Recent Advances in Transform and Hybrid Domain Digital Watermarking Techniques—A Survey

M. Sajeer, Ashutosh Mishra, and P. S. Sathidevi

Abstract In the older days, watermarking has been extensively used in different forms in diverse fields, mainly to recognize an entity's ownership. At the early stages, its analog rendition has been utilized, like stamps or currencies, perceptible to the users. In the present scenario, the situation changed from analog-to-digital watermarking; mostly, the watermarks are imperceptible to the users, requiring some processing steps to figure out the entity's possession. The processing steps may vary from the type or the application area of the watermark that has been utilized. This paper aims to review the basic idea of digital watermarking techniques, current trends, and future scopes that have been occurred in this area during recent years.

Keywords Digital watermarking · Transform domain schemes · DFT · DCT · DWT · SVD · Hybrid domain schemes

1 Introduction

In the present situation, mostly the data is stored and communicated in digital form. So authenticity has a vital role in identifying the source of data. Digital watermarking resolves this problem [1], which is the technique of inserting data (called watermark) into the original cover or carrier image, and it can extract to verify the authorized creator or provider of the data [2]. It can be perceivable or hidden to the users. A general watermarking approach consists of three processes, watermark creation, watermark implanting, and watermark separation. Watermark creation is the technique of creating a watermark based upon a generation algorithm. The method of hiding a watermark into a host image using an embedding algorithm may define as watermark implanting, and the corresponding image is called a watermarked image. The watermark separation extracts a watermark using an extraction algorithm [3], as shown in Fig. 1. Recently, the watermarking techniques have many potential applications such as ownership authentication, copyright protection, telemedicine,

M. Sajeer (✉) · A. Mishra · P. S. Sathidevi
National Institute of Technology, Calicut, Kerala, India
e-mail: sajeer@sctce.ac.in

G. Ranganathan et al. (eds.), *Soft Computing for Security Applications*,
Advances in Intelligent Systems and Computing 1397,
https://doi.org/10.1007/978-981-16-5301-8_59

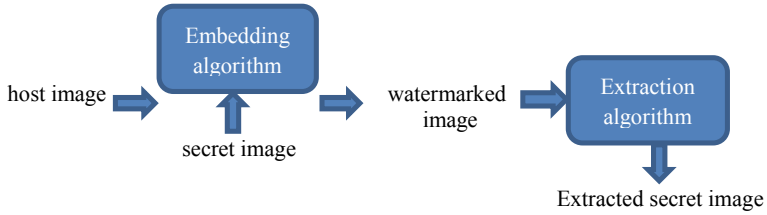

Fig. 1 Watermarking process

electronic governance, media file archiving, web publishing, media forensics, digital libraries, artificial intelligence, military, secure E-voting, different licenses, real-time audio/video, and robotics [4–7].

1.1 Characteristics of a General Watermarking System

There are different characteristics essential for a general watermarking system [8]. Fidelity is an important characteristic, which defines the analogy between the carrier image and the watermarked image [9, 10]. Robustness is the ability to resist different geometric operations and image processing attacks. Data payload (capacity) may be defined as the amount of information present in a watermark [11]. Security is a vital characteristic to identify genuine authors to withstand intentional attacks [12]. Computational complexity explains the total time required for a system to finish watermark embedding and watermark separation processes [13]. Perceptibility is the measurement of distortion in a watermarked image, or it should be invisible to the users [8]. Reversibility outlines the ability to restore the watermark and original image, which is essential for medical applications [14]. Reliability can identify the genuine person to receive the message without data degradation [15].

1.2 Categorization of Digital Watermarking Techniques

Digital watermarking techniques can be categorized as follows [16]. The first classification consists of document, hiding domain, human discrimination, and reversibility [8]. The document type may be image, text, video, or audio. Based on the hiding domain, the watermarking technique is classified into a spatial or transform style. In the spatial method, watermarking is done directly on the host image's pixel values, but in the frequency domain, watermarking performs on the host image's transform coefficients [17]. Invisible (the watermark is invisible to human), visible (the watermark is perceivable), and dual (a combination of visual and hidden) watermarking techniques are coming under human perception [18]. The secret watermarking scheme may be fragile, robust, semi-fragile, or hybrid approaches based on

withstanding image processing attacks and geometrical operations [8]. Reversible (lossless watermarking) and non-reversible (lossy watermarking) techniques are another classification of the watermarking scheme [14].

1.3 Types of Watermarking Attacks

Watermarking attacks are the processes that make alterations to the contents of the watermark by unauthorized users. It may also cause the revealing of the hidden data in a watermark—they include.

Signal Processing Attacks They are also called non-geometrical attacks. It may be due to the addition of noise, and some non-geometrical operations such as histogram equalization and gamma correction.

Geometrical Attacks It includes some geometrical operations such as scaling, rotation, translation, shearing, and cropping.

Cryptographic Attacks Cryptographic attacks usually affect the secret information in the watermark.

Protocol Attacks These attacks encompass the copy and protocol attacks, where the interferer will try to change the watermarks in the data.

1.4 Performance Measurement in Watermarking System

There are different matrices to assess the potential of a watermarking system. They compare the cover image and the watermarked image. They include:

Mean Square Error or MSE [19]—It is the average squared error between the original image and the watermarked image. Its value should be deficient. Ideally, its value is zero.

Peak Signal-to-Ratio or PSNR [20]—The ratio of signal-to-noise measures the watermarked image's visual quality. Usually, its value will be high (generally more than 30 dB), which is the measure of similarity between the watermarked and host image.

Normalized Coefficient or NC [20]—It finds the compatibility between embedded and extracted watermark. Its value comes between zero and one. Ideally, it is one.

Structural Similarity Index or SSIM [20]—This shows the closeness of the original and watermarked image. The value of SSIM varies from -1 to $+1$. Ideally, it is $+1$.

Bit Error Ratio or BER [21]—The ratio of the number of received bits as the error to the binary sequence's total length in a watermark. Its value should be low, and ideally, it is zero.

UACI and NPCR [22]—UACI is the unified averaged changed intensity, NPCR is the pixel changing rate used to investigate encryption algorithms' performance against different attacks. Ideally, their value is very high.

The rest of the paper is described as follows: Section 2 explains different domain schemes used in digital watermarking, mainly various transform domains and different hybrid domain techniques; challenges in watermarking domains are presented in Sect. 3. The conclusion summarizes the survey.

2 Survey of Different Watermarking Schemes

Based on the domain, the watermarking technique may be spatial or transform type. The spatial domain schemes have advantages like a high payload, less computational complexity, and less processing time, but they have less imperceptibility and less robustness against watermarking attacks. LSB or least significant bit technique, correlation-based methods, patchwork methods, spread spectrum methods, etc., are coming under this scheme. Transform domain techniques such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD) are having advantages like high imperceptibility and very high robustness against attacks. Disadvantages of these methods are less watermarking capacity, high computational complexity, and increased processing time. Most of the researchers are currently using hybrid approaches, which combine the above transform domain methods based on the applications [22].

2.1 Transform Domain Watermarking Schemes

There are distinct transform domain schemes introduced by various authors like [23–35], and their observations are summarized in Table 1.

Andalibi and Chandler [23] proposed a DWT domain invisible watermarking process using adaptive logo texturization. Initially, the carrier image is separated into a sufficiently textured area and a poorly textured region using the ALT-MARK algorithm. Then modified the watermark into a perceptibly similar structure as that of a carrier image using the methods like Arnold transform, lossless rotation. For every blocks, inserted the modified watermark into that region using the DWT technique. An affine parameter is utilized to withstand geometrical transformations. The process measured the PSNR for checking the imperceptibility and obtained values varying

Table 1 Summary of transform domain watermarking techniques

Refs	Techniques/algorithms performed	Cover image/watermark specifications	Dataset used	Attacks handled	Area of application
[23]	DWT, ALT-MARK algorithm, Arnold transform	512 × 512 (gray), 64 × 64 (gray)	CSIQ	AGN, JPEG, HE, BR, RO, SC, CR, CMB	Logo watermarking
[24]	IWT	265 × 190 (gray), --	CT, MRI and PET images	AGN, S&P, JPEG, LPF	Tamper detection in ROI of medical images
[25]	DCT, Visual cryptography	--, 64 × 64 text image	CASIA V4,UBIRIS V1	AGN, MF, HE, JPEG, S&P, CR	Iris biometric protection
[26]	Hessenberg decomposition, Arnold transform	512 × 512 (color), 32 × 32 (color)	CVG-UGR	AGN, JPEG, S&P, MF, BLPF, SC, BR, RO	Copyright protection of color image
[27]	DCT	512 × 512 (gray), –	–	AGN, JPEG, SC, CLC	Image watermarking
[28]	DCT, Fractal encoding	1024 × 1024 (gray), 256 × 256 (gray)	–	WN, JPEG, GF	Image watermarking
[29]	DCT	512 × 512 (gray), 32 × 32 (binary)	–	AGN, MF, WF, AF, GLP, HE, JPEG, S&P, SN, PN, CR, SC, SH, CMB	Copyright protection
[30]	Ripplet-II transform, DFT	512 × 512 (Gray), 256 × 256 (binary)	USC-SIPI	AGN, MF, GLP, HE, JPEG, S&P, SN, CR, SH, RO, TR	Copyright protection

(continued)

Table 1 (continued)

Refs	Techniques/algorithms performed	Cover image/watermark specifications	Dataset used	Attacks handled	Area of application
[31]	DCT	512 × 512 (color), 32 × 32 (binary)	CVG–UGR, USC-SIPI	AGN, JPEG, MF, S&P, AF, GLP, SC, CR	Logo watermarking
[32]	DCT, additive watermarking	256 × 256 (gray), 32 × 32 (binary)	–	MF, GF, PN, SN, S&P, JPEG, SH, BR	Logo watermarking
[33]	DCT, Bees algorithm	512 × 512 (gray), 32 × 32 (binary)	–	AGN, MF, AF, GLP, HE, JPEG, S&P, CR, SC, SH, GC, RO	Logo watermarking
[34]	Histogram, HFCM	Gray	–	AGN, JPEG, S&P, MF, SC, SH, RO, CR, BE, JT	Image watermarking
[35]	DCT, QIM-DM	1024 × 728 (color), 64 × 64 (color)	USC-SIPI	AGN, JPEG, AF, MF	Color image watermarking

*Non-geometrical attacks: Additive Gaussian Noise (AGN) [23], JPEG compression (JPEG) [24], Histogram Equalization (HE) [25], Motion Blurring (BR) [26], White noise (WN) [28], Poisson Noise (PN) [32], Salt and Pepper Noise (S&P) [30], Gaussian Filter (GF) [32], Median Filter (MF) [31], Constant Luminance Change (CLC) [27], Weiner Filter (WF) [29], Speckle Noise (SN) [30], Average Filter (AF) [31], Gamma Correction (GC) [33]; Geometrical attacks: Rotation (RO) [33], Scaling (SC) [34], Cropping (CR) [34], Translation (TR) [30], Shearing (SH) [33], Bending (BE) [34], Jittering (JT) [34]; Combinational Attacks (CMB) [29]

*Techniques or algorithms used: Discrete Wavelet Transform (DWT) [23], Integer Wavelet Transform (IWT) [24], Discrete Fourier Transform (DFT) [30], Discrete Cosine Transform (DCT) [31], High-Frequency Component Modification (HFCM [34]), Quantization Index Modulation–Dither Modulation (QIM-DM) [35]

from 29.68 to 44.21 dB for different watermarked images. Robustness is evaluated by applying some non-geometrical attacks like JPEG compression, blurring, and Gaussian noise; geometrical attacks like rotation, scaling, and cropping; and combinational attacks. The method obtained good robustness results for the consecutive attacks (Gaussian noise of density 0.1% + counterclockwise direction of 10° + cropping of 40 pixels from the top and bottom of the image) and significant values for

JPEG compression, and cropping. The scheme has to improve the robustness against attacks like histogram equalization, motion blurring, and rotation.

Easwaraiah et al. [24] developed a novel watermarking method for medical images based on an integer wavelet transform (IWT). Medical images consist of region of non-interest (RONI) and region of interest (ROI) regions. In this method, the watermark, which consists of patient data, the hash value of ROI, and recovery data of ROI, is inserted in the RONI region using Cohen–Daubechies–Fauraue IWT. When an attacker tampers the ROI, the receiver can reconstruct it using the RONI watermark. In this method, a rectangle-shaped ROI of size 3×3 is used, marked by the physician. The process has experimented with CT, MRI, Ultrasound, PET images, and 20 images in each modality. The method's performance is measured by using PSNR, weighted PSNR (WPSNR), mean SSIM (MSSIM), and total perceptual error (TPE). The average values obtained for PSNR and WPSNR are above 40 dB, desirable for medical images. The scheme's robustness is evaluated by applying attacks like noise addition, JPEG compression, filtering, and finding the normalized correlation (NC) and obtained significant results. ROI's size should be < 20% of the whole image's size and is the main limitation of the above method.

Abdullah et al. [25] used fusion of visual cryptography and watermarking for the protection of iris image and its templates. It used DCT coefficients of the host image's middle band frequencies to implant text watermark, which holds personal data. Template protection is carried out using visual cryptography technique. Different matrices are employed for measuring the system's performance; PSNR, BER values obtained for the watermarked images are 38.47 dB and 0.22%, and that for separated text are 84.63 dB and 0.023%, respectively. The system's robustness is evaluated by applying some attacks like JPEG compression, the addition of Gaussian noise; image manipulations such as histogram equalization, median filtering, and cropping, which obtained significant values for all the attacks. A strength constant is used to improve withstanding capability against different attacks; the images are distorted for less strength constant values by median filtering and compression attacks. It can enhance them by using high-strength constant values. Another limitation is that the watermark's text length is more dependent on the size of the iris image.

Su [26] designed a watermarking technology using Hessenberg decomposition, which decomposes the original color carrier image into a matrix of size 4×4; inserted the watermark on the specified columns in the orthogonal matrix, obtained by the host image decomposition. The watermark pixel position is shuffled using an Arnold transform. The extraction process did not require either the carrier image or watermark image. The similarity measurement of the scheme is evaluated using PSNR and SSIM, obtained values above 35 dB and 0.9616, respectively, under no attack. The watermark's robustness is calculated using NC values, against attacks like JPEG 2000 compression, the addition of noise, filtering, scaling operation, blurring, and rotation. The method resulted in NC values of more than 0.9 in almost all attacks and deals ranges from 0.8 to 0.9 for JPEG 2000 compression and Gaussian noise attacks, which has to be improved.

Zong et al. [27] introduced a rank-based watermarking scheme. This method divided the cover image into blocks: applied 2D-DCT to obtain DCT coefficients in

each block. A confidential key is used to randomly selecting some DCT values for the watermark inserting. A rank-based embedding rule is employed to implant the watermark into the image structure by altering some DCT coefficients. PSNR and BER values are measured to evaluate the watermarked image's perceptual quality and robustness against attacks. The average values obtained for the PSNR are above 40 dB, which is a significant one. The proposed method's robustness is evaluated by applying JPEG compression, constant luminance change, amplitude scaling, and noise addition attacks. The scheme calculated the BER for different episodes with different '*K*' values, where '*K*' is the number of DCT coefficients selected for embedding the watermarks in each block. They obtained 0 deal for BER without any attacks, amplitude scaling, and constant luminance change attacks. The BER values obtained for JPEG compression and Gaussian noise addition attacks are low, desirable for a watermarking scheme. The inserting capacity also is high since the approach used 2 DCT values to implant a single watermark bit in each block.

Liu et al. [28] developed a digital watermarking technique based on fractal encoding and DCT. First, the host image is encoded by fractal encoding and used encoded parameters in the DCT domain, which enabled a two-level encryption scheme. The watermark is inserted in the middle- and lower-frequency coefficients, resisting more JPEG compression with extensive embedded data. The technique measured the watermarked image's perceptual quality using PSNR and obtained a value of above 40 dB. Different attacks like JPEG compression, noise, and Gaussian filter are employed for the robustness measurement of the proposed scheme and obtained different mutual correlation coefficient (MCC) values of more than 0.9 in all the cases. But the technique handled only a small number of attacks to verify its robustness.

Ernawan and Kabir [29] presented an optimal DCT psycho-visual threshold watermarking method for copyright protection. The watermark is disarranged before inserting, which provides additional security. The carrier image is split into blocks of size 8×8 and computed for each block's modified entropy. Applied DCT to some lowest entropy-valued blocks and selected some coefficients for watermark embedding based on a psycho-visual threshold in lower frequencies. The selected coefficients are modified to insert the shuffled watermark, to form a watermarked image. The proposed scheme's imperceptibility is measured using PSNR, absolute reconstruction error (ARE), and SSIM and obtained a value of above 44 dB for PSNR; the average values of ARE and SSIM are 0.317 and 0.994. Robustness is evaluated using attacks like filtering, noise addition, JPEG compression, histogram equalization, cropping, scaling. The method obtained better robustness results for the attacks like Gaussian noise, median filtering, histogram equalization; weak robustness to the rotation, translation, and Poisson noise, which needs to be improved.

Shahdoosti and Salehi [30] designed a transform-based watermarking technique for copyright protection, used the ripplet-II transform. Here, the ripplet-II transform's rotation-invariant property is used, which provides good robustness to rotation attacks. The cover image is transformed to matrix coefficients using ripplet-II transform, DFT is employed to rows of the resulted matrix to obtain the Fourier matrix. The Fourier matrix consists of a phase matrix and an amplitude matrix, the

former saved for inverse transform and the latter for watermarking. A cost function improves the invisibility of the scheme in the ripplet-II transform. Then added a ridge regularization constant to the cost function, which avoids the singularity problem. The weights of the transform are adjusted by varying the cost function. The scheme's watermark invisibility is measured using the matrices PSNR and SSIM and obtained outstanding results a value of above 73 dB for PSNR and 1 for SSIM. The robustness is checked using BER by applying attacks like filtering, noise addition, JPEG compression, histogram equalization, edge sharpening, rotation, translation, and cropping. Significant results are obtained for the attacks like rotation and cropping. The scheme results in fewer values for translation attacks.

Byun et al. [31] proposed a novel watermarking scheme using DCT. Initially, a host image's DCT coefficients for a particular location are calculated and modified the coefficient according to a variation value based on inserting bits and quantization levels. The watermark bits are inserted by changing some pixel merits in DCT, which reduces computational complexity. The method obtained an embedding time of less than 1 ms because of less computational complexity. PSNR and SSIM matrices are employed to evaluate the proposed scheme's invisibility and brought an average value of 42 dB for PSNR and 0.97 for SSIM. Different attacks like noise, filtering, scaling, JPEG compression, and cropping are applied and calculated BER and NC values. The results implied that improvements to be needed for the JPEG attack.

Srivastava et al. [32] introduced a joint imperceptible image watermarking with JPEG compression using DCT. An additive watermarking is performed by adding a scaled watermark to the DCT coefficient of the cover image. The carrier image is subdivided into blocks of size 8×8, applied DCT on each block, embedded watermark using additive watermarking before quantization and after quantization of blocks resulting in a compressed watermarked image. Extraction of the watermark is done using the reverse process of embedding. The scheme's performance is compared in terms of PSNR, correlation, compression ratio, different quantization matrices with various Q factor, and DCT block sizes. The results indicated that the watermarking after quantization performed well compared to watermarking after DCT and obtained the values of 36.24 and 36 dB for PSNR in the above two cases. The scheme got a significant number of 0.83 for the compression ratio. Different attacks like sharpening, blurring, median filtering, Gaussian filtering, Poisson and speckle attacks, salt-and-pepper noise are applied to measure the robustness resulted in moderate values for blurring, Poisson, and speckle attacks. The main limitation is the less robustness against sharpening, median filtering, and Gaussian filtering attacks.

Abdelhakim et al. [33] designed a DCT-based watermarking technique that uses Bees algorithm for optimization. The carrier image is subdivided into blocks, applied DCT to each block, and selected some coefficients in the high-frequency region for the watermark embedding. Fitness functions are used to adjust the optimization between imperceptibility and robustness against different attacks. The method resulted in a maximum PSNR of 46.02 dB with the implemented fitness function and BCR values of more than 0.9 to attacks. The scheme used JPEG compression,

filtering, gamma correction, the addition of different noises, histogram equalization, and various geometrical attacks for measuring robustness. The technique has to enhance the robustness against noise attacks.

Zong et al. [34] proposed a gray-level watermarking scheme to increase the robustness to cropping and random bending attacks. The cover image is preprocessed using a Gaussian low-pass filter, which removes high-frequency components. The filtered image's histogram is obtained and selected different gray levels from the histogram using a secret key. An index based on the shape of the histogram is used for choosing a pixel for watermark embedding and a high-frequency component modification to nullify the effect of low-pass filtering. At the receiver end, decoded the watermark using the secret key. The method obtained a PSNR value of above 40 dB and an SSIM of more than 0.9. Robustness is measured to different signal processing, and geometrical attacks and brought significant results. The method has to enhance the robustness against JPEG compression.

Muñoz et al. [35] designed a color watermark embedding scheme using DCT. First, the carrier color image is separated into R, G, B images, further converted each sub-image into non-overlapping blocks of size 8×8. Then performed DCT to each block and arranged the DC coefficients to form a new matrix. DCT is applied to this new matrix, embedded subsampled binary values of watermarks to the new coefficients with the help of the quantization modulation technique. Then performed inverse DCT to form the watermarked image. For watermark extraction, the reverse of the inserting process is done. The technique obtained a maximum PSNR of 44.82 dB and an SSIM value of 0.99. Different attacks are applied to evaluate the performance and resulted in significant results. The method needs to enhance the performance against the average filtering.

2.2 Hybrid Domain Watermarking Schemes

There are different hybrid watermarking schemes proposed by various authors like [36–42], whose inferences are demonstrated in Table 2.

Muhammad and Bibi [36] presented a hybrid technique using discrete wavelet transform and singular value decomposition. Initially, the carrier image is fragmented using DWT, SVD, PPLU algorithm, which factorizes the watermark into permutation and triangular matrices. The permutation matrix is the key for the authentication. A weightage-based differential evaluation algorithm is performed to obtain better robustness against attacks. Measurement matrices like PSNR, structure similarity index (SSIM), and correlation coefficient (CC) are utilized to estimate the invisibility of the scheme. The average value obtained for PSNR is above 40 dB; CC index is nearly equal to 1. It has a high embedding capacity of 20,888 bits. Different fragile watermarking operations like noise, rescaling, blurring, histogram, contrast, and gamma corrections are performed to assess the method's robustness and also tried a JPEG compression with a compression ratio between 70–90% for evaluating

Table 2 Summary of hybrid domain watermarking techniques

Refs	Techniques/algorithms performed	Cover image/watermark specifications	Dataset used	Attacks handled	Area of application
[36]	DWT,SVD,PPLU algorithm, Weightage-based differential algorithm	512 × 512 (gray), 256 × 256 (binary)	SIPI	NS, JPEG, SC, BR, HE, CT, GC	Image watermarking
[37]	DWT, QR, FA algorithm	512 × 512 (gray), 64 × 64 (binary)	–	JPEG, SN, GLP, GC, RO, SC	Image watermarking
[38]	DWT, DCT, SVD	512 × 512 (gray), 256 × 256 (binary), Text (50 characters)	–	JPEG, MF, GLP, HE, S&P, SC	Iris biometric protection
[39]	FDCuT, DCT	1024 × 1024 (Gray), 128 × 128 (binary)	Med Pix	AGN, MF, AF, GLP, JPEG, S&P, SN, CR, SH, RO, FP, BR	Medical image watermarking
[40]	NSCT,RDWT, SVD, Logistic map chaotic encryption algorithm	512 × 512 (gray), 256 × 256 (gray), 128 × 128(text)	–	AGN, MF, GLP, JPEG, S&P, SC, RO, HE	Multiple medical image watermarking
[41]	DWT, DCT, SVD, Chaotic encryption algorithm	512 × 512 (gray), 256 × 256 (gray)	–	AGN, MF, GLP, JPEG, S&P, SC, RO, HE, CR, SH	Medical image watermarking
[42]	DWT,SVD, hash function	1024 × 1024 (gray), 1024 × 1024 (gray) (equal size for cover image and watermark)	–	AGN, MF, AF, S&P, SN, SC, RO, HE, CR, GC	Medical and non-medical image watermarking

*Non-geometrical attacks: Additive Gaussian Noise (AGN) [39], JPEG compression (JPEG) [36], Histogram Equalization (HE [38]), Motion Blurring (BR) [39], Noise (NS) [36], Speckle Noise (SN) [42], Salt and Pepper Noise (S&P) [40], Average Filter (AF), Median Filter (MF) [31], Gaussian Low Pass Filter (GLP) [37], Gamma Correction (GC) [37], Contrast (CT) [36]; Geometrical attacks: Rotation (RO) [42], Scaling (SC) [42], Cropping (CR) [41], Shearing (SH) [39], Flipping (FP) [39]

*Techniques or algorithms used: Discrete Wavelet Transform (DWT) [36], Discrete Cosine Transform (DCT) [38], Singular Value Decomposition (SVD) [41], Partial Pivoting Lower–Upper triangular decomposition algorithm (PPLU) [36], Firefly Algorithm (FA) [37], Fast Discrete Curvelet Transform (FDCuT) [39], Non-Subsampled Counterlet Transform (NSCT) [40], Redundant Discrete Wavelet Transform (RDWT) [40]

the robustness and obtained CC values ranging from 0.9090 to 0.9849. The scheme successfully withstands almost all attacks but handled less number of attacks.

Guo et al. [37] designed an optimized blind watermarking approach for images, which uses the firefly algorithm in the DWT-QR domain. Firefly algorithm is an optimization algorithm with advantages like local attraction and automatic regrouping. DWT transform domain methods have properties like high energy compression, high robustness against watermarking attacks, and multi-resolution representation. The main disadvantage is the low withstanding capability to some geometric attacks, which is avoided by the matrix factorization method- QR decomposition. It provides high robustness against geometric attacks. FA is used to optimize embedding strength, which improved the scheme's performance. At the initial stage, the carrier image is scrambled and disintegrated into sub-bands using 1 level DWT, divided LL sub-band into blocks, and applied QR factorization to all blocks. The R-matrix is employed for binary watermark insertion. The watermarked image's invisibility is checked by using performance matrices PSNR, SSIM, correlation, and NC. The method obtained a value of above 35 dB for PSNR and above 0.93 for all other matrices. Here, applied various attacks like rescaling, rotation, JPEG compression, gamma correction, filtering, and speckle noise for robustness measurement. Matrices like SSIM, BER, and NC are utilized for the quality checking of the process. The method resulted in outstanding robustness to gamma correction and comparable performance to other attacks.

Singh et al. [38] proposed multiple watermarking methods using DWT, DCT, and SVD and applied for medical images. At first carrier medical image is disintegrated to the two-level of coefficients using DWT. The resulting LL band is altered using DCT and SVD; the same transformation is practiced to the watermark image also. The embedding is accomplished using the singular values. Text watermark or personal data, embedded at the two-level of the high-frequency band, HH of the carrier image after encoding. Different gain factors like 0.05, 0.5, and 1 are utilized for the experimentation. The method used PSNR, NC, and BER as the measurement matrices. PSNR values of 35.84 dB, BER = 0, and NC = 0.9802 are obtained at a gain factor of 0.01 with encryption. The scheme's robustness is calculated using different attacks like median filtering, noise addition, JPEG compression, scaling, Gaussian filtering, and histogram equalization; significant values are obtained for compression and median filtering. It has low robustness to attacks like histogram equalization, noise, and scaling.

Thanki et al. [39] introduced a blind watermarking process for medical images utilizing DCT and FDCuT, which represents an image as to edges. FDCuT is implemented to cover images to procure different low-, medium-, and high-frequency sub-bands and performed DCT to the HF curvelet sub-band. Gaussian Noise sequences are inserted into mid-band frequency coefficients, to acquire the embedded image. Using the correlation among the Gaussian noise sequence and watermarked data, the watermark separation is done. The scheme's performance is assessed using matrices like NC, PSNR. An average value of PSNR = 49.36 dB, NC = 0.9618, is obtained at a gain factor = 2. Various attacks—noise addition, JPEG compression, cropping, rotation, flipping, filtering, blurring, and sharpening–are used to validate the scheme's

robustness and obtained medium values. The method has limitations like noise in the separated watermark and difficulty of embedding the text watermark.

Thakur et al. [40] designed a watermarking method that used Contourlet transform–discrete wavelet transform–SVD techniques. It used multiple watermarking—a medical image and personal data. Initially, the original carrier image is disintegrated into subsampled components using the sub-sampling method and applied Contourlet transform to maximum entropy components. Then applied redundant DWT to the HF sub-bands of Contourlet transform decomposed image and performed SVD to the selected sub-bands of DWT transformed images. Similar strategy is employed for both the images and embedded the watermark utilizing modified SVD coefficients with a pre-defined gain factor. The personal data watermark is separated using the logistic map chaotic encryption algorithm. The scheme's performance is measured by employing PSNR, NC, number of changing pixel rate (NPCR), unified averaged change intensity (UACI) and obtained maximum values 54.49 dB, 0.9993, 0.99, and 0.34. The method's robustness is evaluated by applying salt-and-pepper noise, Gaussian noise, JPEG compression, rotation, Gaussian LPF, scaling, median filtering, and histogram equalization and obtained comparable results.

Thakur et al. [41] introduced a watermarking process, which uses DWT-DCT-SVD with chaotic encryption for tele-health applications. The original carrier image is transformed using DWT-DCT-SVD domain; watermark image is using DCT-SVD domain. Singular values resulted are used for the creation of the final watermarked image and are encrypted by a chaotic encryption algorithm. The recovery process is done using the reverse embedding process. The system's performance is evaluated using PSNR, NC, SSIM, NPCR, and UACI and obtained the maximum value of 74.60 dB, 0.9999, 1, 0.9962, and 0.4835. The scheme's robustness is measured using different attacks like JPEG compression, salt-and-pepper noise, Gaussian noise, cropping, rotation, scaling, Gaussian low-pass filter, sharpening, median filter, histogram equalization and obtained medium values. The technique needs to enhance the robustness against attacks like rotation, Gaussian LPF, and histogram equalization.

Araghi and Manaf [42] developed a hybrid watermarking scheme using DWT-2 level SVD methods, which can apply for both medical and non-medical images. Initially, the watermark is preprocessed by duplicating it to the host image's size. Then applied DWT to the original cover image, separated the high-frequency sub-band into 16×16 non-overlapping blocks. After that, performed 1 level SVD to all the blocks, selected one singular value from each block to form a creative matrix. Two-level SVD is employed in this matrix. Singular value coefficients of this decomposed matrix are employed for the watermark inserting. The same procedure is applied for the watermark after preprocessing. Two-level security is performed using the hash function for authenticity. The scheme obtained an average value of 46.94 dB for PSNR, measured the robustness to distinct attacks filtering, noise addition, scaling, cropping, rotation, histogram equalization, gamma correction and resulted in nearly 0.99 of NC for almost all the attacks. The scheme does not handle any compression attack.

3 Discussion on Research Challenges and Opportunities in the Area of Digital Watermarking

There are different characteristics for a watermarking system: imperceptibility, robustness, embedding capacity, and data security are very important. Many authors presented various techniques to handle the situation. But only a less number of approaches are accomplished in it. So it will be a challenging one to deal with them effectively. Watermarking with cryptographic methods can be employed to enhance security issues, requiring more attention in this field. Multiple watermarking has prominent applications, where users can insert different watermarks, which provide more authenticity to the system. While implementing a watermarking approach for medical application, it should be reversible; otherwise, it may cause the disease's misdiagnosis due to data loss. Nowadays, watermarking has immense applications in biometric security, where different biometric templates like fingerprint and iris can be stored or transmitted with cover images. Here efficient encryption algorithms can be effectively used in order to prevent it from unauthorized users. Another issue is developing real-time watermarking systems, where execution time should be crucial with all other characteristics. Mostly the watermarking schemes are software-based digital signal processing (DSP) boards, field-programmable gate arrays (FPGAs), graphical processing units (GPUs), etc., can be employed for hardware implementation [11]. In the present scenario, we used the tele-biometric system and the tele-medical healthcare system in the medical field. The blockchain–Internet of Things (IoT) combination techniques may come into the picture, where data security happens to be a significant issue. It can use digital watermarking with suitable compression schemes to resolve this problem, protect the data, and be a challenging opportunity for current researchers [43, 44]. Machine learning and deep learning methods can also incorporate into the watermarking, so that we can use the marking technique effectively.

4 Conclusion

Digital watermarking, the process of embedding a secret image into a host image, has immense applications in almost all areas and has been popularly used especially for authenticity and data protection. This survey paper discussed the basics of digital watermarking process and recently used various transform and hybrid domain techniques. Transform domain watermarking techniques such as DFT, DCT, and DWT have advantages like high imperceptibility and very high robustness against attacks. Disadvantages of these methods are less watermarking capacity, high computational complexity, and increased processing time. Hybrid domain approaches combine the transform domain techniques, so that we can utilize the advantages of the above methods. We prepared summary tables with observations, which highlight the attributes of each method. Challenges and research opportunities, which may be

beneficial for current researchers working in this relevant field, are explained. New techniques should be introduced, which can efficiently handle all the issues related to conventional schemes.

References

1. F. Shih, *Digital Watermarking and Steganography, Fundamentals and Techniques* (CRC Press, USA, 2008)
2. S.P. Mohanty, Watermarking of digital images. M.S. thesis (Indian Institute of Science, India, 1999)
3. H. Nyeem, W. Boles, C. Boyd, A review of medical image watermarking requirements for teleradiology. J. Digit. Imaging **26**, 326–343 (2013)
4. N. Morimoto, Digital watermarking technology with practical applications, Inf. Sci. Spec. Issue Multimedia Inf. Technol. Part 1 **2**(4), 107–111 (1999)
5. F. Hartung, F. Ramme, Digital rights management and watermarking of multimedia content for m-commerce applications. IEEE Commun. Mag. **38**((11), 78–84 (2000)
6. B.L. Gunjal, S.N. Mali, *Applications of Digital İmage Watermarking in Industries* (CSI Communications, 2012), pp. 5–7
7. A.K. Singh, B. Kumar, M. Dave, S.P. Ghrera, A. Mohan, Digital image watermarking: techniques and emerging applications. In: *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (IGI Global, USA, 2016), pp. 246–272
8. S.M. Mousavi, A. Naghsh, S. Abu-Bakar, Watermarking techniques used in medical images: a survey. J. Digit. Imaging **27**, 714–729 (2014)
9. C. Fung, A. Gortan, W.G. Junior, A review study on image digital watermarking, in *The Tenth İnternational Conference on Networks* (2011), pp. 24–28
10. I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, 2nd edn. (Morgan Kaufmann, Burlington, 2008), pp. 425–467
11. Mohanty, S.P., Sengupta, A., Guturu, P., E. Kougianos, Everything you want to know about watermarking (IEEE Consumer Electronics Magazine, 2017), pp. 83–91
12. L.O.M. Kobayashi, S.S. Furuie, P.S.L.M. Barreto, Providing integrity and authenticity in DICOM images: a novel approach. IEEE Trans. Inf. Technol. Biomed. **13**, 582–589 (2009)
13. J.D. Gordy, L.T. Bruton, Performance evaluation of digital audio watermarking algorithms, in *Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems* (2000), pp. 456–459
14. N. Thilagavathi, D. Saravanan, S. Kumarakrishnan, S. Punniakodi, J. Amudhavel, U. Prabu, A survey of reversible watermarking techniques, application and attacks, in *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology* (ICARCSET, 2015), p. 37
15. Z. Fan, Z. Hongbin, Capacity and reliability of digital watermarking, in *Proceedings of the IEEE International Conference on the Business of Electronic Product Reliability and Liability* (2004)
16. A.F. Qasim, F. Meziane, R. Aspin, Digital watermarking: applicability for developing trust in medical imaging workflows state of the art review. Comput. Sci. Rev. **27**, 45–60 (2018)
17. A.-N. Yahya, H.A. Jalab, A. Wahid, R.M. Noor, Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. J. King Saud Univ.-Comput. Inf. Sci. **27**, 393–401 (2015)
18. A. Hassani Allaf, M. Ait K bir, A review of digital watermarking applications for medical images exchange security. in*Lecture Notes in İntelligent Transportation and İnfrastructure Book Series* (Springer, 2019)
19. A. Mohanarathinam,·S. Kamalraj, G.K.D. Prasanna Venkatesan, R.V.Ravi, C.S. Manikandababu, Digital watermarking techniques for image security: a review, J. Ambient Intell. Hum. Comput. **11**, 3221–3229 (2020)

20. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—A survey. IEEE **87**(7), 1062–1078 (1999)
21. A.K. Singh, B. Kumar, M. Dave, A. Mohan, Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun **80**(4), 1415–1433 (2014)
22. A. Anand, A.K. Singh, Watermarking techniques for medical data authentication: a survey, in *Multimedia Tools and Applications* (Springer, 2020), pp. 1–33
23. M. Andalibi, D.M. Chandler, Digital ımage watermarking via adaptive logo texturization. IEEE Trans. Image Process. **24**(12) (2015)
24. R. Easwaraiah, E. Sreenivasa Reddy, Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. IET Image Process. **9**(8), 615–625 (2015)
25. M.A.M. Abdullah, S.S. Dlay, W.L. Woo, J.A. Chambers, A framework for iris biometrics protection: a marriage between watermarking and visual cryptography. IEEE Access **4**, 10180–10193 (2016)
26. Q. Su, Novel blind colour image watermarking technique using Hessenberg decomposition. IET Image Process. **10**(11), 817–829 (2016)
27. T. Zong, Y. Xiang, S. Guo, Y. Rong, Rank-based image watermarking method with high embedding capacity and robustness. IEEE Access **4**, 1689–1699 (2016)
28. S. Liu, Z. Pan, H. Song, Digital image watermarking method based on DCT and fractal encoding. IET Image Process. **11**(10), 815–821 (2017)
29. F. Ernawan, M.N. Kabir, A robust image watermarking technique with an optimal DCT-psychovisual threshold. IEEE Access **6**, 20464–20480 (2018)
30. H.R. Shahdoosti, M. Salehi, Transform-based watermarking algorithm maintaining perceptual transparency. IET Image Process. **12**(5), 751–759 (2018)
31. S.-W. Byun, H.-S. Son, S.-P. Lee, Fast and robust watermarking method based on DCT specific location. IEEE Access **6**, 20464–20480 (2018)
32. R. Srivastava, B. Kumar, A.K. Singh, A. Mohan, Computationally efficient joint imperceptible image watermarking and JPEG compression: a green computing approach, in *Multimedia Tools and Applications* (Springer, 2017), pp. 1–13
33. A.M. Abdelhakim, H.I. Saleh, A.M. Nassar, Quality metric based fitness function for robust watermarking optimisation with Bees algorithm. IET Image Process. **10**(3), 247–252 (2016)
34. T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, G. Beliakov, Robust histogram shape-based method for ımage watermarking. IEEE Trans. Circ. Syst. Video Technol. **25**(5) (2015)
35. D. Muñoz, V. Ponomaryov, R. Reyes-Reyes, C. Cruz-Ramos, S. Sadovnychiy, Embedding a color watermark into DC coefficients of DCT from digital ımages. IEEE Latin Am. Trans. **17**(8) (2019)
36. N. Muhammad, N. Bibi, Digital image watermarking using partial pivoting lower and upper triangular wavelet decomposition into the wavelet domain. IET Image Proces. **9**(9), 795–803 (2015)
37. Y. Guo, B.-Z. Li, N. Goel, Optimised blind image watermarking method based on firefly algorithm in DWT-QR transform domain. IET Image Process. **11**(6), 406–415 (2017)
38. A.K. Singh, M. Dave, A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images, in *Multimedia Tools and Applications* (Springer, 2015), pp. 1–21
39. R. Thanki, S. Borra, V. Dwivedi, K. Borisagar, An efficient medical image watermarking scheme based on FDCuT-DCT. Eng. Sci. Technol. Int. J. **20**, 1366–1379 (2017) (Elsevier)
40. S. Thakur, A.K. Singh, S.P. Ghrera, A Mohan, Chaotic based secure watermarking approach for medical images, in *Multimedia Tools and Applications* (Springer, 2018), pp. 1–14
41. S. Thakur, A. K. Singh, S.P. Ghrera, M. Elhoseny, Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications, in *Multimedia Tools and Applications* (Springer, 2018), pp. 1–14
42. T.K. Araghi, A.A.Manaf, An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-DSVD.Future Gener. Comput. Syst. **101**, 1223—1246 (2019)

43. A. Castiglione, K.-K. Raymond Choo, M. Nappi, F. Narducci, Biometrics in the cloud: challenges and research opportunities. IEEE Cloud Comput. Mag. (2017)
44. H.-N. Dai, M. Imran, N. Haider, Blockchain-enabled internet of medical things to combat covid-19. IEEE Internet Things Mag. (2020)