International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-2, March, 2019

Robust Image Watermarking Theories and Techniques in Transform Domain: A Review

Ramneek Kaur Brar
Department of Electronics & Communication Engineering
Chandigarh Engineering College
Mohali, India
ramneekbrar2021@gmail.com

Harpal Singh
Department of Electronics & Communication Engineering
Chandigarh Engineering College
Mohali, India
harpal.ece@cgc.edu.in

Abstract—The protection of multimedia contents has turn out to be a crucial problem with the explosive expansion in the development of electronic commerce and online services. Watermarking is one of the most widely used technologies to tackle this problem in which a watermark is added to the original multimedia in such a way that it must not cause serious degradation of the original digital media. A good watermarking algorithm must satisfy three criteria: the lawful ownership security, sturdiness in opposition to the image manipulations, and imperceptibility of the watermark. In this paper, we have reviewed the theoretical analysis of various watermarking techniques in wavelet domain. In addition, a brief discussion on the properties of watermarking systems, wavelet domain, watermarking attacks, various domains of watermarking and robustness and security considerations for digital watermarking has been presented. With extensive research in the field of digital image watermarking, we find a huge scope in the development of novel watermarking techniques by hybridization of various transforms.

Keywords – Digital image watermarking, attacks, watermarking domains, transform domain.

I. INTRODUCTION

In digital management, multimedia content and data can effortlessly be used in an illegitimate way- being imitated, customized and disseminated all over again. Authenticity of content and material rights protection, copyright protection and intellectual rights protection for proprietors, customers, author, and distributors are critical features in solving an imperative and real predicament. In such state of affairs digital watermarking techniques [1] [2] [3] [4] [5] are up-and-coming as a convincing solution. Digital watermark is a perceptible or imperceptible identification code that is undyingly embedded in the host image. Invisible watermark is indiscernible copyright information which is straightforwardly concealed in media content in such an approach that it can only be read or extracted by the suitable party and under explicit conditions. Discouraging the unlawful replication of media content is the core endeavor of watermarking. A characteristic formulation of watermarking course of action counts two schemes: embedding and detection. The objective of embedding scheme is encoding the watermark signal into an image, while in the detection scheme it checks the existence of the watermark signal into watermarked image computing the relationship between the watermarked components of the image and the original watermarking signal by means of a correlation function and a predetermined threshold. Watermarking method can be classified into spatial domain techniques and transform domain schemes founded on the approach followed to process the original image. In spatial domain modus operandi, pixels of an image are unswervingly modified for encoding the watermark. In transform domain methods, the watermarking is encoded by changing some frequency components acquired by transforming the image in the frequency domain. Spatial domain methods are not as much of complex but they are less robust to tampering and attacks than transform domain techniques which put the watermark signal in the most perceptually momentous components of a transform domain. Diverse signal processing or geometric operations can modify the digital data. We can categorize the attacks on watermarked content as removal attacks, geometric attacks, cryptographic attacks and protocol attacks. [6] [7] [8] [9].

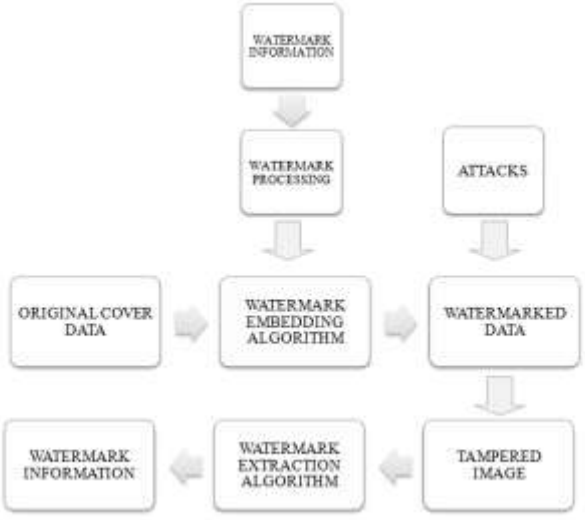

Figure1. Watermark embedding and extraction process in general.

II. PROPERTIES OF WATERMARKING SYSTEMS

The fundamental requirements of the digital watermarking can be treated as characteristics, properties. The diverse characteristics of the watermarking are as follows:

Robustness- The watermark system must be plausibly resilient to a variety of attacks and signal processing operations. Robust watermarks are intended to defend against common signal processing.

Imperceptibility- The watermarked content and the original one must be evidently analogous and incorporation of the watermark should transform the original signal indiscernibly.

Capacity/Data Payload- The maximum amount of information that can be concealed without degrading the image quality is what is referred to as capacity or data payload. It relies on the size of the original data.

Robustness, imperceptibility and capacity are confined and limited by each other. Robustness can be augmented by escalating the watermark strength but this result in a more detectable watermark. Correspondingly data payload can be amplified by diminishing the number of samples allocated to each hidden bit but this leads to loss of robustness. As a result it is not viable to meet these three necessities all together for any watermarking scheme and a good trade-off has to be achieved.

Security- The watermarking algorithm should be secure enough such that an unauthorized person should not be capable to eliminate the watermark without knowing the embedding process and the key used for watermarking the digital content.

Computational complexity- The amount of time taken by the watermarking algorithm for embedding and extraction process is defined as the computational complexity of the watermarking system.

III. OVERVIEW OF WATERMARKING ATTACKS

Figure 2 shows a brief description of various watermarking attacks. The attacks to the watermarking systems can be categorized broadly as geometric attacks, protocol attacks, removal attacks and cryptographic attacks. [6] [7] [8] [9]

Removal attacks- The intention of these attacks is to completely remove the watermark without having any acquaintance of the embedding algorithm or the key used for watermark embedding. This class includes quantization, compression, de-noising, re-modulation and collusion attacks. De-noising attacks aim at impairing the watermark maintaining the quality of the attacked data.

Collusion attacks are applied when several copies of the given data each with a diverse key or watermark can be attained by an attacker. In such a case a successful attack is achieved by averaging all the copies.

Geometric attacks- The embedded watermark in these attacks is not essentially removed but the intention behind these attacks is to distort the watermark detector harmonization with the embedded information. These attacks include rotation, scaling, warping, cropping, translation, etc.

Cryptographic attacks- These attacks aim at finding an approach to eliminate the embedded watermark information or to embed a ambiguous watermark by cracking the security methods in watermarking schemes. Such attacks include oracle attack and brute-force search.

Protocol attacks- Invertible watermark is one category of protocol attack in which the attacker subtracts his own watermark from the watermarked content and creates an ambiguity with respect to the exact possession of the data by claiming to be the proprietor of the watermarked data. Copy attack is one more type of protocol attack where the purpose is to calculate approximately a watermark and copy it to some other data called the target data. Onother form of protocol attacks is mosaic attack in which a browser imperceptibly renders the small blocks (into which an image is chopped) to look the same as single image. There are two issues in this case, one being the geometrical attack or cropping and that the image may be too small to embed a meaningful watermark in it.

Estimation-based attacks- The notion behind these attacks is derived from the assumption that the original data or the watermark can be anticipated from the watermarked data without knowing the key or the embedding decree. These attacks comprise removal attacks and de-synchronization attacks.

Re-modulation attacks- The aim of these attacks is to modulate the watermark contrary to that used in embedding process.

Synchronization removal attacks- The fundamental thought behind these attacks is to identify the synchronization patterns, eradicate them and apply de-synchronization procedure.

Non-geometric attacks- These attacks include common image processing attacks like compression, brightness, average filtering, sharpening, printing, scanning, gamma correction, noise addition, etc.

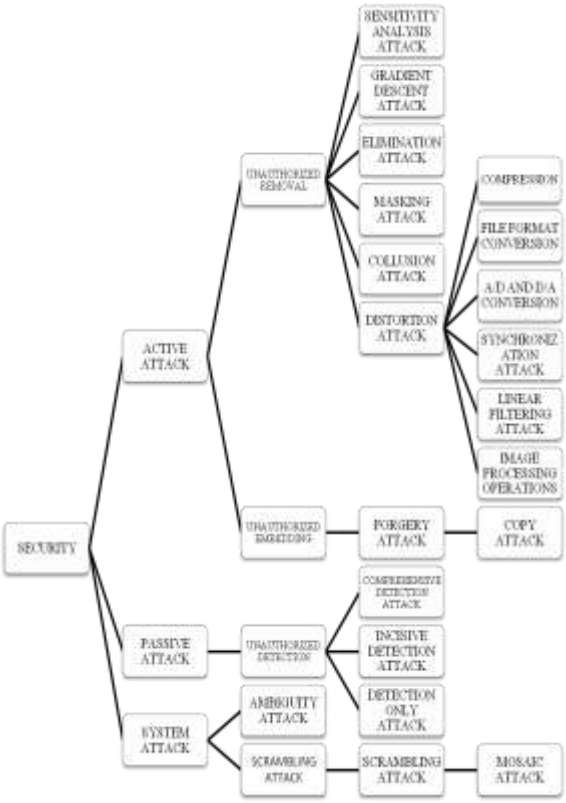

Figure2. Image processing attacks

A. Robustness and Security Considerations in Watermarking Systems

B. Robustness can precisely be defined as the extent of resistance that a watermarking scheme can provide to the modifications made in the cover signal caused by ordinary signal processing or operations developed to render the watermark barely discernible. On the other hand, security is defined as the capability of the watermark to survive various types of attacks. Thus, the necessity of robustness and security can be observed from the attack and distortion space correspondingly. All the pertinent image processing methods or transforms causing distortions need to be taken into consideration for evaluating the requisite degree of robustness. In the same way, different kinds of attacks have to be considered for the required security analysis. Developing a watermarking scheme which is sufficiently robust to any distortion and assuming that it would be secure against any attack may bring about technical errors and system vulnerabilities since such proposal may be secure only to those attacks which cause malevolent distortions. As a result, one should meticulously consider the requirements of both the robustness and security for examining and analyzing a watermarking system for a particular application. [9]

A.

IV. VARIOUS DOMAINS IN DIGITAL WATERMARKING

Spatial domain: The spatial domain techniques modulate the pixels of the image directly, modifying the pixel values of an image for embedding the watermark information. The simplest of the approaches refers to the bit-plane manipulation of the least significant bit, contributing rapid and easy decoding. Linear addition of the watermark information to the cover data is another method which offers inherent security and difficult decoding.

Transform domain: The transform domain techniques transform the DCT, DWT, DFT or any other transformed coefficients. In these methods the perceptual characteristics of the images are better exploited, thus improved performance is accomplished. In transform domain techniques, watermarking procedure is performed independent of compression.

Compressed domain: In the compressed domain techniques, compression framework is incorporated with watermarking by directly labeling the compressed or quantized symbol streams. Since compression is nearly ubiquitous for multimedia in the compression domain, there is little loss in general.

Since transform domain provides better performance and is more robust as compared to other watermarking domains, a detailed discussion is provided about the same in the corresponding section.

V. TRANSFORM DOMAIN

Transform domain or frequency domain is more robust as compared to the spatial domain. The transform domain technique includes the use of basic transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Transform domain is found to be more resistant to common watermarking attacks and signal processing. In order to preserve the watermark information in lossy compression environment, it is essential to place the watermark in the perceptually significant region of the data. This type of processing by and large takes place in the human perceivable frequency domain. Significant frequency components must be utilized for watermark embedding since data loss usually occurs in very low or high frequency components. These methods can embed more watermark bits as compared to spatial domain techniques and are comparatively more robust to attacks. Transform domain methods are favored owing to the fact that they allow more information to be embedded and provide exceptional robustness in opposition to attacks. The most frequently adopted transforms have been DCT and DWT. Due to its powerful properties, SVD is widely used as a transform in watermarking. But SVD is not preferred to be used alone owing to its substantial computation and thus, hybrid SVD-based watermarking methods are used to embed the watermark into the singular values of the host image. Watermarking process using various transforms is briefly explained below:

A. Digital Watermarking Using Discrete Cosine (DCT)

Image watermarking in DCT is similar to that in spatial domain but here the LSB of the image bit plane pixels are not altered, instead the alteration is done in the frequency coefficients. In DCT, the image can be decomposed into frequency bands and thus it becomes easier to embed the watermark in frequency bands of the image. The preferred frequency bands for embedding purpose are the middle frequency bands which provide higher robustness. In DCT the cover image is divided into 8 X 8 blocks of pixels and then the transform is individually applied to each block. To extract the middle frequency range from the DCT coefficients, a middle frequency 2-D mask is applied. Both pixel-based and block-based permutations are applied using a fast 2-D pseudo random number, assuming the watermark to be a binary image. Both the cover image and the watermark are used for watermark extraction process in which first the DCT is performed on the watermarked and cover images and then the original cover image is subtracted from the watermarked image. Both the permutations are reversed in order to extract the watermark.

B. Digital Watermarking Using Discrete Wavelet (DWT)

In 2D-DWT an image is decomposed into four different frequency sub bands which have their sizes abridged to 1/4th of the original size. DWT [10] [11] [12] [13] [14] [15] characterizes an image in both the spatial domain and frequency domain and has the property of frequency separation which is exploited in digital watermarking to insert watermarks in different frequency sub bands. Subsequent to passing through high pass filter and low pass filter on level 1, the output of the low pass filter designated as the approximate coefficients and the output of high pass filter, designated as detailed coefficients of the level 1 is filtered yet again by second level decomposition, the signal is decomposed into four feature groups. One group including the lowest frequency components, called as the approximate information and three groups containing progressively higher frequency components, called the detailed information. Image features such as edges and borders are well evaluated by the wavelet functions owing to the excellent space-frequency localization. Processing the data at different scales or resolutions is the key property of wavelet functions, highlighting both large and small features. Wavelet functions which can process signals containing many discontinuities and sharp changes are used in a number of fields including signal de-noising, image compression, texture analysis and image smoothing. Watermarking system turns out to be more robust with wavelet functions in comparison to spatial methods on account of irregular distribution of the inverse transform value, leading to the watermark being distributed over the image. DWT has a number of advantages over DCT such as 1) it provides a hierarchical analysis due to its multi-resolution properties, 2) it requires lower computational time in view of the fact that it does not suffer from blocking artifacts, and 3) integrating DWT in a watermarking procedure creates a watermark with a spatially global and spatially local support since wavelets provide a trade-off between time/space and frequency/space.

C. Digital Watermarking Using Singular Value Decomposition (SVD)

The application of SVD [16] in digital image watermarking permits embedding of the watermark onto the singular matrix of the frequency domain or spatial domain coefficients of the image as a replacement for of the watermark being directly embedded onto the coefficients of the image. The singular matrix is resistant to change caused by different category of attacks. Consequently, the watermark can be extracted with very less amount of loss of information and safe transmission of data can be implemented. There are a small number of key properties to make use of the SVD technique in digital watermarking scheme: Few singular values can correspond to huge segment of signal's energy. It can be applied to both rectangular and square images. The singular values of an image have very fine noise immunity, i.e. the singular values do not vary to a large extent when a small perturbation is added to an image. Singular values correspond to intrinsic algebraic properties.

D. Digital Watermarking Using Fractional Fourier Transform (FRFT)

The fractional Fourier transform is a generalized form of the Fourier transform and has become a powerful and potential tool for time-varying and non-stationary signal processing. As the classical Fourier transform corresponds to a rotation in the time-frequency plane over an angle, the FRFT can be considered as a comprehensive form that corresponds to a rotation over some arbitrary angle. FRFT has widely been used in digital watermarking in hybridization with other transforms to provide enhanced performance and robustness.[17][18][19][20][21][22].

E. Digital Watermarking Using Fractional Wavelet Transform (FRWT)

FRWT was proposed to resolve the limitations of wavelet transform (DWT) and fractional Fourier transform (FRFT) . It inherits the multi-resolution analysis advantage of the wavelet transform (DWT) and has the capability of signal representations in the fractional domain as in FRFT. FRWT is the generalization of wavelet transform in which the advantages of DWT and FRFT are combined to provide higher performance, security and robustness. [23]

F. Digital Watermarking Using Redundant Wavelet Transform (RDWT)

RDWT has recently been utilized in digital image watermarking field because of its spatio-frequency localization property. Being shift invariant, it overcomes the shift variance problem of DWT and avoids the down sampling process of each level done in DWT. RDWT eliminates the up sampling and down sampling for its coefficients and each sub band has the same size as the original image, thus keeping the significant texture of the cover image at the same spatial position in each sub band. The output coefficients of RDWT have the same size as that of input at each level. RDWT

provides higher watermark embedding capacity as compared to DWT.

Based on various domains and transforms, researchers have come up with a vast progress in the watermarking field. Hybridization or integration of various techniques has given an abrupt upsurge to the number of digital watermarking methods being proposed. Some of the important advances in digital watermarking is discussed in the corresponding section.

VI. SOME IMPORTANT ADVANCES IN DIGITAL IMAGE WATERMARKING

In [12] a robust watermarking method has been proposed in which a binary watermark is embedded into the detail sub-bands of the wavelet transform. A different threshold, which is calculated using the statistical analysis of wavelet coefficients, is used to choose the perceptually significant coefficients. To achieve higher robustness, the watermark is embedded a number of times. In 2016, R. Choudhary et al. [13] implemented a watermarking technique using 2-level DWT in which the variable visibility factor is utilized to insert the watermark into the low frequency component of the host image. N. Li et al. [14] presented a robust algorithm based on discrete wavelet transform in which a binary image watermark is added into a gray scale image and the host image is a requisite for detecting purpose. Spatial correlation is eliminated with the use of Arnold transform pretreatment which scatters the error bits amongst all the pixels making the watermarking technique more robust. P. Saravanan in 2016, [15] discussed a digital image watermarking technique based on DWT+DFT+SVD transforms. DWT is performed by using Daubechies wavelet family [24]. Subsequently the DFT stage has been used to reimburse for the translation variance predicament of DWT. Then, DCT is used in compression owing to its compact representation power. Finally, SVD is used for embedding the watermark into the image. J. L. Vehel et al. [25] proposed a digital image watermarking method in which certain subsets, which are determined both from a secret key and an image dependent procedure, of the wavelet packet decomposition are modified for watermark embedding procedure. C. Chang et al. [26], projected an image watermarking scheme based on SVD. SVD trans-formation is reasonably different from the frequently used DCT, DFT, and DWT transformations in view of the fact that non-fixed orthogonal bases and one-way non-symmetrical decomposition are used in SVD. S. Wang et al. [27] proposed a wavelet-tree-based blind water marking scheme for copyright safeguarding in which the wavelet coefficients of the host image are grouped into super trees. Quantization of these super trees is done for watermark embedding. Perceptually significant frequency bands are preferred to embed each watermark bit which makes the mark more resistant to frequency based attacks. Also, the watermark is spread all through the large spatial regions yielding more robustness against geometric attacks. In [28] T. Lin et al. in 2009 proposed a lossless and robust technique for digital images which is derived from cryptography and watermarking where the logo is not embedded into the host image. The secret key is generated by means of local features extracted subsequent to the digital wavelet transform from the perceptually important components of the host image. For further protection, digital signature and time-stamping tools are used. In 2018, Neeru Jindal et al. [29] described the fractional transforms and provided an exhaustive detail about their applicability and use in image processing. C. Lai in 2011 [30] discussed an enhanced SVD-based watermarking technique taking into consideration the human visual characteristics and in 2011 itself they also presented [31] a robust digital image watermarking method anchored in singular value decomposition (SVD) and a tiny genetic algorithm (Tiny-GA) in which the watermark image is embedded by modifying the singular values of a host image by multiple scale factors. In [32], a hybrid image-watermarking technique based on discrete wavelet transform (DWT) and singular value decomposition (SVD) is presented in which the watermark is not embedded in a straight line on the wavelet coefficients but on the elements of singular values of DWT sub-bands of the cover image. In 2012, N. Kashyap [33] implemented an image watermarking method for the exclusive rights protection based on 3-level discrete wavelet transform (DWT) in which a multi-bit watermark is embedded into the low frequency sub-band of a host image by means of alpha blending procedure. In [34] G. Bhatnagar discussed a reference watermarking scheme based on wavelet packet transform (WPT) and bi-diagonal singular value decomposition (BSVD) in which a logo is used instead of arbitrarily created Gaussian noise type watermark. The embedding procedure is done in wavelet packet domain by modifying the bi-diagonal singular values. G. Bhatnagar et al. in 2011 [35] projected a watermarking algorithm using fractional wavelet packet transform (FRWPT) and singular value decomposition (SVD) which is based on embedding in the singular values of the cover image. W. Lu et al. [36] proposed a robust digital image watermarking scheme based on feature point detection and watermark template-match. The feature points of original image are extracted by using the scale interactive model based filter, founded on which a watermark template is created and embedded into these points. In [37] at first the watermark synchronization is achieved by local invariant regions which are created by means of scale normalization and image feature points. The watermark is embedded in spatial domain into the entire local regions repetitively. M. T. Taba in 2013 [17] discussed the implementation of a watermarking technique based on the discrete Fractional Fourier Transform has been discussed which is made for the

detection of the watermark based on coding the 0 and 1 with different PN sequence code. In 2012 Y. Chen et al. discussed [18] a watermarking technique founded on the hybridization of DFRFT DWT and SVD in which the watermark is embedded into the cover image by transforming the singular values. In 2013, S. Bansal [20] enlightened the issue of false positive problem and a false watermark is extracted by using the proposed algorithm in Fractional Fourier Transform domain. In [21] a novel digital watermarking method for image is proposed, in which the chirp signal is used as a watermark and is embedded in the fractional Fourier transform (FRFT) domain. The encryption keys used in this technique are the watermark position and the transform order. In 2014, H. Singh et al. [38] discussed a multi-resolution logo watermarking method by means of fractional M-band wavelet transform (Fr-M-band-WT). SVD is used for embedding the watermark in the multi-resolution Fr-M-band-WT coefficients of low frequency sub-bands of the host image. H. Singh et al. in 2014 [39] proposed a logo watermarking method based on fractional M-band dual-tree complex wavelet transform (Fr-M-band-DT-CWT). The collective model of M-band wavelets and DT-CWT has been implemented to examine low frequency signal to augment the performance. In 2018, S. P. Singh et al. [40] discussed a robust watermarking method in which integer discrete cosine transform, non-linear chaotic map and dynamic stochastic resonance (DSR) are used. The host image is first transformed into integer DCT domain partitioning the coefficients into non-over-lapping blocks. The selected blocks are used to construct a circulant matrix which is used for embedding the watermark by SVD. S. Liu et al. in 2017 [41] combined the fractal encoding technique and DCT system for double encryptions to advance the traditional DCT technique. As the first encryption fractal encoding is used to encode the image, and subsequently the encoded parameters are utilized in DCT scheme as the second encryption. In 2016, B. E. Khoo et al. [42] exploited the entropy and edge entropy as HVS characteristics to select the significant blocks for embedding the watermark, which is a binary watermark logo. The blocks of the lowest entropy values and edge entropy values are preferred as the preeminent regions for inserting the watermark. SVD is performed on lowest sub-band following the first level of DWT decomposition. In 2013, G. Bhatnagar et al. [43] proposed a robust watermarking scheme which is based on redundant fractional wavelet transform, reversible extension transform and singular value decomposition (SVD) in which two watermarks i.e. gray scale and binary image or logo are embedded. Further, the thresholding used for verification has improved the security of the watermarked image. In [44], a watermarking technique is proposed based on redundant discrete wavelet transform (RDWT) and Singular Value Decomposition (SVD) in which subsequent to applying RDWT to the host image, SVD is applied to each sub-band and singular values of the host image are modified using singular values of the watermark. D. Hien [45] discussed a digital watermarking method in which redundant wavelet transform (RDWT) is used for watermark embedding and independent component analysis (ICA) is applied for watermark extraction. In 2018, F. Ernawan et al. [46] discussed a hybrid blind watermarking method which combines RDWT with SVD. Modified entropy of the image is used to find out the watermark embedding locations. Watermark embedding is implemented by examining the orthogonal matrix acquired from the hybrid technique, RDWT-SVD and to provide extra security the watermark image in binary format is scrambled by Arnold chaotic map.

From the exhaustive discussion done above, we find that various techniques and transforms can be hybridized to form a novel watermarking method and this provides a great scope for the development and advancement of the watermarking system in future.

VII. CONCLUSION

With the rapid expansion of network technologies and multimedia systems, it has become easy to acquire, duplicate, share and broadcast the digital contents without degradation of quality. But this has also made it easy for manipulation of the digital data. The lack of security has given rise to a technique called as digital watermarking to overcome these issues. Watermarking deals with the practice of embedding a watermark into the multimedia contents in such a manner that it does not has a significant impact on the perceptual quality of the data. In this paper, a number of watermarking techniques have been discussed and such extensive research provides us a huge scope in the development of new watermarking techniques based on the hybridization of various transforms. Also a brief discussion on watermarking properties, attacks, various domains, wavelet domain and robustness and security considerations has been provided. The aim of this paper is to bring to light the various advancements that have already been proposed and discussed by numerous analysts and researchers and the importance of digital watermarking systems in providing secure transmission of data over digital media. Some objectives can be formulated after having been done with a vast and extensive literature survey:

- The viability of coming up with enhanced novel watermarking algorithms offering more robustness and security.
- Analyzing the aforesaid transforms and hybridizing or amalgamating them to provide an innovative watermarking algorithm with enhanced performance.

REFERENCES

[1] J. Liu and X. He, “A Review Study on Digital

Watermarking," Inf. Commun. Technol., pp. 337–341, 2007.
[2] J. Nin and S. Ricciardi, "Digital watermarking techniques and security issues in the information and communication society," Proc. - 27th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2013, pp. 1553–1558, 2013.
[3] I. J. Cox and M. L. Miller, "A Rewiew of Watermarking and the Importance of Perceptual Modeling," Proc. SPIE, Hum. Vis. Electron. Imaging II, vol. 3016, pp. 92–99, 1997.
[4] B. Mishra and R. Kashyap, "A Review Paper on Digital Watermarking Techniques & Its Applications," vol. 5, no. 6, pp. 1864–1868, 2016.
[5] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," J. Appl. Res. Technol., vol. 12, no. 1, pp. 122–138, 2014.
[6] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," IEEE Multimed., vol. 12, no. 3, pp. 68–78, 2005.
[7] M. Tanha, S. D. S. Torshizi, M. T. Abdullah, and F. Hashim, "An overview of attacks against digital watermarking and their respective countermeasures," Proc. 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic, CyberSec 2012, pp. 265–270, 2012.
[8] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, "Analysis of digital image watermark attacks," 2010 7th IEEE Consum. Commun. Netw. Conf. CCNC 2010, 2010.
[9] H. Nyeem, W. Boles, and C. Boyd, "On the robustness and security of digital image watermarking," 2012 Int. Conf. Informatics, Electron. Vision, ICIEV 2012, pp. 1136–1141, 2012.
[10] Y. Yusof and O. O. Khalifa, "Digital watermarking for digital images using wavelet transform," Proceeding - 2007 IEEE Int. Conf. Telecommun. Malaysia Int. Conf. Commun. ICT-MICC 2007, no. May, pp. 665–669, 2007.
[11] S. Agreste, G. Andaloro, D. Prestipino, and L. Puccio, "An image adaptive, wavelet-based watermarking of digital images," J. Comput. Appl. Math., vol. 210, no. 1–2, pp. 13–21, 2007.
[12] C. Nafornita, S. Member, A. Isar, and M. Borda, "Image Watermarking Based on the Discrete Wave let Transform Statistical Characteristics," vol. 1, no. i, 2005.
[13] R. Choudhary, "A Robust image Watermarking Technique using 2-level Discrete Wavelet Transform (DWT)," no. Ll, pp. 0–4, 2016.
[14] N. Li, X. Zheng, Y. Zhao, H. Wu, and S. Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," pp. 942–945, 2008.
[15] P. Saravanan, M. Sreekara, and K. Manikantan, "Digital Image Watermarking using Daubechies wavelets," 3rd Int. Conf. Signal Process. Integr. Networks, SPIN 2016, pp. 57–62, 2016.
[16] H. C. Andrews and C. L. Patterson, "Singular Value Decompositions And Digital Image Processing," IEEE Trans. Acoust., vol. 24, no. 1, pp. 26–53, 1976.
[17] M. T. Taba, "The fractional fourier transform and its application to digital watermarking," 2013 8th Int. Work. Syst. Signal Process. Their Appl. WoSSPA 2013, pp. 262–266, 2013.
[18] Y. Chen, W. Yu, and J. C. Feng, "A digital watermarking based on discrete fractional Fourier transformation DWT and SVD," Proc. 2012 24th Chinese Control Decis. Conf. CCDC 2012, no. 3, pp. 1383–1386, 2012.
[19] D. Cui, ."_Digital watermarking algorithm for image based on fractional Fourier transform.pdf."
[20] S. Bansal, "On the security of robust reference logo watermarking scheme in Fractional Fourier Transform Domain," pp. 200–205, 2013.
[21] F. Q. Yu, Z. K. Zhang, and M. H. Xu, "A digital watermarking algorithm for image based on fractional fourier transform," 2006 1st IEEE Conf. Ind. Electron. Appl., 2006.
[22] Y. Zhang and F. Zhao, "The algorithm of fractional fourier transform and application in digital image encryption," Proc. - 2009 Int. Conf. Inf. Eng. Comput. Sci. ICIECS 2009, no. 1, pp. 2–5, 2009.
[23] J. Shi, N. T. Zhang, and X. P. Liu, "A novel fractional wavelet transform and its applications," Sci. China Inf. Sci., vol. 55, no. 6, pp. 1270–1279, 2012.
[24] K. Rana, "Comparisons o f Wavelets and Algorithms based on Wavelets and Comparing the R esults with JPEG," 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput., no. 1, pp. 3871–3876, 2017.
[25] J. L. Vehel et al., "Wavelet packet based digital watermarking," pp. 413–416, 2000.
[26] C. Chang, P. Tsai, and C. Lin, "SVD-based digital image watermarking scheme," vol. 26, pp. 1577–1586, 2005.
[27] S. Wang and Y. Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking," vol. 13, no. 2, pp. 154–165, 2004.
[28] T. Lin and C. Lin, "Wavelet-based copyright-protection scheme for digital images based on local features," Inf. Sci. (Ny)., vol. 179, no. 19, pp. 3349–3358, 2009.
[29] Z. Yuefeng and L. Li, "DIGITAL IMAGE WATERMARKING ALGORITHMS BASED ON DUAL TRANSFORM DOMAIN AND SELF-RECOVERY," vol. 8, no. 1, pp. 199–219, 2015.
[30] C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," OPTICS, vol. 284, no. 4, pp. 938–944, 2011.
[31] C. Lai, "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm," Digit. Signal Process., vol. 21, no. 4, pp. 522–527, 2011.
[32] C. Lai and C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," vol. 59, no. 11, pp. 3060–3063, 2010.
[33] N. Kashyap, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)," no. April, pp. 50–56, 2012.
[34] G. Bhatnagar and B. Raman, "BIDIAGONAL-SINGULAR VALUE DECOMPOSITION," vol. 9, no. 3, pp. 449–477, 2009.
[35] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "A new robust adjustable logo watermarking scheme," Comput. Secur., vol. 31, no. 1, pp. 40–58, 2011.
[36] W. Lu, H. Lu, and F. L. Chung, "Feature based watermarking using watermark template match," Appl. Math. Comput., vol. 177, no. 1, pp. 377–386, 2006.
[37] L. Da Li and B. L. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks," AEU - Int. J. Electron. Commun., vol. 63, no. 2, pp. 123–131, 2009.
[38] H. Singh, L. Kaur, and K. Singh, "A novel robust logo watermarking scheme using fractional M-band wavelet transform," J. Commun. Technol. Electron., vol. 59, no. 11, pp. 1234–1246, 2014.
[39] H. Singh, L. Kaur, and K. Singh, "Fractional M-band dual tree complex wavelet transform for digital watermarking," Sadhana - Acad. Proc. Eng. Sci., vol. 39, no. 2, pp. 345–361, 2014.
[40] S. P. Singh and G. Bhatnagar, "A new robust watermarking

system in integer DCT domain," J. Vis. Commun. Image Represent., vol. 53, no. February, pp. 86–101, 2018.
[41] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," IET Image Process., vol. 11, no. 10, pp. 815–821, 2017.
[42] B. E. Khoo, N. M. Makbol, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," IET Image Process., vol. 10, no. 1, pp. 34–52, 2016.
[43] G. Bhatnagar and Q. M. Jonathan Wu, "A new logo watermarking based on redundant fractional wavelet transform," Math. Comput. Model., vol. 58, no. 1–2, pp. 204–218, 2013.
[44] S. Lagzian, "Robust watermarking scheme based on RDWT-SVD : Embedding Data in All subbands," pp. 48–52, 2011.
[45] D. Hien, "RDWT Domain Watermarking based on Independent Component Analysis Extraction."
[46] F. Ernawan and M. N. Kabir, "A Blind Watermarking Technique using Redundant Wavelet Transform for Copyright Protection," no. March, pp. 9–10, 2018.

AUTHOR'S BIOGRAPHIES

Ramneek Kaur Brar received her degree in B.Tech in ECE from Punjab Technical University in the year 2016. She is currently pursuing M.tech in ECE from Punjab Technical University. Her research interests are in the field of image processing and watermarking.

Dr. Harpal Singh is working as Professor in Chandigarh Engineering College, Mohali, India. He has more than 20 years of experience, many national and international journal research papers to his credit and filed three patents. His areas of interest are Image Processing, Control Automation and Biological Engineering.