electron Imaging 3657:204–213
34. Anderson RJ, Petitcolas FAP (1998) On the limits of Steganography. IEEE J Sel Areas Commun 16:474–481
35. Brassil J, Low S, Maxemchuk N, O'Gorman L (1995) Hiding information in document images. In: Proceedings of the 29th annual conference on information sciences and systems, pp 482–489
36. Dey N, Biswas S, Roy AB, Das A, Chowdhuri SS (2013) Analysis of photoplethysmographic signals modified by reversible watermarking technique using prediction-error in wireless telecardiology
37. Dey N, Biswas S, Das P, Das A, Chaudhuri SS (2012) Feature analysis for the reversible watermarked electrooculography signal using low distortion prediction-error expansion. In: 2012 International conference on communications, devices and intelligent systems (CODIS). IEEE, pp 624–627
38. Chakraborty S, Maji P, Pal AK, Biswas D, Dey N (2014) Reversible color image watermarking using trigonometric functions. In: 2014 International conference on electronic systems, signal processing and computing technologies (ICESC). IEEE, pp 105–110
39. Dey N, Maji P, Das P, Biswas S, Das A, Chaudhuri SS (2013) Embedding of blink frequency in electrooculography signal using difference expansion based reversible watermarking technique. arXiv preprint arXiv:1304.2310
40. Dey N, Pal M, Das A (2012) A session based watermarking technique within the NROI of retinal fundus images for authentication using DWT, spread spectrum and Harris corner detection. Int J Mod Eng Res 2(3):749–757

41. Liu K-C (2009) Human visual system based watermarking for color images. In: Fifth international conference on information assurance and security, vol 2, pp 623–626
42. Qiang S, Hongbin Z (2010) Color image self-embedding and watermarking based on DWT. In: International conference on measuring technology and mechatronics automation, vol 1, pp 796–799
43. Dey N, Samanta S, Chakraborty S, Das A, Chaudhuri SS, Suri JS (2014) Firefly algorithm for optimization of scaling factors during embedding of manifold medical information: an application in ophthalmology imaging. J Med Imaging Health Inform 4(3):384–394
44. Dey N, Samanta S, Yang XS, Das A, Chaudhuri SS (2013) Optimisation of scaling factors in electrocardiogram signal watermarking using cuckoo search. Int J Bio-Inspired Comput 5 (5):315–326
45. Acharjee S, Chakraborty S, Samanta S, Azar AT, Hassanien AE, Dey N (2014) Highly secured multilayered motion vector watermarking. In: advanced machine learning technologies and applications. Springer, Berlin, pp 121–134
46. Dey, N., Das, P., Roy, A. B., Das, A., &Chaudhuri, S. S. (2012, October). DWT-DCT-SVD based intravascular ultrasound video watermarking. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 224–229). IEEE
47. Chakraborty S, Samanta S, Biswas D, Dey N, Chaudhuri, SS (2013) Particle swarm optimization based parameter optimization technique in medical information hiding. In: 2013 IEEE international conference on computational intelligence and computing research (ICCIC). IEEE, pp 1–6
48. Voloshynovskiy S, Pereira S, Iquise V, Pun T (2001) Attack modelling: towards a second generation watermarking benchmark. In: Signal processing, Special Issue on Information Theoretic Issues in Digital Watermarking
49. Hartung F, Su JK, Girod B (1999) Spread spectrum watermarking: malicious attacks and counter-attacks. In: Proceedings of SPIE vol 3657: security and watermarking of multimedia contents, San Jose, CA, USA
50. Kutter M, Voloshynovskiy S, Herrigel A (2000) Watermark copy attack. In: Wong PW, Delp EJ (eds) IS&T/SPIE's 12th annual symposium, electronic imaging 2000: security and watermarking of multimedia content II, vol 3971 of SPIE Proceedings, San Jose, California USA, 23–28 January 2000
51. Liu L-M, Han G-Q, Wo Y, Wang C-S (2010) A wavelet-domain watermarking algorithm against geometric attacks based on SUSAN feature points. IEEE, pp 1–5
52. Pal AK, Das P, Dey N (2013) Odd-even embedding scheme based modified reversible watermarking technique using Blueprint. arXiv preprint arXiv:1303.5972