Multimedia Tools and Applications (2020) 79:20149–20197
https://doi.org/10.1007/s11042-020-08881-y

A Recent Survey on Multimedia and Database Watermarking

Sanjay Kumar[1] **· Binod Kumar Singh**[1] **· Mohit Yadav**[1]

Received: 25 April 2019 / Revised: 31 January 2020 / Accepted: 23 March 2020 /
Published online: 15 April 2020

Abstract
In today's digital era, it is very easy to copy, manipulate and distribute multimedia data over an open channel. Copyright protection, content authentication, identity theft, and ownership identification have become challenging issues for content owners/distributors. Off late data hiding methods have gained prominence in areas such as medical/healthcare, e-voting systems, military, communication, remote education, media file archiving, insurance companies, etc. Digital watermarking is one of the burning research areas to address these issues. In this survey, we present various aspects of watermarking. In addition, various classification of watermarking is presented. Here various state-of-the-art of multimedia and database watermarking is discussed. With this survey, researchers will be able to implement efficient watermarking techniques for the security of multimedia and database.

Keywords Frequency Domain · Spatial Domain · Robustness · Capacity · PSNR

1 Introduction

Digital data has invaded all kinds of public media such as video, image, audio, and text. Digital data are transmitted frequently over the Internet. Efficient global computer networks have acted as a catalyst for the ever-growing demand for digital media. Hence, digital data are more susceptible to attacks and can be easily compromised [4, 5, 47]. With the help of watermarking, it is possible to identify the (creator, owner, distributor or approved consumer) of an image or document [37, 48, 59]. It can also aid in detecting whether the image or document has been tampered with. Developing a robust watermarking technique having

✉ Sanjay Kumar
2017rscs001@nitjsr.ac.in

Binod Kumar Singh
bksingh.cse@nitjsr.ac.in

Mohit Yadav
mohityadav12041995@gmail.com

[1] National Institute of Technology, Jamshedpur, Jamshedpur, India

high computational efficiency is the need of the hour. There is always a trade-off between the features of watermarking. Existing methodologies are primarily concerned about the robustness, imperceptibility and embedding capacity. Security and complexity features are given less priority in the development of the watermarking scheme. Nowadays powerful multimedia editing software has invaded the market, thus increasing the gravity of malicious media content. Methods like cryptography and steganography can protect digital content. However, one of the most efficient countermeasures against malicious data is digital fragile watermarking [23]. However, most of the existing methods focus on embedding capacity, robustness and losing sight of security. For the security of watermark, the encryption technique can be used [52, 54]. During the last few years, the multimedia watermarking scheme has been evolved rapidly. Apart from this, watermarking is also evolved in the area of IP protection, relational database, cyber-physical system, IOT & 5g technology, and e-governance [9, 24, 25, 58, 72, 76, 79, 80, 83]. Watermarks should be sturdy against information manipulations (like advanced arrange transformation and reckoning digital-to-analog conversion). The following elementary conditions in watermarking apply to all or any media: i) A watermark ought to provide the maximum amount of knowledge as conceivable, which means the watermark data rate must be high, ii) A watermark must stay inside the host data no matter anything happens to the host data. This necessity is stated as robustness, iii) A watermark must be irremovable, iv) A watermark must be common, secret as well as accessible to the authorized party.

During, the last decades, a number of the comprehensive surveys have been published in the area of digital watermarking [2, 32–34, 36, 40, 87, 102, 109]. This survey focuses on the various features and application of the watermarking. In this work, we had done a comprehensive survey based on the multimedia type. Key features of this survey include-

i) Comprehensive literature review of watermarking based on different multimedia types.
ii) Comparative analysis in terms of techniques used and the purpose of the proposed watermarking scheme.
iii) This literature review also deals with the different features and its trade-offs, additionally, it deals with the various attacks on watermarking which will helps the researcher to design an optimal watermarking scheme.
iv) This paper will also help the researchers in a concerned field to analyses that which technique is best in terms of that particular application, attacks, and features.

The outline of the rest of the paper is given below. Section 2 presents the basic concept of watermarking and its classification. Features of watermarking are section 3. In Section 4 State-of-the-art of watermarking techniques is presented. Section 5 deals with the various performance measure of watermarking. Several attacks of watermarking are discussed in Section 6, and finally, we conclude our works in Section 7.

2 Digital Watermarking and its Classification

Digital Watermarking is a method used to set up the identity of any information to protect it from any kind of illegal alteration or use [13, 38, 85]. Digital watermarking process involves two steps - i) Watermark Embedding - in this step the watermark is inserted into the host signal by utilizing the defined algorithm and ii) Watermark Extraction - in this step the watermark is extracted from the watermarked signal.

The watermarking methods are often classified into varied categories. Several authors have classified the watermarking approach in various classes. Fig. 1 presents the various classification of the watermarking. In this work we had classified the watermarking in the three classes - i) classification based on multimedia, ii) classification based on characteristics and iii) classification based on application

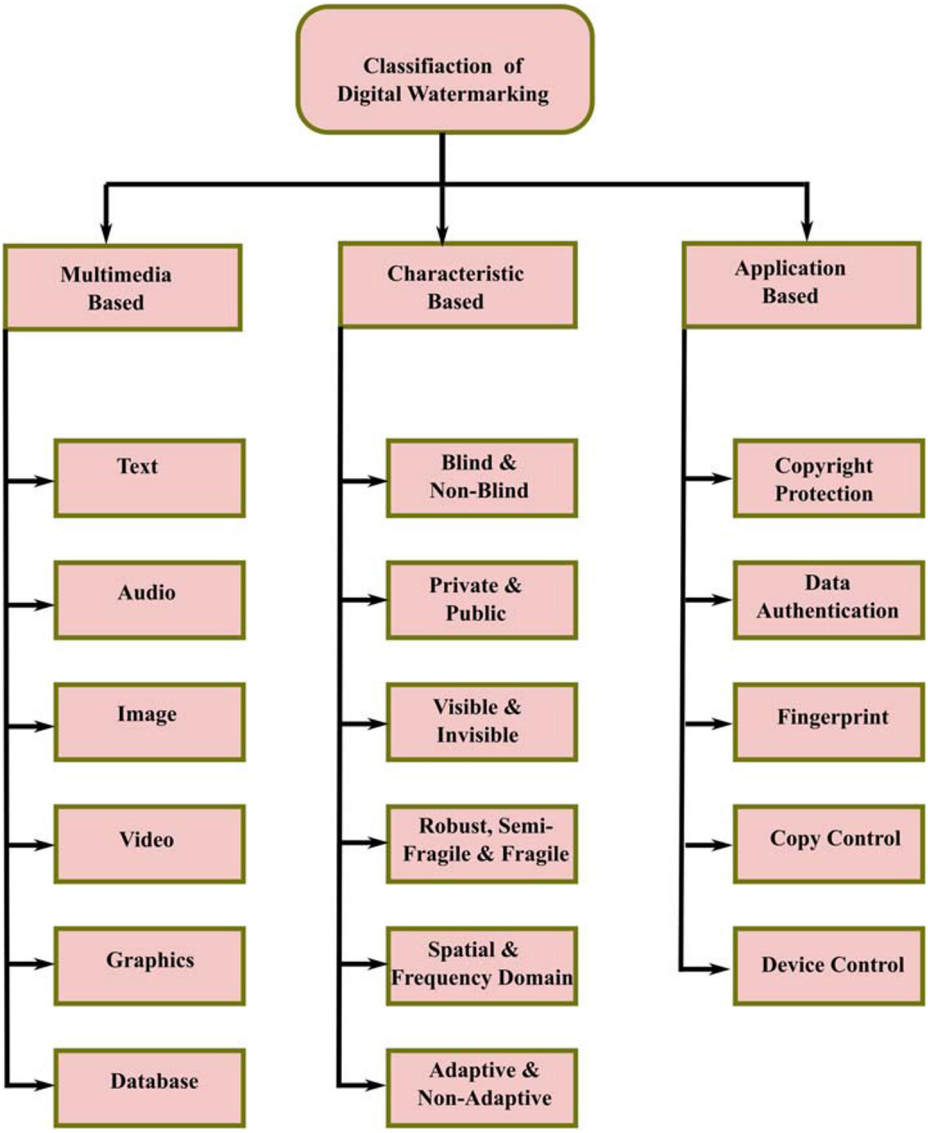

Fig. 1 Classification of Digital Watermarking

2.1 Classification based on Multimedia

Digital text watermarking: - Text data consist of different semantic entities, such as word, sentence, row, paragraph and punctuation mark, etc. The role of syntax and semantics is quite important here, all trans-formation required here is related to one of them to embed the digital watermark into cover text (i.e. text in which watermarks have to be embedded).

Audio watermarking: - Audio watermarking is more challenging than image and video watermarking, since the Human Auditory System (HAS), is notably more sensitive than the Human Visual System (HVS).

Image watermarking: - Image is generally of large size compressed, highly robust & imperceptible watermarks are required to embed into the cover image.

Video watermarking: - Due to 3D characteristics of the video, imperceptibility of the watermark is difficult in video watermarking. The other issues with video watermarking are that video signals are extremely vulnerable to pirate attacks.

Graphic watermarking: - 2D or 3D computerized graphics can have a watermark embedded to indicate the copyright protection.

Database watermarking: - Database can gain more security in terms of confidentiality, integrity, etc. by embedding a digital watermark in the database. To deploy database watermarking, particularly in the healthcare domain, distortion caused due to the watermark should be least to ensure the correct interpretation of records.

2.2 Classification based on Characteristics

Based on characteristics the watermarking methods will be of the subsequent sorts i.e. i) Non-Blind & Blind, ii) Imperceptible & Perceptible, iii) Public & Private, iv) Robust, Fragile & Semi-Fragile digital watermarking, v) Frequency & Spatial Domain

i) Blind and Non- Blind digital watermarking: -Based on the watermark extraction, watermarking technique can be classified into 3 classes like blind, semi-blind, and non-blind. In blind watermarking the watermark is extracted without the cover/original data.
ii) Visible & Invisible Watermarking: - A watermark that is visible to the human eyes is called visible watermarking, otherwise the watermark is said to be invisible. Visible and invisible watermarking techniques are also known as perceptible and imperceptible watermarking respectively.
iii) Private and public digital watermarking: - if a watermark is detectable only by authorized users than it is said to be a private digital watermark. When compared with a public digital watermark it is found that private digital watermarking is more robust. If a watermark is detectable by anyone then it is said to be a public digital watermark. There is another form of it known as asymmetric form, through that without disturbing watermark any user can read it. In this case, verification is done by public key & embedding done using the private key.
iv) Robust, Semi-fragile and Fragile digital watermarking: - if watermarks survive malicious (i.e. that destroys watermark) and non-malicious (do not explicitly mean to modify it) attacks then those watermarks are known as a robust watermark. Copyright protection is one of the applications were using this kind of digital watermark will be beneficial as they are more prone to malicious & non-malicious attacks. A semi-fragile watermark is proposed to sense any unauthorized alteration, & parallel allowing some

image processing operations. They find their application in some selected authentication techniques. Even a slightest change (intentional/unintentional)in watermarked image can be detected by the fragile watermarking scheme.

v) Frequency & Spatial Domain-based: - The watermark is deep-rooted in the cover image (data) by neutering the gray-scale value of the pixels of the novel image (data) while not applying any conversion in case of the spatial domain. While in frequency domain digital watermarking can be done using some transformations such as DWT, Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT), etc. Spatial domain techniques are less robust than the Frequency domain.

vi) Adaptive & Non-Adaptive: - In adaptive, the embedded data is varied on the basis of local properties of host data. Varying the embedded data includes locally adjusting the amount of embedding power and/or controlling the locations where embedding is to be done. Whereas, in the non-adaptive techniques global properties of the host data are used to control the global embedding parameter.

2.3 Classification Based on Application

i) Copyright Protection: - One of the major drawbacks of digital multimedia is that it is prone to easy illegal copying techniques like piracy. So, the need for the techniques to protect the copyright of digital data is needed.

ii) Data Authentication: - A digital signature is one of the outstanding cryptanalytic methodologies for data confirmation. In any case, just in case of the loss of the signature, the confirmation work couldn't be performed. The solution for this is that the signature will specifically be inserted in the work utilizing watermarking. A viable authentication arranges must have the capability to manage whether or not an image or document has been adjusted or not, ready to distinguish any modification created on the image or text.

iii) Fingerprint: - As a result of the progression of innovation, one of the conceivable uses of digital watermarking is fingerprinting. Fingerprinting in digital watermarking is for the most part utilized as the way toward inserting the uniqueness to the image with the end goal that it is hard to temper or abrogate. This allows the copyright holder to find a freebooter if the image is circulated illicitly.

iv) Copy Control: - Copy control is limitation of the advanced media. It can be duplicated without degrading the original quality. Several research are going on to restrict the copy control. IBM, Tokyo Research Laboratory initially proposed the utilization of watermarking innovation for DVD duplicate assurance in September 1996. The security and control can be kept up at the season of dispersing and distributing data, two methodologies might be utilized i) Use of copyright watermark, ii) Laying the foundation for digital right administration framework to get duplicate control of appropriated data where scholarly right assurance and duplicate control are significant concerns.

v) Device management: - The device management watermarking may be a system within which, watermarks are constituted to manage access to an asset plus utilizing a corroboratory device. A few methods of watermarking are created in sound gadgets in past decades, including lowest-bit coding, spread range quantization. Video watermarking on a cell phone is an incredible test because of the constrained asset of the gadget. One of the methods for video watermarking in mobile transforms the video to YC_bC_r portrayal and embeds the watermark in the Y segment of the extracted frame of the video.

3 Features of Digital Watermarking

The features of watermarking plays an important role in the development of a watermarking system for the different applications[45, 77]. As there is a trade-off between these features, so one should keep in mind which feature is to be focused on. Various features of watermarking have been discussed in [2, 36, 87, 102] and is shown in Fig 2. Table 1 shows the vital characteristics and corresponding applications of digital watermark in short.

Image fidelity: - Fidelity is the visual similarity between the watermarked image and its cover image. In other words, fidelity is the amount of imperceptibility of the watermark in the watermarked signal.

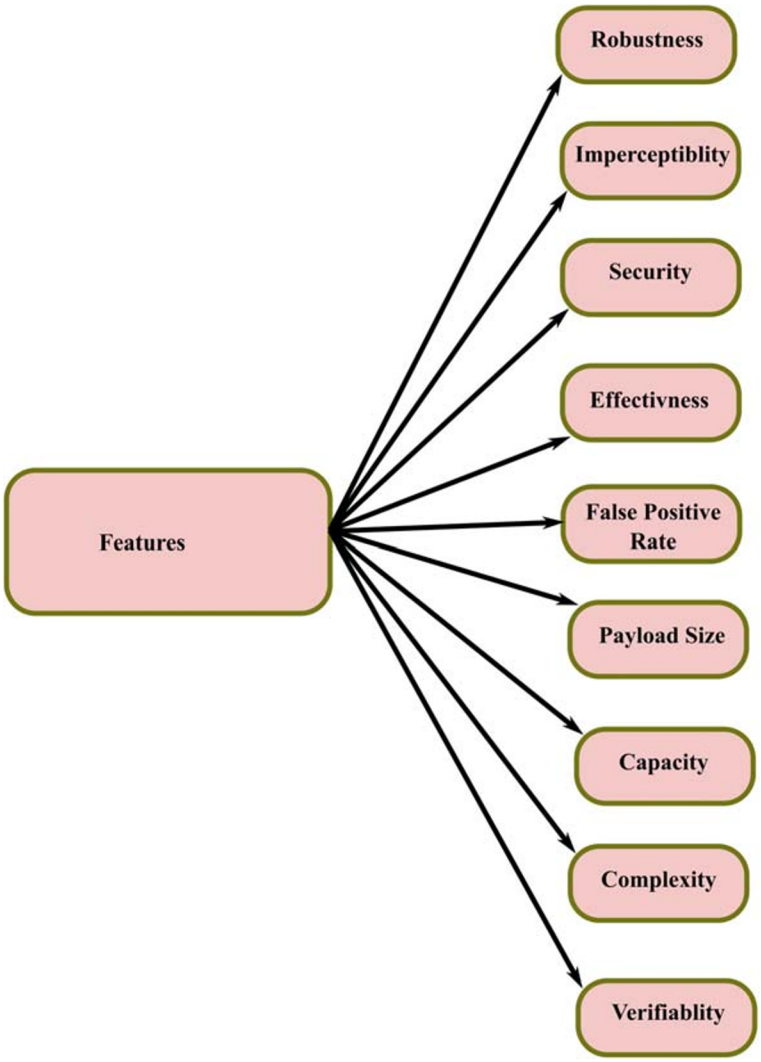

Fig. 2 Feaures of Digital Watermarking

Table 1 Application of watermarking corresponding to features

Sl.	Basic Features	Application
1	Robustness	copyright protection, telemedicine,Digital Image Processing etc.
2	Imperceptiblity	data authentication, telemedicine, digital documents etc.
3	Security	Military, Ownership proof,telemedicine,data aggregation etc.
4	Effictivness	owner identification, telemedicine, copyright protection etc.
5	False Positive rate	tamper detection,telemedicine,etc.
6	Payload size	sensors,digital imaging,video etc.
7	Capacity	Tele-medicine, broadcast monitoring etc.
8	Complexity	copyright protection, sensors, tele-medicine etc.
9	Verifiability	owner indentification, tamper detection, tele-medicine etc.

Robustness: if watermarks survive malicious (i.e. that destroys watermark) and non-malicious (do not explicitly mean to modify it) attacks then those watermarks are known as a robust watermark. Copyright protection is one of the applications were using this kind of digital watermark will be beneficial as they are more prone to malicious & non-malicious attackss.

Imperceptibility: The watermarked image ought to seem like the same as the cover image to the human eye. The spectator can't identify that the watermark is inserted in it.

Security: An unauthorized user cannot distinguish, retrieve or modify the inserted watermark. Nowadays the researcher is giving prime importance to the security of watermark.

Effectiveness: This refers to the odds that the message in the watermarked picture would be accurately distinguished; In a perfect scenario, probability needs to be 1.

False positive rate: This refers to the number of digital works that are recognized to have a watermark inserted whereas in actuality it has no watermark inserted. Hence, it ought to be held less to watermarked frameworks.

Payload size: Data payload or payload size can be defined as the number of watermark bits embedded in a cover data.

Capacity: Without inherent redundancy presented by error-correcting codes for channel coding, the maximum repetition of data payload within the signal(audio, image. etc) is the watermark capacity.

Low Complexity: The cost of computation is directly related to thecomplexity of watermarking. As the complexity of watermarking will be increased automatically cost will also increase.

Verifiability: The watermark ought to have the capacity to give full and dependable proof to the responsibility for secured data items. It very well may be utilized to decide if the data is to be ensured and monitor the spread of the information being secured, recognize the validness, and control unlawful duplicating.

Security: Security in watermarking signifies the capability of resisting the intentional attacks. This feature is very vital to the watermarking system. The security requirements for watermarking schemes differ significantly from application to application.

4 State-of-the-Art

This section contains the recent research worked of many authors on different types of multimedia and database techniques. This section is further subdivided into the various

subsections. Sections 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6 deal with state-of-the-art of image, video, audio, text, graphics, and database watermarking techniques respectively. Limitations and challenges of watermarking techniques are discussed in section 4.7.

4.1 Images

In this section, we had discussed various recent state-of-the-art image-based on watermarking techniques like DCT, DWT, etc. on color, grayscale, medical, etc. images, which has been evaluated based on various performance matrices such as Bit Error Rate (BER), Peak-Signal-to-Noise-Ratio (PSNR), etc. Various attack like image processing and geometric attack, noise, filtering, tampering, etc. also has been performed to check the robustness, imperceptibility, etc. of these techniques for various applications like owner identification/verification, copyright protection, etc.

Su et al.[90] proposed a novel blind color image watermarking scheme. Here, QR decomposition techniques are used to embed the color image watermark into the color host image.

Su et al. [93] proposed a spatial domain blind color image watermarking technique for the copyright protection of color image. Here, by using algebra operation maximum Eigenvalue of Schur decomposition is obtained to embed the watermark.

Su et al. [92] proposed a novel watermarking scheme for the copyright protection of the color image using the DC coefficient and the AC coefficient of the color host image. Experiment results show that the proposed scheme shows better imperceptibility and also is robust against several attacks.

Su et al. [89] has proposed and investigated a spatial domain watermarking scheme for the copyright protection of the color image. Here, based on the features of the DC coefficient of DFT blind and the robust watermarking scheme is developed.

Su [88] has presented a novel blind watermarking based on Hessenberg decomposition. The presented schemes show lower computational complexity than other methods based on singular value decomposition or QR decomposition.

Qin et al [71] have proposed a completely unique self-implanting fragile watermarking technique for images. This system is developed for meddling recovery and is predicated on the reference-data interlocking mechanism and adaptation choice of embedding mode. Experimental results reveal this method is more powerful compared with the rumored schemes.

Roy et al. [78] proposed a method to avoid geometric and image transformation attacks. This method is independent of the cover image. It is purely based on the key. Experimental results reveal that this procedure works well for simple scenarios. It is robust. The fidelity of the cover is also maintained. However, in the case of complex attacks (cropping, rotation, scaling), this method falters. Comparative analysis suggests that the projected technique performs well each in terms of hardiness and time demand than several alternative watermarking techniques. Future work can emphasize rising the projected technique for incorporating higher resistance to compression attacks still as composite attacks involving a combination of scaling, cropping and rotation attacks along.

Parah et al. [66] planned a strong blind watermarking technique, supported block-based DCT constant modification. The experimental results show the common PSNR price of the projected scheme is 41.25 dB that is better than the number of state-of-the-art. Also, Normalized Correction (NC) value are higher than [91, 99].

Huynh et al.[30] planned a completely unique strong blind color image watermarking methodology. Hereby rotten a gray-scale image to binary pictures from LSB to MSB for the

embedment, a gray-scale watermark is totally encoded into a color host image employing a quantization technique within the rippling domain. The experimental results prove that the planned methodology reaches a high performance in a physical property of embedded host pictures and hardiness of extracted watermarks and is superior to the remainder of state-of-the-art.

Aggarwal et al. [1] planned and compared four blind watermarking methods. Here the author has performed eight experiments for a close analysis of the pro- exhibit watermarking strategies S1, S2, S3, and S4. The experimentalresult shows that S3 and S4 have higher PSNR than [46, 56] whereas the S1, S2 has less PSNR.

Vaidya & PVSSR [100] planned a strong blind watermarking methodology using Bhattacharyya distance and mathematical function. The experimental results compared with the state-of-the-art and show a better result.

Thongkor et al. [97] presented a digital watermarking scheme for camera-captured images. In this scheme, to embed a binary image with the same size as the host image each pixel of the host image was used to carry a watermark bit. The average wPSNR of the proposed scheme is 35dB, whereas the average SSIM value is 0.93.

Lai [42] planned a method primarily based upon single value decomposition (SVD) & Tiny-Genetic algorithm. Here, the singular values of the cover image are adapted to embed the watermark. Simulation results have shown that the watermark that has been embedded is robust enough to resist attacks or image process operations and also the hardiness performance of this planned approach is superior to the opposite similar approaches.

Najih et al. [62] devised a contourlet transformation & quantization index modulation primarily based watermarking technique. Lagrange technique was also utilized for optimization. Experiments show higher transparency & more practical physical property &, additionally smart capability and provide better hardiness than other techniques for different attacks.

Sarreshtedari & Akhaee [84] proposed a way to handle image security. The idea was to encode the source channel. It was based on Reed- Solomon (RS) and set partitioning in hierarchical transforms (SPIHT). The initial segment includes the encoder- bits used for content recovery, the second section is made of parity bits and the last region comprises of check bits. The experimentresult shows the effectiveness and superiority of their proposed method in comparison to other methods.

The comparative analysis of state-of-the-art of image watermarking is depicted in Table 2, and Table 3 depicts the summary of image watermarking state-of-the-art.

4.2 Video

In this section we had discussed various recent state-of-the-art of video based on watermarking techniques like multi-resolution wavelet decomposition, chirp Z-transformation & entropy analysis, etc. Various attack like blurring, compression, change in brightness & contrast and geometric attack, noise, filtering and averaging, etc. also has been performed to check the robustness, imperceptibility of these techniquesfor various application like video copyright protection without dropping visual quality, cloud-assisted secure video transmission & sharing, secure blind video watermarking for medical purposes & to limit the pirated copy of digital video distribution, etc.

Venugopala et al. [101] proposed a bitstream video watermarking technique that is carried out by study of the temporal and spatial domain. In their experiment execution time of insertion & execution process was examined, using a mobile device. As a result of the experiment PSNR value of the extracted image is within the acceptable range, which was

Table 2 Comparative analysis of image watermarking

Ref. no.	Domain	Robust	Inperceptiblity	Capacity	Blind	Watermark Type	Objectives
[90]	Transform	√	√	Low	√	Color Image	————
[93]	Spatial	√	√	Low	√	Color Image	Copyright Protection
[92]	Transform	√	√	Low	×	Color Image	Copyright Protection
[89]	Spatial	√	√	——	√	Color Image	Copyright Protection
[88]	Transform	√	√	High	√	Color Image	Copyright Protection
[71]	Spatial	×	√	High	×	Random Sequence	Tamper Detection
[78]	Spatial	√	√	———-	√	Binary Image	Models geometric attack on watermarked images
[66]	Transform	√	√	High	√	Binary Image	——
[30]	Transform	√	√	Low	√	Grayscale Image	Robust blind image color watermarking technique
[1]	Transform	√	√	———	√	Grayscale Image	Owner identification
[100]	Dual	√	√	———-	√	Binary Image	Copyright protection
[97]	Spatial	√	√	Dependent	×	Binary Sequence	Copyright protection
[42]	Transform	√	√	Dependent	×	Grayscale Image	To find optimal scale factor
[62]	Transform	√	√	High	×	Random Sequence	Content authentication
[84]	Spatial	×	√	High	×		detection

Table 3 Summary of recent state-of-the-art of image watermarking techniques

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[90]	to design a blind color image watermarking scheme	QR decomposition	Cover color image: - 512x512 Color Watermark image: 32x32	NC, PSNR & SSIM	JPEG 2000 Compression, Geometric attacks & common image processing attacks.	-robust against common image processing and geometric attacks.
[93]	to protect the copyright of color images	Schur decomposition-based spatial domain blind color image watermarking ,	Cover color image: - 512x512 Color watermark image:- 32x32	PSNR, SSIM & NC	JPEG Compression, Geometric attacks & common image processing attacks.	- real time advantage along with strong robustness.
[92]	robust color image watermarking	two-level DCT	Cover color image: - 512x512 Color watermark image:- 64x64	PSNR, SSIM & NC	JPEG compression, JPEG2000 com- pression, cropping, adding noise, scaling, low-pass filtering, median filtering, rotation, blurring	-Relatively, the capacity of the proposed method is bigger than the state-of-the-art,
[89]	protect the copyright of the color image	features of the DC coefficient of 2D-DFT	Cover color image: - 512x512 Color watermark image :- 32x32	PSNR, SSIM & NC	standard benchmark Optimark software	- the proposed method has the short running time and strong robustness.

Table 3 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[88]	protect the copyright of the color image	Hessenberg decomposition	Cover color image: - 512x512 Color watermark image:- 32x32	PSNR, SSIM & NC	JPEG 2000 Compression, Geometric attacks & common image processing attacks.	-proposed method has lower computational complexity than other methods
[71]	tampering recovery	Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode	Image size 512x512	PSNR, SSIM	Tampering	-content recovery for intentional meddling and inadvertent meddling of block missing within the wireless attenuation channels are simulated to show their scheme's effectiveness
[78]	Stand against Geometric attack	Blind image technique	Cover color image: - 613x833 Watermark image: 100x91	BER, PSNR & SSIM	Geometric attacks & common image processing attacks.	-high visual fidelity of the watermarked cover. -needs better resistance to compression attacks.
[66]	Robust and blind watermarking technique	DCT, Inter-Block Coefficient Differencing	Color & Gray scale image 512x512 Binary watermark image 64x64	PSNR ,BER & NC	Geometric attack, singular and hybrid attacks	-Robust to singular & numerous hybrid attacks. -capable of top quality watermarked pictures s

Table 3 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[30]	robust blind color image watermarking	Selective bit embedding scheme	Eight 512x512 color images Four 64x64 gray-scale watermark image	PSNR, SSIM, NC, CPSNR & NCC.	Average & Median Filtering, Motion Blurring, Rotation & Cropping, Salt & Pepper Noise & Gaussian Noise JPEG Compression (lossy).	-high performance in imperceptibility of embedded host images and is robust
[1]	owner identification/verification technology	RDWT & DWT	8-bit gray scale image 512x512 8-bit gray scale face image as watermark image 64x64	PSNR, NC	cropping from center, Gaussian filtering, salt and pepper noise, rotation, JPEG compression, Resize	- weighted binary coding has drastically improved the performance of watermarking methods.
[100]	Ownership identification and copyright protection	Bhattacharyya distance and bit manipulation, DWT	Host image 512x512 Watermark image 64x64	PSNR, NCC	Salt & Pepper Noise, Mean filtering, Gaussian noise, Median filtering, Cropping, Scaling, Speckle Noise, Rotation, Blurring Translate & JPEG compression	- face up to numerous Signal & Image Processing attacks - marginal distinction of NCC & PSNR
[97]	Protect Camera-Captured Images	Wiener filtering and low noticeable distortion	Image by -DSLR camera - Compact camera - Camera phone	RMSE, wPSNR, NC and SSIM	————————	Robust against various attack ,achieve both reliable watermark extraction from a printed.

Table 3 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[42]	Improvements of The Scaling Factors That Are Used to Control the Strength of The Embedded Watermark	SVD & tiny GA	Cover image 256x256 Watermark image 64x64 gray-level	NC	Image processing attack	-Offers a way to improve Watermark scaling factor.
[62]	Authentication Over an Unknown Channel And Imperceptibility	Angle Quantization in Discrete Contourlet Transform	Cover & watermark image 512 x512 pix, 262,144 samples	NCC & PSNR etc.	Gausian noise, Salt & pep- per noise, Poison noise, Speckle noise, Gaussian Motion Median & Weiner Histogram equalization, Cropping, Rotation, Resizing (512–256–512) , JPEG2000 (Q=1) , JPEG (Q =1) , Gray scale inversion, Gamma corrector 1.6 , Gaussian blur	-higher robustness -more effective imperceptibility -higher transparency -good capacity.
[84]	Detecting the Tampered Area of The Received Image and Recovering the Lost Information in The Tampered Zones.	source-channel coding, SPIHT encoding RS code	Image 8-bit grayscale 512x512	TTR & PSNR	Tampering	-effective under the condition of tampering channel parity bits compare to other scheme

embedded in the video. Also, execution time and power devoured in a cell phone are inside satisfactory breaking points. Also, BER was constant for the entire image.

Preda & Vizireanu [70] has proposed a novel digital watermarking for video dependent on multi-resolution wavelet decomposition. They used the blind watermarking method & binary image as a watermark image. The watermark was inserted into the sub-bands i.e. LH, HL, HH by quantization. The performance was increased by inserting the same watermark in dissimilar frames of the video need improvement against geometric distortion, some detection problem and perceptual quality of watermarked videos & some arithmetical complexity.

Liu et al. [51] projected zero-watermarking novel sturdy techniques for 3- Dimensional videos for DRM- Digital Right Management based mostly upon TIRIs, 2D- DCT, VSS. In their experiment every depth maps and 2nd frames of input 3-D video are first of all smoothed and so subsampled at intervals spatial in addition as a temporal domain. Secondly, by averaging these frames & its depth maps TIRIs are generated. For 2D-DCT, transformations are performed on these TIRIs. Remaining low-frequency coefficients are then chosen for the extraction of coefficients of low frequency to form positive that the strength of content-based choices as a result of they embody the foremost energy of the initial TIRIs to an extent. First, the projected theme doesn't insert the copyright data into the 3D videos and may avoid content distortion that is an improvement over the 2nd video frame-based scheme. More enhancements are needed on robustness against geometrical attackslike cropping & rotation.

Nezhadarya & Ward [63] proposed a semi-blind methodology to test the standard of video degraded by H.26/AVC decompression/compression. Using 2D spread transform modulation bits of watermark are inserted within the multiscale derivative domain. New merit-score (MS) was purposed to seek out the best watermarking parameter & to test the standard of assessment methodology. The results of the experiment show mistreatment STDM methodology yields higher benefit scores rather than inserting in one scale solely & high watermark capability and lustiness against distortion was obtained. Numerous alternative varieties of channel distortion weren't tested like & packet loss and AWGN noise and another challenge is to estimate the standard in terms of other human sensory systems (HVS) based mostly video quality metrics, like VQM and MPQM.

Thanki et al. [96] proposed a hybrid watermarking scheme to achieve fragility and security (copyright ownership or authentication) scheme that uses curvelet transformation with combinations of DCT, CS (Compressive Sensing), DWT & SVD. The result of this scheme claimed faster execution time, high-payload capacity & multimedia data authentication. The quality measures values of the projected theme also are higher than quality measures values of existed schemes within the literature. Further to improve performance instead of wavelet transform, curvelet transform can be used & real-time implementation yet need to perform.

Rasti et al. [73] proposed imperceptible non-blind & robust video frame water-marking technique using QR decomposition SVD; Chirp Z-transform (CZT), DWT & entropy analysis. To evaluate the robustness Correlation Coefficient (CC) metric (variant to contrast & brightness) is used. In this method, frames are divided into moving and non-moving parts. The block-based watermarking theme was used for non- moving parts of every color channel. More for embedding the watermark image instead of the common entropy of all blocks, blocks with entropy lower are subjected. When witnessing the experiment with common signal process attacks results show the proposed scheme is strong & impalpable in nature & performs better than its state-of-the-art.

Loganthan & Kaliyaperumal [55] proposed a reversible adaptive video watermarking technique based on neural network, fuzzy inference system (HVS based) & bidirectional

associative memory (BAM). The first BAM neural network trains multiple watermarks. Second fuzzy inference system of HVS base, embedding adaptive factors are computed that is used to infix the weight matrix generated on the lower video end in its both components luminance & chrominance. Using PLA, coefficients embedding is done. The result of this experiment shows this technique is better where a large number of watermarks are required with good imperceptibility, robustness & good watermark embedded capacity in comparison to other methods. The experiment fails to withstand medium filter Gaussian filter & rotation attacks. Also, it doesn't support fast motion video.

Hossain et al. [26] in order to secure video sharing & transmission proposed a cloud-assisted framework, where mobile client's capabilities are limited. In their proposed work keyframes are deleted using GA when a video is captured by smartphones. Watermark is inserted in the keyframes using the DWT based watermarking technique. Based on error-correcting codes a two-way layer protection mechanism is applied to the identity or signature of an individual to create a watermark that is embedded into the video to protect against attack & transmission loss. Using Shamir's secret theory key is shared among entrusted entities. Then watermark is transmitted to the cloud. SSIM and PSNR were used to carry imperceptibility analysis of the video. The proposed framework has space optimum transmission and security.

Cediclo-Herandez et al. [11] have worked on to improve the video watermarking schemes where distortion is below the sensitivity threshold. They proposed a profile, Saliency-modulated JND (Just Noticeable Distortion) that adopts watermark strength to obtain imperceptibility & robustness. First JND pro le is created using 3 steps (i) Saliency mapping, (ii) JND estimation, (iii) modulation stage. Second JND is used for tuning a basic video watermarking technique's energy. As a result, this experiment generates a lot of powerful video watermarking methodology with a gain of 14.6dB approx. where an unmodulated JND profile gain is 3.11dB. Model V of their approach obtains the most effective performance when put next to different models.

Madine et al. [57] presented a robust blind watermarking scheme for the raw video signal. Here, the watermark is embedded into the HH subband coefficient of the 3 level 2D-DWT of the video frame. The proposed scheme offers low computational complexity which eases the implementation.

Yassin et al. [108] introduced a blind digital watermarking video theme. For security, one secret key's used throughout the recovery of the watermark. In their experiment, using DWT, every video frame is decomposed into a variety of sub-bands. To Quantize the most constant blocks of PCA of every sub-band, quantization Index Modulation (QIM) is employed. Results reveal high imperceptible property. The experiment was conducted on two medical videos. This scheme was extremely strong against several attacks like histograms equalization, noise, gamma correction, JPEG coding.

Nouioua et al. [65] conferred novel and powerful digital video watermarking technique using the SVD. During this recommended technique, the author has resolved the matter of embedding the watermark. It's been done by choosing solely the frames that have huge motion energy that is appropriate to the HSV. The comparison of the results with different video watermarking techniques indicates the prevalence of their theme.

Farri & Ayubi [17] has given a strong secure and video watermarking technique supported whole number rippling remodel and also the generalized chaotic trigonometric function map. The experimental results show that the PSNR value of the projected techniques is 45.07 dB.

Asikuzzaman et al. [10] has planned a basic blind digital video watermarking scheme based on the DT CWT. In the planned technique, the author has embedded the watermark into the low-frequency parts of the U channel in a YUV illustration wherever these components guarantee hardiness and exploitation the U channel enhances the physical property. The experimental results show that this theme is additionally sturdy to compression, cam-cording, watermark estimation re-modulation, temporal frame averaging, multiple watermark embedding, different geometric attacks and downscaling in resolution

The comparative analysis of state-of-the-art video watermarking is depicted in Table 4, and Table 5 depicts the summary of video watermarking state-of-the-art.

4.3 Audio

In this section, we have discussed various recent state-of-the-art audio based on watermarking techniques like DWT, DCT, Arnold Transformation, Entropy, Fast Fourier Transform (FFT) spectrum, etc., ona various set of audio clips of different length. This has been evaluated based on various performance metrics such as signal-to-noise ratio (SNR), Segmental Signal-to-Noise Ratio (SSNR), Mean Opinion Score (MOS), BER, Percent Root-Mean-Square Difference (PRD), and Time-Scale. Modification (TSM), Objective Difference Grade (ODF) & NC etc. Various attacks like AWGN, re-sampling, re-quantization, amplification, cropping, noise, filtering, echo, jittering, stir-mark also has been performed to check the robustness for various applications like authenticity verification of audio signals, copyright protection & privacy protection in biomedical signals, etc.

Saadi et al. [82] proposed a method of blind watermarking of audio signals and speech. After the signal is framed, they used the DWT and then applied the discrete cosine transform (DCT) on each frame. For correlation purposes, the frame is decomposed into two segments to perform sub-sampling. In order to a security concern, Arnold transform is applied to the watermark. Without using the insertion parameter & original speech/audio signal the fully blind detection is accomplished. Experimental comparisons and assessments of their scheme with other schemes determine a good balance between robustness, security, capacity & imperceptibility. The decomposing with sub-sampling declines robustness against the re-sampling attack.

Hu et al. [27] introduced a blind watermarking scheme in audio files using distributive characteristics of the wavelet coefficient. Results establish the strength of the projected LWT-SSR against time-shifting and time-scaling attacks and customary signal process operations compared with four different progressive techniques.

Renza & Lemus et al. [74] introduced a new fragile scheme for audio forensics purposes, like digital audio authenticity based on the OVSF (Orthogonal Variable Spreading Factor) & QIM. The main feature of their proposal is that the process which is embedded is accustomed in accordance with the amplitude/length and the value/length of the mark of the audio signal. Through quantization index modulation (QIM) in the wavelet domain using a min value of quantization support the embedding process which increases the fragility. Kappa index, sensitivity, and specificity used for performance analysis against several attacks.

Hwang et al. [31] has proposed QIM-based watermarking techniques for stereo audio signals that fully exploits the key features of SVD. As the proposed method efficiently exploits the ratio of singular values, the embedded watermark is extremely imperceptible and robust against volumetric scaling attacks.

Dhar & Shimamura [14] has proposed an audio watermarking scheme using Log-Polar Transformation (LPT) and entropy-based on SVD in DCT domain. First, their scheme utilizes entropy, LPT, DCT, quantization, and SVD jointly. In the end, the highest entropy DCT

Table 4 Comparative Analysis of Video Watermarking Techniques

Ref. no.	Domain	Robust	Blind	Imperceptibility	Video preprocessing	Message preprocessing
[101]	Spatial		×	√	×	×
[70]	Transform	√	×	√	×	×
[51]	Transform	√	×	√	√	√
[63]	Transform	×	×	√	×	×
[96]	Transform	×	×	√	×	×
[73]	Transform	√	×	√	√	√
[55]	Transform	√	×	√	√	×
[26]	Transform	√	×	√	√	√
[11]	Transform	√	×	√	×	×
[57]	Transform	√	√	√	×	√
[108]	Transform	√	√	√	×	×
[65]	Transform	√	√	√	√	√
[17]	Transform	√	√	√	×	×
[10]	Transform	√	√	√	×	×

Table 5 Summary of recent state-of-the-art of video watermarking techniques

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[101]	Embedding Image as watermark in Video using mobile device	bitstream video watermarking technique	Video of .mpg format Watermark image of .png format of various size 15x13 25x36 etc.	BER, PSNR	———————-	-execution time and power devoured in a cell phone are inside satisfactory breaking points. -Reasonable for utilizing in real-life application of video watermarking. -bit error rate was constant for all the image.
[70]	video copyright protection	Robust watermarking based on multi-resolution wavelet decomposition.	videos are in RGB uncompressed avi format, of 1s duration, resolution 352x 288 and frame rate 30 frames/s. watermark is of binary image 64 x16 pixels	PSNR, BER	Blurring, Brighten, Gaussian Noise, Median Filtering, Salt & Pepper noise, Frame Averaging, Frame Removal, JPEG, MPEG-2 4Mbps, MPED-2Mbps.	-performance was increased by inserting the same watermark in dissimilar frames of the video -need improvement against geometric distortion
[51]	digital rights management of 3D videos	Novel robust zero-watermarking scheme, TIRIs &VSS	Interview: 120 Frames (720x576) Dancer & Ballet: 100 frames (1024x748) Manual Video: 120 frames (1920x1080) 50 images: (320x120)	NCs, PSNR, SSIM and error probability	Gaussian Blurring, Changes in Brightness Change in Contrast, Gaussian Noise, Median Filtering, Salt & Pepper noise, Average Filtering, Rotation, Cropping, Resize.	-improvement are required on robustness against geometrical attack.

Table 5 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[63]	Semi-blind quality estimation of compressed videos using digital watermarking	pseudo-random binary watermarks in the I-frames, STDM	Video QCIF (176 x 144) 4:2:0 sequences "Suzie", "Carphone", "Foreman" and "Mobile", at Sample rate: 30 fps	QA (PSNR, SSIM BER)	Compressions	-precisely estimates Video quality distorted by H.264/AVC compression/decompression. -robustness against distortion - high watermarking capacity
[96]	Security of multimedia data	A hybrid watermarking scheme based on CS, DCT, DWT & SVD.	This video contains 15 frames with a size of 256x 256 pixels.	PSNR, SSIM	Geometric Attacks, Signal Processing Attacks, And Compression Attacks	-high fragility, faster execution time, high-payload capacity & multimedia data authentication. - instead of wavelet transform curvelet transform can used -real time implementation yet need to perform
[73]	video watermarking without dropping the visual quality of the sequences	QR decomposition SVD, Chirp Z-transform (CZT), DWT & entropy analysis.	-300 frames - Each size 1024 x1024 - Akiyo video -150 frames - Each size 1024x1024 - Bus video - Watermark Image 128x128.	CC metric, PSNR	signal processing attacks (Frame number, Flipping, Histograms Equalization, JPEG, Cropping, Blurring, Gaussian Noise, Contrast, Salt and pepper noise, Sharpening, AWGN, Scaling, Gamma Correction	-robust & imperceptible in nature against common signal processing attacks.

Table 5 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[55]	secure video transmission over a communication	Multi-BAM-FUZ	Various different size of video with different no of frames and diff length are used. 352x288 25fps 12s , 512x512 28fps 20s etc	PSNR, SSIM, NCC, BCR	Frame Noising, Gamma Correction, Frame Filtering, Brightness Adjustment, Histogram Attack, Frame Resizing, Frame Cropping, Frame Rotation, Frame Swapping, Frame Dropping, Frame rate Conversion Frame Averaging, MPEG Compression and JPEG Compression	(i) -this technique is better were large number of watermarks are required with good imperceptibility, robustness & good watermark embedded capacity. -Experiment fails to withstand medium filter gaussian filter & rotation attack. -doesn't support fast motion video.
[26]	Cloud-assisted secure video transmission and sharing framework for smart cities	GA & DWT	H.264 video each frame 512x512	SSIM, PSNR	————	- Proposed framework has space optimum transmission and security.
[11]	improving video watermarking schemes	A spatiotemporal saliency-modulated JND profile	First 10 videos:- Resolution: 352x288 px; Frame rate: 30 fps; Remaining videos:- Size: 704x576 px Frame Rate: 24 fps	PSNR, SSIM, BER	Compression and noise	-robust video watermarking method with average gain of 14.6dB -where an unmodulated JND profiles gain is 3.11 dB.
[57]	robust watermarking method for raw video signals	multiplicative watermarking techniques	YUV 4 : 2: :2 CIF resolution (352×288)	PSNR, BER	Gaussian noise, median filtering, frame removal, and H.264/AVC compression attacks	-the receiver requires no side information but a simple secret key to extract the embedded watermark.

Table 5 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance Metrics	Attack Performed	Remark
[108]	secure blind video watermarking for medical purposes	DWT, PCA & QIM	-Video of heart failure -Video of CT scan of Head -Frame size: 256x2 . -Binary Image watermark 32x32.	NC, PSNR	Gamma correction 0.5, Gamma correction 2, Gamma correction 4, Automatic equalization, Gaussian noise (5 Contrast factor (10), Contrast factor (30), JPEG Quality (80 JPEG Quality (50 JPEG Quality (40 MPEG 1.5 Mbps, Resize 256:512:256 Rotate 5, Cropping	- highly robust to various attacks such as Histograms equalization, JPEG coding, gamma correction, Gaussian Noise
[65]	To eliminate the problem of embedding watermark in all video frames	SVD and MR-SVD	RGB uncompressed avi format, frame rate 30fps Binary watermarked image 9x11	NC, BER, MSSIM	Median filter, Gaussian filter, sharpening, frame Averaging/dropping attack, & Compression attack.	- secure & robust to a va- riety of attacks. -also ro- bust to synchronization at- Tack
[17]	video copyright protection.	IWT and 3D generalized chaotic sine map	-CIF format -288x352 watermark, - Binary Logo of Islamic Azad University Size: 32x32 (1024 bits)	PSNR, BER, NCC, SSIM	jpeg compression, cjpeg 2000, salt and peppers, Gaussian noise, histogram equalization, median filter, gamma correction, averaging filter, low- pass filter, rotation,	- used to hide data in many applications, including video monitoring and authentication. - good resistance to any type of attack.
[10]	To limit the pirated copy of digital video Distribution	DT CWT	video sequences of resolution 1080x1920 & 288x352: 300 frames	NCC, FALSE NEGATIVE RATE (%),	lossy compression, frame rate conversion, downscaling in resolution, multiple watermark embedding, WER, TFA, and geometric attacks	-incorporated an angular registration strategy that improves the robustness to rotation. Robust to all this attack and also to camcording from a large screen

sub-band is used to obtain the highest singular value and its Cartesian component is quantized to embed the watermark. Simulation results prove that this technique can be used for the purpose of copyright protection of the audio signal.

Fallahpour & Megias [16] proposed an audio watermarking system with high- capacity to insert and extract data way by changing the certain number of FFT spectrum magnitudes by Fibonacci number. A particular frequency band of the FFT spectrum was selected to insert secret bits. Secondly, a large Fibonacci number (lower than the magnitude of each FFT spectrum) was calculated. These were then embedded in each frame. Results reveal the algorithm to be robust with a capacity of 700 bps to 3 kbps. The comparison proves the prevalence in each capability and imperceptibility of the recommended technique with relevance to different techniques within the literature.

Xiang et al. [105] suggested an audio watermarking method based upon orthogonal PN (Pseudo Noise) sequence, DCT, variable embedding strengths and polarities while preserving the embedding capability. During embedding, DCT is applied to the audio signals to obtain segments of audio in the DCT domain. Post this, a bunch of orthogonal PN sequences is generated, each containing several bits for watermarking. An embedding algorithm is then used to introduce a watermarking sequence in an audio sample. The watermarked bits are obtained by comparing & computing the correlations among orthonormal PN sequences and the watermarked audio segments. Some of the pros of this scheme include robustness, high embedding capability, quality preservation & low computational complexity. Simulation results demonstrate the superior performance than the other progressive technique.

Hua et al. [28] with optimized imperceptibility and hardiness, they proposed an audio watermarking methodology that supported time-spread echo. An FIR- filter based on convex optimization was accustomed to getting the best echo filter coefficients. The echo filter power spectrum is molded by (ATH- Absolute Threshold of Hearing) & (MPSM-Maximum Power Spectral Margin). However, there was scope for improvement against de-synchronization attacks. Though relaxation has been employed in the improvement for economical solutions, the designed watermark still enjoys vital improvement in terms of each imperceptibility and hardiness as compared to the present state-of-the-art solutions [105] and [106].

Xiang et al. [104] proposed a patchwork-based audio watermarking strategy against de-synchronization attacks such as jitter attacks, time-scaling and pitch-scaling utilizing DCT and logarithmic DCT (LDCT). The proposed scheme shows high embedding capacity compared with other audio watermarking techniques.

Lei et al. [44] proposed a Quaternion Wavelet Transform (QWT), Self-Adaptive Particle Swarm Optimization (SAPSO) and chaotic outline based audio watermarking scheme. The highlight of this schemes are - (i) an ideal adjust of the conflicting watermarking prerequisites is decided by the SAPSO calculation without SAPSO parameters tuning; (ii) both SVD & QWD are investigated to improve performance; and (iii) a (MSS - Modified Spread Spectrum) based watermarking strategy is proposed to embed the watermark bit & synchronization code utilizing the 4D QWT coefficients. The proposed algorithm is exceptionally robust against attacks like re-quantization, resampling, MP3 compression, additive noise without significantly corrupting imperceptibility. The method comes about to illustrate that the proposed algorithm outflanks SVD- related, optimization-based, and conventional wavelet techniques. It is seen that their projected scheme outperforms the present chosen audio watermarking Schemes with respect to SNR and Corr values.

Yuan et al. [110] proposed a novel advanced audio watermarking technique based upon strong (DT CWT - Dual-Tree Complex Wavelet Transform) and (MFC- CFD - Mel-frequency Cepstral coefficients feature detection). The vigorous MFC- CFD strategy is proposed to extricate the highlight segments that ought to be migrated when they have audio signal attacked by different mutilations counting both the common & conventional geometric mutilations. The direct relationship is calculated to evaluate the presence of the watermark amid the watermark detection. Experiments reveal that the suggested methodology can accomplish robustness against MP3 compression, low-pass filtering, normalization, volume alter, geometric distortions, like pitch invariant TSM, resample Time-Scale Modification (TSM) and beat invariant pitch moving. The comparison results reveal that the projected scheme performs far better than its state-of-the-art.

Ali et al. [7] projected a zero-watermarking for the privacy protected healthcare system. Here the proposed framework includes 2 modules, initial zero- watermarking to secure the identity of a person. The second module is made for the invention of vocal overlay muddle. The performance of this approach is assessed by utilizing the MEEI voice clutter database. The experimental results show that the projected algorithmic rule is reliable within the detection of a subject's identity and strong against noise attacks with varied SNR when putting next to alternative state-of-the-art technique.

Table 6 depicts a summary of the state-of-the-art audio watermarking techniques.

4.4 Text

In this section, we have discussed various recent state-of-the-art text-based watermarking techniques like character encoding & attributes, open word space, homoglyphs substitution, semantic role labeling, new-defined character, etc. Various attacks like deletion, insertion copying, pasting, replacing, etc. also been discussed.

Rui et al. [81] suggested a watermarking method based upon character encoding and properties for texts blended in Chinese and English. To begin with, information required to watermark was encoded after that key was connected and after that, it was stratified. The MD5 encryption technique is used to enhance security. This scheme shows a high embedding capacity.

Alotaibi & Elrefaei [8] proposed two imperceptible watermarking methods for Arabic content based on the pseudo-space. Within the first proposed strategy, based on dotting include in Arabic content the pseudo-space is embedded before and after typical word space. The second proposed strategy increment the capacity by embedding the pseudo-space and extra three small or zero-width spaces, where the absence demonstrates bit "0" and the presence of them shows bit "1". Utilizing variable measure text samples with different watermark lengths for the proposed strategy a few tests are conducted. As a result of this, Strategy 2 has the most noteworthy capacity but marginally lower imperceptibility than Strategy 1. Also, they are vigorous against electronic content attacks such as content designing, replicating and sticking, and content altering for altering proportion up to 84%. Further, rather than utilizing binary bits text watermark can be utilized with compression calculations such as Huffman calculation to represent the watermark. Within the proposed watermarking strategies, a private key may well be utilized to demonstrate the genuineness. The capacity results of the proposed methods are higher than the other watermarking scheme.

Mir [60] has proposed a web-based text watermarking scheme for HTML text in the webpage. HTML body is parsed to serve as the watermark. Post parsing, a hash function is used to embed undetectable control characters. This results in an undetectable set of

Table 6 Summary of recent state-of-the-art of audio watermarking techniques

Ref. no.	Purpose	Techinques Used	Input/Output	Performance matrixs	Attack Performed	Remark
[82]	Novel secured scheme for blind audio/speech	v Arnold transform, Sub-Sampling, Norm-space, DWT & DCT	Speech & Audio signal 16-bit mono wave file, and frequency 44,100 Hz	SNR, SSNR, MOS, BER, NC	AWGN, Re-sampling Re-quantization, Echo, Amplification + Cropping.	-good tradeoff between robustness, capacity, security and imperceptibility against various signal processing attacks. - The decomposing with sub-sampling declines robustness against the re-sampling attack
[27]	Synchronous blind audio watermarking	Synchronous blind audio watermarking (LWT-SSR)	audio signals were sampled at 44.1 kHz with 16-bit resolution (45, 30s music clip)	SNR, BER	Requantization, Amplitude scaring, Noise corruption, lowpass filtering, DA/AD conversion Echo, Jittering MPEG-1 LAYER 3, TIME SHIFT, PSM	-Highly robust against time-scaling and time-shifting attacks.as well as common signal processing operations. -PEAQ watermarked audio signals used are closer to the original
[74]	Authenticity verification of audio signals	a new fragile watermarking scheme based on OVSF & QIM	15 voice files and 15 music files	PRD, NC, PSNR	mute attack, substitution attack, additive noise, localized amplitude reduction attack	-Used for audio forensics verification -Professional system to pick out the Delta worth or to select the ripple coefficient for the insertion method are often used.

Table 6 (continued)

Ref. no.	Purpose	Techinques Used	Input/Output	Performance matrixs	Attack Performed	Remark
[31]	Blind digital audio watermarking	SVD-Based Adaptive QIM Watermarking	20 stereo audio sequences in the unified speech and audio (USAC) database, sampled at 48 kHz with 16-bit quantization	WSR, BER	scaling attack, Resampling, AWGN	-proposed scheme had robustness to volumetric scaling attacks
[14]	Copyright protection of audio Signal	Blind watermarking scheme based on entropy, LPT (based on SVD in DCT domain)	four different types of 16-bit mono audio signals (Jazz, Blues, Folk, and Classical) sampled at 44.1 kHz	NC, BER, SNR	Noise addition, Cropping, Resampling, Requantization, Signal addition and subtraction, MP3 compression.	–To improve the performance of the proposed scheme, synchronization code and error correcting need to be incorporated.
[16]	Novel high-capacity audio watermarking	Fibonacci Numbers (FFT Spectrum)	All audio clips are sampled at 44.1 kHz with 16 bits per sample and two channels.	ODG, SNR, BER	AddBrumm, AddDynNoise, AddNoise, AddSinus, Amlify BassBoost, Echo, FFT RealReverse, FFT Stat1, Invert, RC HighPass & LowPass, Stat1 Synchronisation	-high capacity (700 bps to 3 kbps) deprived of distortion (ODG 1). - robust against signal processing attacks attacks
[105]	Copyright protection of audio data	Spread Spectrum Audio Watermarking Using Multiple Orthogonal PN Sequences and Variable Embedding Strengths and Polarities	Audio clips: Type: mono - channel Duration: 10 sec Sample rate: 44.1kHz 16 bit quan- tization.	DR, ODG	Closed-loop, Re-quantization, Noise, Amplitude, MP3, AAC, HPF, LPF	-highly robust against many strong attacks -has highly embedding capacity without degrading the perceptual quality -low computational complexity.

Table 6 (continued)

Ref. no.	Purpose	Techinques Used	Input/Output	Performance matrixs	Attack Performed	Remark
[28]	audio watermarking scheme with optimized imperceptibility and robustness.	time-spread echo-based audio water- marking scheme based on FIR, ATH, MPSM	v 15 host audio clips. mono-channel less than 30s, 44.1 kHz sampling frequency, and 16-bit quantization.	DR, SNR, fwsSNR	Closed-loop, Re-quantization, WGN, Amplitude scaling, MP3, AAC, Pitch Scaling	-work need to done to enhance the robustness against de-synchronization attacks.
[104]	audio watermarking method to resist de-synchronization attacks	patchwork-based audio watermarking (DCT & LDCT)	30 mono-channel audio clips. Each audio clip of 10s sampled at the rate of 44.1 kHz and 16-bit quantization	DR, ODG	Closed-loop, Re-quantization, Noise, Amplitude, MP3, AAC, HPF, LPF, Re-sampling, Pitch-scaring, Time-scaring, Jitter, Time-shifting	-computational error could occur due to performing interpolation in the discrete-time domain. -all watermark extract errors are due to miss detection
[44]	To addresses the conflicting problem of robustness, imperceptibility, and capacity of audio watermarking scheme	SAPSO & QWT	full songs and human voice signal. The wave files are 16-bit mono file, sampled at 44.1 kHz.12 scenarios are utilized as test sample	False positive Error, MSE, Entropy, SF, Corr, SNR	AddBrumm, AddDynNoise, AddNoise, AddSinus, Amlify BassBoost, Compressor,Copysamples, Cutsamples, Echo, Exchange, Extrastereo, FFT RealReverse, FFT Stat1, Invert, RC HighPass & LowPass, Stat1 etc(Stir-mark)	Robust against Requantizzation, Additive noise, MP3 Compression Resampling

Table 6 (continued)

Ref. no.	Purpose	Techinques Used	Input/Output	Performance matrixs	Attack Performed	Remark
[110]	Stand against audio signal processing and the conventional geometric distortions,	DT- CWT & MFCCFD	16 bit mono .WAV audio Sample rate 44.1 kH	TSM, PSNR	Stir-mark, MP3, Low pass, Resample Volume, Echo Equalization , Dnoise.	Robust against Echo addition, MP3 Compression, Geometric distortion, Pitch Shifting etc.
[7]	Privacy Protection in Biomedical Signals	Zero-watermarking algorithm	Audio samples 60 dB noise	MEEI voice disorder database, SPE, ACC, SNE, ROC, SNR, BER =1.1, NCR =0.99, ENR =0.98 .	Addition of noise, White-Gaussian noise	-robust against noise attacks with various SNR -imperceptible and reliable in its extraction of identity -application: electronic health care system

watermarks. Specific verbs (is, are), articles (a, an), & often occurring prefix letters (wh, th) of English dictionary are used.

Rizzo et al. [75] suggested a watermarking method able to work on all the SM (Social Media) stages based on the homoglyphs substitution. Hash work is used to embed the text content by substituting their homoglyphs with unique symbols. For evaluation, they select 18 different SM stages, utilizing 6,000 posts from 6 profiles of public personalities.

Halvani et al. [22] proposed four natural language watermark embedding scheme, to operate on the lexical and syntactic layer of German texts. The presented scheme has the advantages like sovereignty from complex NLP methods and rich lexical resources. Also, the proposed scheme shows better run-time efficiency.

Liu et al. [50] proposed strategies for graphic digital text Watermarking. This comprises 8 levels, etymon, line, push, section, page, character, pixel, and chapter; 3 parts, structural feature, similitude, and self-characteristics. They portray the implementation and focuses on the effectiveness of hypothetically.

Chen et al. [12] proposed a new technique for watermarking text which employs the linguistics roles to implant the watermark information. (NLP- Natural Language Processing) is applied to seek out and tag the 3 types of linguistics elements A0, A1, and ADV in content. Here, the watermark is changed into the hexadecimal Unicode and then compressed using Huffman encoding.

Zhang et al. [111] proposed a modern watermarking algorithm for Microsoft Word reports based on newly defined characters utilizing TrueType. The proposed algorithm specially designed for the copyright assurance of Microsoft Word records. In this scheme, the TrueType function produces newly defined characters that are utilized as a watermark, and after that concurring, to a few rules, this watermark is implanted into the MSWord document. This algorithm was simulated using C++. Results show that this algorithm has high strength, total imperceptibility against numerous sorts of attacks and can find the alter range. Additionally, it can be connected to both English and Chinese. In spite of the fact that the scheme has effective performance, it can be optimized, for illustration, the semantic approach can be utilized to decide the inserting positions, and the watermark can be prepared before implanting, etc.

Zhang et al. [112] presented a watermarking procedure for texts written in Chinese. The methodology inserts the watermarking signals into a few Chinese characters by modifying the dimensions of closed rectangular regions in these elements, thus it's entirely primarily based upon the content. Compared to strategy [94], this is often a lot of economical in concealing the characters.

Al-Sewad et al. [6] planned a text/content watermarking scheme for making certain the possession and property rights of the color images. Inserting is accomplished by embedding texts indiscriminately into the color image as clamor. They embraced the YIQ image for the implanting method as a result of it had been found to be faster than different image handling ways. A discretionary alternative of encrypting the text watermark before inserting is in addition prescribed, where, the content may be encrypted utilizing any enciphering procedure.

Summary of the recent state-of-the-art text watermarking is depicted in Table 7.

4.5 Graphics

In this section, we had discussed various recent state-of-the-art graphics based on watermarking techniques.

Table 7 Summary of recent state-of-the-art of Text watermarking techniques

Ref. no.	Purpose	Techniques Used	Input/Output	Performance Metrics	Attack Performed	Remark
[81]	Better robustness and security	Multiple watermarking algorithm based on character encoding and attributes	TText file (English + Chinese words mixed)	Capacity	deleting or adding character	Large watermarking capacity, strong security, auto error correction and imperceptibility. Algorithm easily decodable
[8]	protect text copyright and to detect unauthorized use.	Open word space	Arabic text	Capacity Ratio	Localized Insertion, Dispersed Insertion, Localized Deletion, Dispersed Deletion, Copying and Pasting, Formatting, Retyping, Printing, and OCR.	Two methods for Arabic text watermarking are proposed by utilizing each word space -test Method 2 has highest capacity but slightly lower imperceptibility than Method 1.
[60]	Copyright for web content	invisible text watermarking	Web page http://en.wikipedia.org/wiki/Cryptographic_has_function	————————	Test related to hashing	- English language rules applied. This method is not dependent on language.
[75]	To investigate whether SM do apply watermarks on the texts. & Design watermarking method able to work on all the SM platforms	homoglyphs substitution	18 the most popular Social Media	Visibility	copy and paste	-ensure length of original text is preserved -robust to copy paste

Table 7 (continued)

Ref. no.	Purpose	Techniques Used	Input/Output	Performance Metrics	Attack Performed	Remark
[22]	Imperceptible Natural LanguageWatermarking for German Text	Imperceptible Natural Language Watermarking scheme	German Text	Corpora	————————	– Not suitable for brief texts. If NLP tools are used, quality of CoSp & CoDe Can be improved
[50]	research framework for Graphic Digital Text Watermarking	Graphic Watermarking Framework	Graphic Digital Text	————————	————————	This algorithm makes full use of the self-characteristics, similarity and structural feature of line, etymon and characters All the similar characters are encoded to a unique binary string,
[12]	natural language based watermarking technique	Semantic Role Labeling Jianping	Xml format file	————————	————————	The algorithm does not make any change to the content and format of a text. Result of experiment show has good disguise and robustness.

Table 7 (continued)

Ref. no.	Purpose	Techniques Used	Input/Output	Performance Metrics	Attack Performed	Remark
[111]	copyright protection for Microsoft Word documents.	New-defined Characters	Chinese & English Text	————————	————————	high robustness, completely imperceptibility against many types of attacks and can locate the tamper area. further it can be optimized
[112]	protecting Chinese data such As integrality , authenticity, , con- fidentiality	Occlusive Components	Chinese Text(.BMP format, length 5475 Characters, Bold -face font)	————————	DDirect Attack (replace occlusive character regions with unmarked characters), Another Attack (destroy Occlusive character regions)	Only tested for bold-face fonts. Method is robust than character, word-shift, line shift coding etc.
[6]	Ownership verification	YIQ image processing model	Text & Color Images	PSNR	————————	PSNR value = 70 dB for a text watermark of 2000 characters which can be considered good enough as compared with other techniques.

Doncel et al. [15] presented an optimal blind detector structure for watermarked polygonal lines in 2 D vector graphics data. Here, Detection error probabilities and ROC curves are used for the performance analysis of the proposed detector.

Lin et al. [49] proposed semi-blind and semi-fragile reversible watermarking techniques for authenticating 2D vector graphics. Here, for the authentication purpose principle of bionic spider web is used.

Xio et al.[107] has proposed combined reversible watermarking techniques for 2D CAD engineering graphics. This scheme has been developed by utilizing the concept of Improved Quantization Index Modulation (IQIM) and Improved Difference Expansion (IDE).

Peng et al. [67] proposed a reversible watermarking scheme based on iterative embedding with virtual coordinates. Experimental results shows that, this scheme can be applied for content authentication and secret communication in 2D CAD engineering graphics.

Summary of the recent state-of-the-art graphics watermarking techniques is depicted in Table 8.

4.6 Database

In this section, we had discussed various recent state-of-the-art of database based watermarking techniques like twice-embedding method, etc. on various data sheets, RDBMS Tuples, etc. which has been evaluated based on various performance matrices such as numerical certainty level, PSNR, Alternation ratio, similarity score, false hits & miss rate & NC, etc. Various attacks like substitution, addition, alteration, vertical partition, invertibility & Mix-Match also has been performed to check the robustness for various applications like database copyright protection, protect valuable numerical relational data from illegal duplication and redistribution.

Guo et al.[20] suggested a twice-embedding approach that uses a fingerprinting solution that acts as a guard to valuable numeric relational data against illegal replications and redistribution. In the principal embedding method, they embed a fingerprint that is unique to recognize every beneficiary. The embedding technique is helmed by a secret key. The second implanting method intends to confirm the extricated fingerprint and give a numerical certainty level. The results illustrate that their arrangement is strong and practical to distinctive attacks.

Zhou et al. [113] proposed a strategy named WDI (Watermarking Databases utilizing Image) i.e. BMP Bit Map Image embedding in the RDBMS to guarantee information's copyrights. The robustness of the algorithm was progressed utilizing BCH (Bose Chaudhuri-Hocquenhem) coding. Moreover, a Trusted Third Party (TTP), is used to embed and recognize the watermark. Besides, they look at the flexibility of the algorithm hypothetically depends upon the principles of insights in detail. Tests illustrated the strategy proposed is robust to various sorts of attacks with the objective that the copyrights can be effectively guaranteed.

Gross-Amblard [19] suggested a Query-preserving technique applicable to databases and XML pages. They first saw that unrestricted databases cannot be watermarked while protecting trivial parametric queries. Here, theauthor has proved that watermarking on the arbitrary instances is not possible.

Unnikrishnan & Pramod[98] suggested a method that relies on a hybrid algorithm HOLPSOFA for relational databases. HOLPSOFA is a mix of Orthogonal Learning Particle Swarm Optimization (OLPSO) & Fiery Algorithm (FA). This methodology joins the benefits of FA & OLPSO, which can discover the optimal-time results at the same time. The relational database watermarking method comprises three phases, (i) Optimal area ID

Table 8 Summary of recent state-of-the-art of graphics watermarking techniques

Ref. no.	Purpose	Techniques Used	Input	Performance metrics	Attack Performed	Remark
[15]	address the problem of watermarking multiple lines	analysis of the statistics of the Fourier descriptors)	different graphics files	Detection error probabilities and ROC curves	Translations, rotations, Gaussian noise, low-pass filter	– the algorithm is not sufficiently robust to polygonal line simplification (vertex removal)
[49]	To authenticate 2D vector graphics	principle of predation using spider web	Five testing 2D vector graphics	RMSE, MSDM (mesh structural distortion measure), PSNR, detection rate	scaling, rotation, translation, and entity rearrangement.	-first attempt to use bionic spider web for data integrity authentication
[107]	to address embedding-limitation problem	reversible watermark scheme based on IQIM and IDE	50 different 2-D CAD engineering graphics (in DWG format)	RMSE, NC, bit/vertex	translation, rotation, scaling	-extracted watermark will be different from the original watermark due to combining IQIM with IDE techniques
[67]	authenticate the integrity of 2D CAD engineering graphics	reversible watermarking method based on iterative embedding and virtual coordinates	50 2D CAD engineering graphics	RMSE, NC, bit/vertex	translation, rotation, scaling	- proposed scheme can be used in content authentication and secret communication in 2D CAD engineering graphics.

through1 HOLPSOFA algorithm (ii) Watermark inserting and (iii) watermark extraction. They also compared the HOLPSOFA algorithm with OLPSO and FA. NC and MSE are used for the performance analysis of watermarking. This is a robust strategy and can withstand different types of attacks like insertion, alteration deletion, etc.

Gupta & Pieprzyk [21] has presented a blind and reversible watermarking model. The capacity of the presented watermarking technique is high and is having the attack resistance probability in between 89 and 98 percent. Here, to achieve reversibility authors utilize difference expansion on integers.

Perez Gort [68] devised a watermarking technique based on the AHK algorithm for the database to increase the embedding capacity of the watermark. Here, Attribute Fraction is used to reduce the number of marked tuples. The author has improved the embedding capacity with this scheme.

Pournaghshband [69] has proposed an effective watermarking framework for relational information that's vigorous against different attacks. Whereas past strategies have stressed around bringing errors into the real data, this technique inserts unused tuples ("fake" tuples), to the relation and it acts as watermarks. In comparison with the previous approaches presented insertion algorithm is probabilistic and the detection algorithm is somewhat deterministic.

Agrawal et al. [3] projected a watermarking methodology for relational data. This strategy ensures that some bit places of a few of the properties of a parcel of the tuples embrace specific values. Explicit bit places and values are chosen algorithmically under the influence of a secret key. This watermarking strategy has four essential tunable parameters. Authors, using DB2 showed that the presented scheme can be used for real-time applications.

Khanduja [35] in this work has focused on security analysis of the work done in the field of database watermarking techniques. Here author has categorized the watermarking systems into four kinds, (i) ATSASB (all tuples, single attribute and single bit), (ii) MTSASB (multiple tuples, single attribute and single bit), (iii) MT- SAMB (multiple tuples, single attribute, and multiple bits) and (iv) MTMAMB (multiple tuples, multiple attributes, and multiple bits. The author has analyzed the security of the watermarking scheme hypothetically investigated its reliance on different parameters :(i) N_r, (ii) M_t, (iii) L_{pa}, (iv) N_{pa}.

Summary of the recent state-of-the-art Database watermarking techniques is depicted in Table 9.

4.7 Limitation and Challenges of Watermarking

In the last two decades, lots of work has been done in the field of watermarking. But still, there are various limitations and challenges in the development of watermarking techniques. In this section, the various limitations and challenges of watermarking are discussed.

Robustness, imperceptibility, payload, and computational cost are the major features of watermarking. There is always a trade-off between these features. It is practically impossible to design a watermarking system to address all these watermarking features[95]. Also, it is practically not possible to develop a distinct system robust to all the well-known attacks at the same time [29, 95]. The development of watermarking scheme to address satisfy these tradeoff is the main challenge [61]. The reversible watermarking field lacks benchmarking tools for its evaluation[34]. Also, there are no industry-wide standards for watermarking in the DRM application[33]. Watermark based forensic techniques had alimitation that watermarks need to be embedded in the multimedia before distribution. The spatial domain watermarking scheme is commonly used for authentication. But, poor robustness against the various attacks is its major drawback[30, 100, 108]. A block-based watermarking scheme is

Table 9 Summary of recent state-of-the-art of Database watermarking techniques

Ref. no.	Purpose	Techniques Used	Input	Performance metrics	Attack Performed	Remark
[20]	solution to protect valuable numeric relational data from illegal duplications and redistributions.	twice-embedding method that uses fingerprinting solution	Forest Cover Type dataset (first 5,000 tuples)	Numerical Certainty Level	Subset selection attack, Subset addition attack, Subset alteration attack	Three algorithm has been used here i.e twice-embedding algorithm, fingerprint extraction algorithm and fingerprint verification algorithm.
[113]	Databases' Copyrights Protection	An Additive-attack-proof Watermarking Mechanism(WDI, BCH, TTP)	RDBMS PostgreSQL 8.1.3	PSNR, Alteration Ratio	Selection and Verticle Partition Attacks, Addition Attack, Alteration Attack, Additive / Invertibility-Attack	-Uses TTP (Trusted Third Party) -Flexible algorithm
[19]	Querypreserving Watermarking of Relational Databases and XML Documents	Query-preserving Watermarking	RDBMS & XML Doc	————————	————————	Incremental aspect of query-preserving watermarking has been considered.
[98]	Robust optimal position detection scheme for relational database watermarking through HOLPSOFA algorithm	HOLPSOFA algorithm (Robust optimal position detection scheme (RTI))	relational database	MSE, NC	Deletion , insertion, Alteration attack.	-An embedding position selection algorithm is proposed to improve the relational water- marking scheme through optimization problem

Table 9 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance metrics	Attack Performed	Remark
[21]	Copyright protection of database	Reversible And Blind Database Watermarking Using Difference Expansion	1000 Files having 200 to 300 tuples, 10 to 20 attributes each	Capacity	Random bitwise Flipping attack, Subtractive attack, Sorting and Secondary watermarking attack	difference expansion on integers is used to achieve reversibility The worst case scenario occured when the attacker modified 48 out of every 100 tuples
[68]	Relational data copyright protection	a nobel high capacity & multi-attribute image- based watermarking	Forest Cover Type relational dataset 581,012 tuples with 54 attributes	CF	tuples addition & deletion attack.	-Follows client-server Architecture - Uses Attribute Function To decrease marked tuples
[69]	Copyright protection of database	Based on AHK algorithm and AF	Database	Similarity Score	Basic Attacks, False Claim of Ownership. Updatability, Sensitivity, Multiple Public Verifiability, Proof of Ownership, Subset of Attributes Attack.	This approach concentrate on tuples with their entirety rather than a subset of their attributes.

Table 9 (continued)

Ref. no.	Purpose	Techniques Used	Input	Performance metrics	Attack Performed	Remark
[3]	effective watermarking technique geared for relational data.	Cryptographic pseudorandom sequences	Forest Cover Type data set 581,012 rows, each with 61 attributes	False hits	Subsetting attacks, Bit-flipping attacks, Mix-and-match attack, False claims of ownership.	v Whether a tuple is marked or not depends only on its primary key attribute. The detection algorithm is blind Implementation has been done on DB2.
[35]	security analysis of the work done so far	Database watermarking	————————	False hit rate & False miss rate	————————	Increase in the number of tuples causes increase in the number of potential locations thus; probability to detect them correctly further decreases in all four cases. For a secure system, this probability should be least

having disadvantages that it is unable to embed a watermark in all the blocks, which leads to low capacity. Recently, several works have been done in the frequency domain. But the high computational cost and low payload capacity is its major limitation [65, 89, 96]. Also, the DWT watermarking suffers from three major drawbacks (i.e. poor directional information, shift sensitivity, and lack of phase information), whereas false-positive problems and higher computational cost are the main drawbacks of the SVD-based watermarking[72]. The selection of optimal scaling factors is the major challenge in DWT as well as SVD based watermarking techniques[24, 100, 104]. Also, the DWT based scheme suffers from rotation attacks. Payload or capacity is the main limitation of the video watermarking scheme. In the visible watermarking scheme, the watermark is visible in the watermarked signal (image, video, and graphics). Visible watermarking can be effortlessly tampered by the attackers with the use of image processing mechanisms [18]. For a 2- D CAD engineering graphics IQIM based scheme is commonly used. The major drawback of the IQIM based scheme is that not every vertex is embeddable[107]. For audio, SS based watermarking is commonly used. A drawback of this technique is the host signal interference problem[105]. This drawback could significantly lower the robustness of watermark extraction. The robustness of audio watermarking against recapturing and desynchronization is still a challenging issue[53]. The study reveals that the main constraint of the existing audio watermarking methods is the difficulty to achieve a favorable trade-off among imperceptibility, robustness, and data payload[14]. Watermarking text on Social Media is having alimitation and specific requirements[75]. The watermark should preserve the length as well as the content of the original text without converting the text into the images. Watermarking natural language is still a challenge in the domain of digital watermarking. Multi-attribute techniques, a common limitation is that often they define a fixed number of attributes for embedding the marks[68]. Large volume and redundant data is the major challenge for database watermarking [35]. Difference expansion based watermarking techniques is one of the major watermarking technique for database and is unable to increase the capacity of the relation without distortion tolerance.

5 Performance Measures in Digital Watermarking

Performance metrics are required for calculating or verifying the effectiveness of watermarking techniques[41, 43, 64]. Some of them are given below:-

Mean Squared Error (MSE) is used to verify mutilations between cover image & watermarked image. This helps to recognize any alteration within the watermarked image.

$$M.S.E = \frac{1}{n}\sum_{i=1}^{n}(A_i - A_i^*)^2 \tag{1}$$

Here A signifies the cover image and A* signifies the watermarked data.

Euclidean distance (ED) In a Euclidean space, it is the common distance between two points. Two-dimensional Euclidean distance is utilized for images. The Euclidean distance between two images is given by: -

$$ED(A, A') = \sum_{i=1}^{M}\sum_{j=1}^{N}(A_{(i,j)} - A'_{(i,j)})^2 \tag{2}$$

Peak-Signal-to-Noise Ratio PSNR utilizes mean squared error to check bending between the watermarked and cover image. PSNR can be calculated by the below mentioned formula. It is widely used to investigate reformation of lossy images. Image is the information here while noise is the error.

$$PSNR = 10log_{10}\left(\frac{MAX_i^2}{MSE}\right) \tag{3}$$

Normalized Correction Normalized correction is a measure of the degree of similitude of two images as a function of a time-lag connected to one of them. The following equation is utilized to calculate normalized correction for two images.

$$NC(A, A') = \sum_{i}^{M}\sum_{j}^{N}\frac{A_{(i,j)} * A'_{(i,j)}}{\sum_{i}^{M}\sum_{j}^{N}(A_{(i,j)})^2} \tag{4}$$

Hamming distance (HD) is applicable for binary images. It can be utilized to measure the exactness of recouped watermark quantitatively. There equations are given underneath. Here, B= original image & B' = processed image, M = width of the image & N = height of the image B (i, j) = pixel position at (i, j) location of B & B' (i, j) = pixel position at (i, j) location of Y'.

$$HD(B, B') = \sum_{i}^{M}\sum_{j}^{N}|B_{(i,j)} - B'_{(i,j)}| \tag{5}$$

Bit error rate (BER) BER is used for binary images. It is utilized to measure the exactness of recuperated watermark quantitatively. There equations are given underneath. Here, B = original image & B' = processed image, M = width of the image & N = height of the image B (i, j) = pixel position at (i, j) location of B & B' (i, j) = pixel position at (i, j) location of Y'.

$$BER(B, B') = \frac{HD(B, B')}{M * N} * 100\% \tag{6}$$

Image Fidelity (IF) IF decides the likeness between the watermarked and un-watermarked image. Higher the IF, the more imperceptible the implanted information is within the watermarked picture.

Bit correction rate (BCR) It is also used for binary images. It can be utilized to degree the precision of recouped watermark quantitatively. There equations are given underneath. Here, B = original image & B' = processed image, M = width of the image & N = height of the image B (i, j) = pixel position at (i, j) location of B & B' (i, j) = pixel position at (i, j) location of B'.

$$BCR(B, B') = \left(1 - \frac{HD(B, B')}{M * N}\right) * 100\% \tag{7}$$

Structural Similarity Index (SSIM) SSIM is used to measure the similitude between two images on the basis of their structure. The basic discernment is made based on pixels inter-dependence with its neighboring pixels. It is better than PSNR & MSE. Neighboring pixels contain critical data in regards to the structural composition of the image.

$$SSIM(a, b) = \frac{(2\mu_a\mu_b + c_1)(2\sigma_{ab} + c_2)}{(\mu_a^2 + \mu_b^2 + c_1)(\sigma_a^2 + \sigma_b^2 + c_2)} \tag{8}$$

$\mu_a$the average of x & μ_b the average of y.
$\sigma_a^2$the variance of a & σ_b^2 the variance of b,
σ_{ab}^2 the covariance of a and b.
$c_1 = (k_1 L)^2$, $c_2(k_2 L)^2$ two variables to stabilize the
division with weak denominator

6 Attacks on Watermarking.

One of the significant characteristics of any watermarking scheme is its robustness against attack. With regard to watermarking, an attack is anything that will harm or debilitate the discovery of the watermark. The processed watermarked information is at that point named as attacked information. In spite of the fact that accomplishing robustness against attacks remains an open issue, a few strategies can survive worldwide attacks. Effective strategies, for the most part, depend on i) embedding data in a space that's invariant to geometric attacks, ii) utilizing layouts, iii) utilizing self-synchronizing watermarks, or iv) utilizing highlight points to realize synchronization.

Watermark attack can be broadly classified into 4 categories namely, removal, geometry, protocol, and cryptographic[39, 86, 103]. These are again subdivided into other sub-classes (Fig. 3).

6.1 Removal Attack

Removal attack aims at the total expulsion of the watermark data without breaking the security of the watermarking algorithm. Advanced removal attacks attempt to optimize operations like quantization or de-noising to impede the inserted watermark as much as conceivable while preserving the quality of the attacked document. Removal attacks can be divided into 4 categories namely Sharpen, Blur, Median Filter, & Noise. The noise can further be classified as, Gaussian noise, Salt & pepper noise, Poisson noise, and Speckle noise.

6.2 Geometry Attack

Geometry attack does not essentially apportion with the watermark itself but it mutilates the watermark locator synchronization with the embedded data. Each geometric attack is characterized by a set of parameters that regulates the operation on the target. Geometry attack can be gathered into 4 classes specifically Rotation, Scaling, Translation, and Cropping.

6.3 Protocol Attack

In a protocol attack, the attacker adds his own watermark to the host data. Such attacks pose a threat to modern digital systems. Examples include the replication of a valid watermark to name a few. Protocol attacks are of 2 types – Invertible & Copy Attack.

6.4 Cryptographic Attack

Cryptographic attacks aim to break the security provided by watermarking. They may be of two types namely Oracle & Brute-Force.

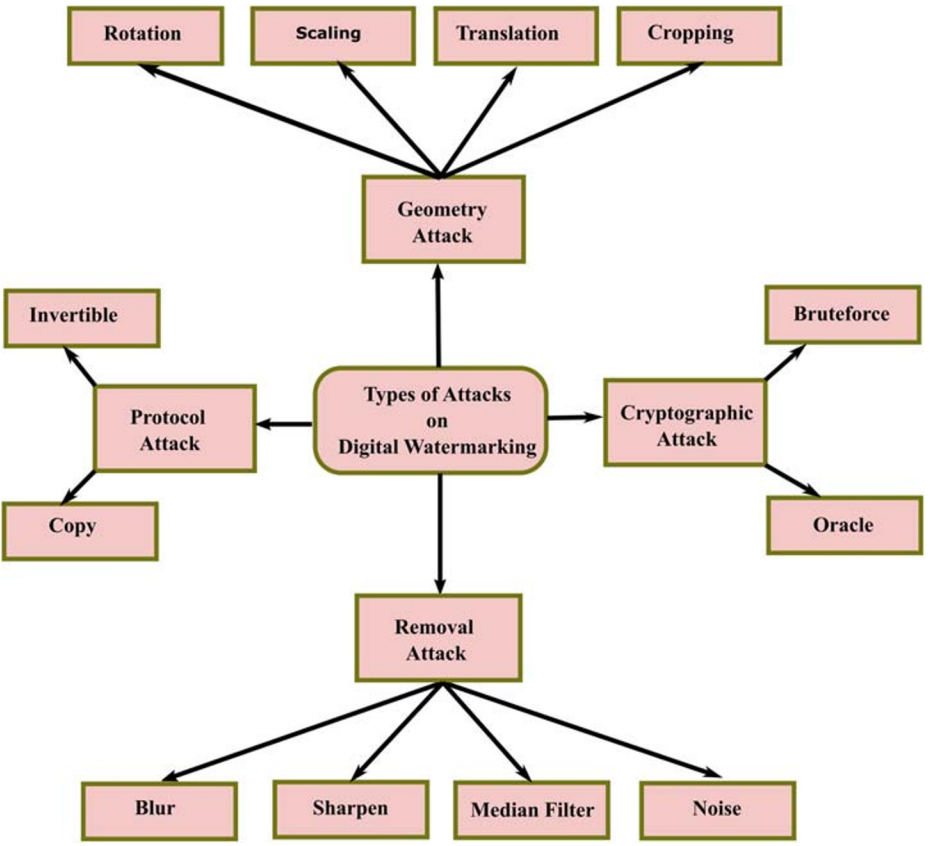

Fig. 3 Attacks on watermarking

Oracle attack: Oracle attack was first introduced by Vaude-nay at Euro Crypt '02. In this, the attack works under the impression of an Oracle which on an encounter of a ciphertext, decrypts it and sends a valid or invalid reply to the sender. It assumes that the attackers can retrieve the padded messages encrypted in CBC mode and have access to the padding oracle. As a result, the attacker can recuperate the plaintext in regard to the cipher content utilizing approx.128b oracle calls, where b suggests a number of bytes in a block. Brute force attack: In this attack, the impersonator tries all possible keys to decrypt the message. It is also known as an exhaustive key search. The amount of time needed to decipher a cipher is proportional to the secret key size. Another kind of attack is a dictionary attack where the impersonator tries to make a guess of the password by using popular expressions or existing words.

7 Conclusion & Future Direction

In this work, we have presented a brief overview of watermarking systems. We have also presented the detailed classification of the watermarking which has been done by the various

researcher. Further, this paper presents the various features of the watermarking approach followed by the summary of various state-of-the-art watermarking approaches and the various attacks on watermarking.

Based on the extensive discussion in the previous sections, it has been found that there is a trade-off between the various features of watermarking. In a single watermarking scheme it is very difficult to address these trade-off issues. The researcher can work to develop a watermarking technique to address these trade-offs. Also, the reversible watermarking field lacks benchmarking tools for its evaluation. The researcher can work for the development of a benchmarking tool to evaluate the reversible watermarking techniques. In image watermarking, the possible research area includes, real-time implementation of watermark, blind watermark detector, better perceptual model, and dual watermarking techniques. In image watermarking, the security of the watermark is given less priority by the researcher in comparison to other features. So, the researcher can also work on the improvement of watermark security. In the area of video watermarking, theresearcher should work to shorten the operation time and to meet the real-time requirements. At the present time, 3D printing models are becoming more popular and commonly used in applications such as medicine, manufacturing, architecture, end-user parts, product development, etc. Also, very few watermarking schemes is available for the animation so, the researcher may work in this area. In, audio watermarking, attacks such as TSM and cropping are prominent challenges for theresearcher. Lots of work, is needed to overcome this challenge. In database watermarking scheme computational time and robustness zero distortion in original data is the prime concern. Text watermarking scheme is generally applied to a particular alphabets only. This diminishes the usability and suitability of the text watermarking scheme. Text watermarking should be applicable to any kind of text. The researcher can identify and proposed an adequate scheme to resolve these issues. Authors believe that this survey paper is helpful for the researcher to work in the direction of data authentication, security and copyright protection of multimedia and databases.

Acknowledgment The authors would like to thank reviewers for their helpful comments. We would also like to thanksthe Ministry of Human Resource Development, India and the National Institute of Technology, Jamshedpur for financial assistance.

References

1. Agarwal H, Raman B, Venkat I (2015) Blind reliable invisible watermarking method in wavelet domain for face image watermark. Multimedia Tools and Applications 74(17):6897–6935
2. Agarwal N, Singh AK, Singh PK Survey of robust and imperceptible watermarking. Multimedia Tools and Applications pp. 1–31
3. Agrawal R, Haas PJ, Kiernan J (2003) Watermarking relational data: framework, algorithms and analysis. The VLDB Journal—The International Journal on Very Large Data Bases 12(2):157–169
4. Akhtar Z, Khan E (2016) Identifying high quality jpeg compressed images through exhaustive recompression technique. In: 2016 International conference on advances in computing, communications and informatics (ICACCI), pp. 652–656. IEEE
5. Akhtar Z, Khan E (2017) Revealing the traces of histogram equalisation in digital images. IET Image Process 12(5):760–768
6. Al-Sewadi HA, Aldakari ANA (2018) Improved processing speed for text watermarking algorithm in color images. In: Proceedings of the 8th International Conference on Information Systems and Technologies, p. 7. ACM
7. Ali Z, Imran M, Alsulaiman M, Zia T, Shoaib M (2018) A zero-watermarking algorithm for privacy protection in biomedical signals. Futur Gener Comput Syst 82:290–303

8. Alotaibi RA, Elrefaei LA (2018) Improved capacity arabic text watermarking methods based on open word space. Journal of King Saud University-Computer and Information Sciences 30(2):236–248
9. Alromih A, Al-Rodhaan M, Tian Y (2018) A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for internet of things applications. Sensors 18(12):4346
10. Asikuzzaman M, Alam MJ, Lambert AJ, Pickering MR (2014) Imperceptible and robust blind video watermarking using chrominance embedding: a set of approaches in the dt cwt domain. IEEE transactions on Information Forensics and Security 9(9):1502–1517
11. Cedillo-Hernandez A, Cedillo-Hernandez M, Miyatake MN, Meana HP (2018) A spatiotemporal saliency-modulated jnd profile applied to video watermarking. J Vis Commun Image Represent 52:106–117
12. Chen J, Yang F, Ma H, Lu Q (2016) Text watermarking algorithm based on semantic role labeling 2016 Third international conference on digital information processing, data mining, and wireless communications (DIPDMWC), pp. 117–120. IEEE
13. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) Digital watermarking and steganography Morgan kaufmann
14. Dhar PK, Shimamura T (2015) Blind svd-based audio watermarking using entropy and log-polar transformation. Journal of Information Security and Applications 20:74–83
15. Doncel VR, Nikolaidis N, Pitas I (2007) An optimal detector structure for the fourier descriptors domain watermarking of 2d vector graphics. IEEE Trans Vis Comput Graph 13(5):851–863
16. Fallahpour M, Megías D (2015) Audio watermarking based on fibonacci numbers. IEEE Transactions on Audio Speech, and Language Processing 23(8):1273–1282
17. Farri E, Ayubi P (2018) A blind and robust video watermarking based on iwt and new 3d generalized chaotic sine map. Nonlinear Dynamics 93:1875–1897
18. Gangadhar Y, Akula VG, Reddy PC (2018) An evolutionary programming approach for securing medical images using watermarking scheme in invariant discrete wavelet transformation. Biomedical Signal Processing and Control 43:31–40
19. Gross-Amblard D (2011) Query-preserving watermarking of relational databases and xml documents. ACM Transactions on Database Systems (TODS) 36(1):3
20. Guo F, Wang J, Li D (2006) Fingerprinting relational databases. In: Proceedings of the 2006 ACM symposium on Applied computing, pp. 487–492. ACM
21. Gupta G, Pieprzyk J (2008) Reversible and blind database watermarking using difference expansion. In: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, p 24, ICST (Institute for Computer Sciences, Social-Informatics and ···
22. Halvani O, Steinebach M, Wolf P, Zimmermann R (2013) Natural language watermarking for german texts. In: Proceedings of the first ACM workshop on Information hiding and multimedia security, pp. 193–202. ACM
23. Horng SJ, Farfoura ME, Fan P, Wang X, Li T, Guo JM (2014) A low cost fragile watermarking scheme in h. 264/avc compressed domain. Multimedia Tools and Applications 72(3):2469–2495
24. Horng SJ, Rosiyadi D, Fan P, Wang X, Khan MK (2014) An adaptive watermarking scheme for e-government document images. Multimedia tools and applications 72(3):3085–3103
25. Horng SJ, Rosiyadi D, Li T, Takao T, Guo M, Khan MK (2013) A blind image copyright protection scheme for e-government. Journal of Visual Communication and Image Representation 24(7):1099–1105
26. Hossain MS, Muhammad G, Abdul W, Song B, Gupta B (2018) Cloud-assisted secure video transmission and sharing framework for smart cities. Futur Gener Comput Syst 83:596–606
27. Hu HT, Chang JR, Lin SJ (2018) Synchronous blind audio watermarking via shape configuration of sorted lwt coefficient magnitudes. Signal Process 147:190–202
28. Hua G, Goh J, Thing VL (2015) Time-spread echo-based audio watermarking with optimized imperceptibility and robustness. IEEE/ACM Transactions on Audio. Speech, and Language Processing 23(2):227–239
29. Hua G, Zhao L, Zhang H, Bi G, Xiang Y (2018) Random matching pursuit for image watermarking. IEEE Transactions on Circuits and Systems for Video Technology 29(3):625–639
30. Huynh-The T, Hua CH, Tu NA, Hur T, Bang J, Kim D, Amin MB, Kang BH, Seung H, Lee S (2018) Selective bit embedding scheme for robust blind color image watermarking. Inf Sci 426:1–18
31. Hwang MJ, Lee J, Lee M, Kang HG (2017) Svd-based adaptive qim watermarking on stereo audio signals. IEEE Transactions on Multimedia 20(1):45–54
32. Jain R, Trivedi MC, Tiwari S (2018) Digital audio watermarking: a survey. In: Advances in computer and computational sciences, pp. 433–443. Springer

33. Khan A, Jabeen F, Naz F, Suhail S, Ahmed M, Nawaz S (2016) Buyer seller watermarking protocols issues and challenges–a survey. J Netw Comput Appl 75:317–334
34. Khan A, Siddiqa A, Munib S, Malik SA (2014) A recent survey of reversible watermarking techniques. Information sciences 279:251–272
35. Khanduja V (2017) Database watermarking, a technological protective measure: Perspective, security analysis and future directions. Journal of information security and applications 37:38–49
36. Kumar C, Singh AK, Kumar P (2018) A recent survey on image watermarking techniques and its application in e-governance. Multimedia Tools and Applications 77(3):3597–3622
37. Kumar S, Dutta A (2016) A novel spatial domain technique for digital image watermarking using block entropy. In: 2016 International conference on recent trends in information technology (ICRTIT), pp. 1–4. IEEE
38. Kumar S, Dutta A (2016) Performance analysis of spatial domain digital watermarking techniques. In: 2016 International conference on information communication and embedded systems (ICICES), pp. 1–4. IEEE
39. Kumar S, Dutta A (2016) A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks. In: 2016 IEEE International conference on recent trends in electronics, information & communication technology (RTEICT), pp. 1802–1806. IEEE
40. Kumar S, Singh BK (2018) A review of digital watermarking in healthcare domain. In: 2018 3Rd international conference on computational systems and information technology for sustainable solutions (CSITSS), pp. 156–159. IEEE
41. Kutter M, Petitcolas FA (1999) Fair benchmark for image watermarking systems. In: Security and watermarking of multimedia contents, vol. 3657, pp. 226–240. International society for optics and photonics
42. Lai CC (2011) A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Processing 21(4):522–527
43. Laouamer L, Tayan O (2018) Performance evaluation of a document image watermarking approach with enhanced tamper localization and recovery. IEEE Access 6(26):144–26,166
44. Lei B, Zhou F, Tan EL, Ni D, Lei H, Chen S, Wang T (2015) Optimal and secure audio watermarking scheme based on self-adaptive particle swarm optimization and quaternion wavelet transform. Signal Process 113:80–94
45. Lin WH, Horng SJ, Kao TW, Chen RJ, Chen YH, Lee CL, Terano T (2009) Image copyright protection with forward error correction. Expert systems with applications 36(9):11,888–11,894
46. Lin WH, Horng SJ, Kao TW, Fan P, Lee CL, Pan Y (2008) An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Transactions on Multimedia 10(5):746–757
47. Lin WH, Wang YR, Horng SJ (2009) A wavelet-tree-based watermarking method using distance vector of binary cluster. Expert Syst Appl 36(6):9869–9878
48. Lin WH, Wang YR, Horng SJ, Kao TW, Pan Y (2009) A blind watermarking method using maximum wavelet coefficient quantization. Expert Systems with Applications 36(9):11,509–11,516
49. Lin ZX, Peng F, Long M (2017) A reversible watermarking for authenticating 2d vector graphics based on bionic spider web. Signal Processing:, Image Communication 57:134–146
50. Liu X, Zhang J, Wang H, Gong X, Cheng Y (2014) A novel text watermarking algorithm based on graphic watermarking framework. In: 2014 Ninth international conference on broadband and wireless computing, communication and applications, pp. 84–88. IEEE
51. Liu X, Zhao R, Li F, Liao S, Ding Y, Zou B (2017) Novel robust zero-watermarking scheme for digital rights management of 3d videos. Signal processing:, Image communication 54:140–151
52. Liu Y, Tang S, Liu R, Zhang L, Ma Z (2018) Secure and robust digital image watermarking scheme using logistic and rsa encryption. Expert Syst Appl 97:95–105
53. Liu Z, Huang Y, Huang J (2018) Patchwork-based audio watermarking robust against de-synchronization and recapturing attacks. IEEE Transactions on Information Forensics and Security 14(5):1171–1180
54. Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access 6(19):876–19,897
55. Loganathan A, Kaliyaperumal G (2016) An adaptive hvs based video watermarking scheme for multiple watermarks using bam neural networks and fuzzy inference system. Expert Syst Appl 63:412–434
56. Ma B, Wang Y, Li C, Zhang Z, Huang D (2014) Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. Multimedia tools and applications 72(1):637–666
57. Madine F, Akhaee MA, Zarmehi N (2018) A multiplicative video watermarking robust to h. 264/avc compression standard. Signal Processing:, Image Communication 68:229–240

58. Manikandan V, Masilamani V (2018) Histogram shifting-based blind watermarking scheme for copyright protection in 5g. Computers & Electrical Engineering 72:614–630
59. Memon N, Wong PW (2001) A buyer-seller watermarking protocol. IEEE Transactions on image processing 10(4):643–649
60. Mir N (2014) Copyright for web content using invisible text watermarking. Comput Hum Behav 30:648–653
61. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using dwt–svd and firefly algorithm. Expert Syst Appl 41(17):7858–7867
62. Najih A, Al-Haddad S, Ramli AR, Hashim S, Nematollahi MA (2017) Digital image watermarking based on angle quantization in discrete contourlet transform. Journal of King Saud University-Computer and Information Sciences 29(3):288–294
63. Nezhadarya E, Ward RK (2013) Semi-blind quality estimation of compressed videos using digital watermarking. Digital Signal Processing 23(5):1483–1495
64. Nikolaidis N, Solachidis V, Tefas A, Pitas I (2002) Watermark detection: benchmarking perspectives. In: Proceedings. IEEE international conference on multimedia and expo, vol. 2, pp. 493–496. IEEE
65. Nouioua I, Amardjia N, Belilita S (2018) A novel blind and robust video watermarking technique in fast motion frames based on svd and mr-svd. Security and Communication Networks, Volume 2018, Article ID 6712065, Pages 1–17
66. Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind watermarking technique in dct domain using inter-block coefficient differencing. Digital Signal Processing 53:11–24
67. Peng F, Long Q, Lin ZX, Long M (2019) A reversible watermarking for authenticating 2d cad engineering graphics based on iterative embedding and virtual coordinates. Multimedia Tools and Applications 78(19):26,885–26,905
68. Pérez Gort ML, Feregrino Uribe C, Nummenmaa J (2017) A minimum distortion: High capacity watermarking technique for relational data. In: Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, pp. 111–121. ACM
69. Pournaghshband V (2008) A new watermarking approach for relational data. In: Proceedings of the 46th annual southeast regional conference on XX, pp. 127–131. ACM
70. Preda RO, Vizireanu DN (2010) A robust digital watermarking scheme for video copyright protection in the wavelet domain. Measurement 43(10):1720–1726
71. Qin C, Wang H, Zhang X, Sun X (2016) Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode. Inf Sci 373:233–250
72. Rai A, Singh HV (2018) Machine learning-based robust watermarking technique for medical image transmitted over lte network. J Intell Syst 27(1):105–114
73. Rasti P, Samiei S, Agoyi M, Escalera S, Anbarjafari G (2016) Robust non-blind color video watermarking using qr decomposition and entropy analysis. J Vis Commun Image Represent 38:838–847
74. Renza D, Lemus C et al (2018) Authenticity verification of audio signals based on fragile watermarking for audio forensics. Expert Syst Appl 91:211–222
75. Rizzo SG, Bertini F, Montesi D, Stomeo C (2017) Text watermarking in social media. In: Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, pp. 208–211. ACM
76. Rosiyadi D, Horng SJ, Fan P, Wang X, Khan MK, Pan Y (2011) Copyright protection for e-government document images. IEEE MultiMedia 19(3):62–73
77. Rosiyadi D, Horng SJ, Suryana N, Masthurah N (2012) A comparison between the hybrid using genetic algorithm and the pure hybrid watermarking scheme. International Journal of Computer Theory and Engineering 4(3):329
78. Roy R, Ahmed T, Changder S (2018) Watermarking through image geometry change tracking. Visual Informatics 2(2):125–135
79. Rubio-Hernan J, De Cicco L, Garcia-Alfaro J (2017) On the use of watermark-based schemes to detect cyber-physical attacks. EURASIP Journal on Information Security 2017(1):8
80. Rubio-Hernan J, De Cicco L, Garcia-Alfaro J (2018) Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. Transactions on Emerging Telecommunications Technologies 29(7):e3209
81. Rui X, XiaoJun C, Jinqiao S (2013) A multiple watermarking algorithm for texts mixed chinese and english. Procedia Computer Science 17:844–851
82. Saadi S, Merrad A, Benziane A (2019) Novel secured scheme for blind audio/speech norm-space watermarking by arnold algorithm. Signal Process 154:74–86
83. Sandberg H, Amin S, Johansson KH (2015) Cyberphysical security in networked control systems: an introduction to the issue. IEEE Control Syst Mag 35(1):20–23

84. Sarreshtedari S, Akhaee MA (2015) A source-channel coding approach to digital image protection and self-recovery. IEEE Trans Image Process 24(7):2266–2277
85. Shih FY (2017) Digital watermarking and steganography: fundamentals and techniques CRC press
86. Song C, Sudirman S, Merabti M, Llewellyn-Jones D (2010) Analysis of digital image watermark attacks 2010 7Th IEEE consumer communications and networking conference, pp. 1–5. IEEE
87. Sreenivas K, Prasad VK (2018) Fragile watermarking schemes for image authentication: a survey. International Journal of Machine Learning and Cybernetics 9(7):1193–1218
88. Su Q (2016) Novel blind colour image watermarking technique using hessenberg decomposition. IET image processing 10(11):817–829
89. Su Q, Liu D, Yuan Z, Wang G, Zhang X, Chen B, Yao T (2019) New rapid and robust color image watermarking technique in spatial domain. IEEE Access 7(30):398–30,409
90. Su Q, Niu Y, Wang G, Jia S, Yue J (2014) Color image blind watermarking scheme based on qr decomposition. Signal Process 94:219–235
91. Su Q, Niu Y, Wang Q, Sheng G (2013) A blind color image watermarking based on dc component in the spatial domain. Optik 124(23):6255–6260
92. Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X (2015) Embedding color image watermark in color image based on two-level dct. SIViP 9(5):991–1007
93. Su Q, Yuan Z, Liu D (2018) An approximate schur decomposition-based spatial domain color image watermarking method. IEEE Access 7:4358–4370
94. Sun X, Luo G, Huang H (2004) Component-based digital watermarking of chinese texts. In: Proceedings of the 3rd international conference on Information security, pp. 76–81. ACM
95. Tao H, Chongmin L, Zain JM, Abdalla AN (2014) Robust image watermarking theories and techniques: a review. Journal of applied research and technology 12(1):122–138
96. Thanki R, Dwivedi V, Borisagar K (2017) A hybrid watermarking scheme with cs theory for security of multimedia data Journal of King Saud University-Computer and Information Sciences
97. Thongkor K, Amornraksa T, Delp EJ (2018) Digital watermarking for camera-captured images based on just noticeable distortion and wiener filtering. J Vis Commun Image Represent 53:146–160
98. Unnikrishnan K, Pramod K (2017) Robust optimal position detection scheme for relational database watermarking through holpsofa algorithm. Journal of Information Security and Applications 35:1–12
99. Vahedi E, Zoroofi RA, Shiva M (2012) Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. Digital Signal Processing 22(1):153–162
100. Vaidya P, PVSSR CM (2018) Adaptive, robust and blind digital watermarking using bhattacharyya distance and bit manipulation. Multimedia Tools and Applications 77(5):5609–5635
101. Venugopala P, Sarojadevi H, Chiplunkar NN (2017) An approach to embed image in video as watermark using a mobile device. Sustainable Computing: Informatics and Systems 15:82–87
102. Verma VS, Jha RK (2015) An overview of robust digital image watermarking. IETE Technical review 32(6):479–496
103. Voloshynovskiy S, Pereira S, Pun T, Eggers JJ, Su JK (2001) Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE communications Magazine 39(8):118–126
104. Xiang Y, Natgunanathan I, Guo S, Zhou W, Nahavandi S (2014) Patchwork-based audio watermarking method robust to de-synchronization attacks. IEEE/ACM Transactions on Audio. Speech, and Language Processing 22(9):1413–1423
105. Xiang Y, Natgunanathan I, Peng D, Hua G, Liu B (2018) Spread spectrum audio watermarking using multiple orthogonal pn sequences and variable embedding strengths and polarities. IEEE/ACM Transactions on Audio. Speech and Language Processing (TASLP) 26(3):529–539
106. Xiang Y, Peng D, Natgunanathan I, Zhou W (2011) Effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time-spread echo-based audio watermarking. IEEE Transactions on Multimedia 13(1):2–13
107. Xiao D, Hu S, Zheng H (2015) A high capacity combined reversible watermarking scheme for 2-d cad engineering graphics. Multimedia Tools and Applications 74(6):2109–2126
108. Yassin NI, Salem NM, El Adawy MI (2014) Qim blind video watermarking scheme based on wavelet transform and principal component analysis. Alexandria Engineering Journal 53(4):833–842
109. Yu X, Wang C, Zhou X (2018) A survey on robust video watermarking algorithms for copyright protection. Appl Sci 8(10):1891
110. Yuan XC, Pun CM, Chen CP (2015) Robust mel-frequency cepstral coefficients feature detection and dual-tree complex wavelet transform for digital audio watermarking. Inf Sci 298:159–179
111. Zhang SR, Yao Z, Meng XC, Liu CC (2014) New digital text watermarking algorithm based on new-defined characters. In: 2014 International symposium on computer, consumer and control, pp. 713–716. IEEE

112. Zhang W, Zeng Z, Pu G, Zhu H (2006) Chinese text watermarking based on occlusive components. In: 2006 2Nd international conference on information & communication technologies, vol. 1, pp. 1850–1854. IEEE
113. Zhou X, Huang M, Peng Z (2007) An additive-attack-proof watermarking mechanism for databases' copyrights protection using image. In: Proceedings of the 2007 ACM symposium on Applied computing, pp. 254–258. ACM

Sanjay Kumar is currently pursuing Ph.D. from National Institute of Technology, Jamshedpur in Department of Computer Science & Engineering. His research interest includes Digital Watermarking, Image Forensics and Cryptography.

Binod Kumar Singh received the bachelor's degree from BIT Sindri (Vinoba Bhave University, Hazaribag) Jharkhand in 1995, the M.Tech degree from IIT ROORKEE in 2007, and the Ph.D. degree from IIT ROORKEE in 2016. He is current Associate Professor & Head Department of Computer Science & Engineering. His Research interest includes Image Processing, Computerized Tomography (CT), Computer Networks, and Network Security.

Mohit Yadav is currently pursuing M.Tech from National Institute of Technology, Jamshedpur in Department of Computer Science & Engineering. His area of interest includes Network Security and Image Forensics.