Transform based Digital Image Watermarking: An Overview

Naina Choubey[1], Mahendra Kumar Pandey[2]

Dept. of Electronics and Communication Engineering, Rustamji Institute of Technology (RJIT) Tekanpur, Gwalior (M.P.) – INDIA 475005

Abstract*— *In this paper, a review analysis of transform based image watermarking technique has been presented. Information security is extremely significant concern for the internet technology due to ease of the duplication, distribution and manipulation of the multimedia data. The digital watermarking is a field of information hiding which hide the crucial information in the original data for protection, illegal duplication and distribution of multimedia data. Analysis has been exploring the performance efficiency of various digital image watermarking techniques that compared on the basis of outputs. In the digital watermarking the secret information are implanted into the original data for protecting the ownership rights of the multimedia data. In this field, transform based techniques has large contribution especially wavelet based techniques. This review elaborates the most important methods transform domain and focuses the merits and demerits of these techniques.

Keywords*— *Watermarking, Compression, wavelet, SVD.

I. INTRODUCTION

In recent years, digitization plays a big role in human life as numerous applications in field of engineering, healthcare, communication, documentation and many more. Here, multimedia content like image and video is major content. Therefore, authentication, information security and other various issues are raised with multimedia sources and content. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using Computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original [1-3].

The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. This idea is implemented in bank currency notes. In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same "watermarking" concept may be used in multimedia digital contents for checking the authenticity of the original content [4-5]. So, A Watermarking is adding "ownership" information in multimedia contents to prove the authenticity. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. Considering the enormous financial implications of copyright protection, there is a need to establish a globally accepted watermarking technique. The sudden increase in watermarking interest is most likely due to the increase in concern over IPR. Today, digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity [1-6].

Generally, the image watermarking can be done in spatial domain or in transform domain [6-24]. The quality of watermarked image can be determined based on some important factors given like as: Firstly, in imperceptibility the quality of original image must not be changed due to the watermark [5] [6]. Secondly, robustness of image, in this the watermark removal is difficult in case of different types of attacks like noise addition, compression, scaling and rotation etc. [7] [8]. Thirdly, in capacity the most information is embedded in spatial domain as well as in transformation domain. But there are some disadvantages in both spatial and transformation domain like in spatial domain it is not much robust against image processing attacks [9, 22-24]. Where as in transformation domain it is not simple and fast as in case of spatial domain, but is having better robust against image processing techniques, so DCT, DWT transformation techniques are mostly used. Nowadays, mostly DWT is being used. We know that the discrete wavelet transform (DWT) suffers a drawback; the DWT is not a time invariant transform. This means that, even with periodic signal extension, the DWT of a translated version of a signal X is not, in general, the translated version of the DWT of X. To avoid this, the idea to average some slightly different DWT, known as stationary wavelet transform (SWT) or un-decimated wavelet transform is proposed. The main advantage of SWT is image de-noising. Therefore, SWT is widely used in image analysis and image processing.

In this paper, a review analysis of transform based different watermarking techniques has been presented. The manuscript followed as: section I illustrate the basic introduction, section II presents the overview of image watermarking, section III described the transform based watermarking scheme and concluding remarks is included in section 4.

II. OVERVIEW OF WATERMARKING

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object called cover/carrier such that watermark can be detected or extracted later to make an assertion about the multimedia object like as an image or audio or video. A watermarking algorithm consists of an embedding algorithm, and an extraction, or detection algorithm as shown in fig. 1. Basically, watermarking process divided into two parts as embedded section and extraction section; where embedded section generate the watermarked image and extraction section has perform extraction of cover/carrier image and embedded image from watermark image. Where, WI represents the watermarked image in embedding process as well as extraction process.

Image watermarking is very emerging technology to protect the images from unauthorized owner. There are several properties are presented to determine the quality of watermarking scheme such as robustness, Imperceptibility, capacity and blind watermarking [1-24]. These properties may vary with different application of watermarking. Therefore, watermarking schemes are classified as per these properties and different application as discussed below.

A. *Types of Image Watermarking*

Visible watermark: visible watermarking technique generate a visible logo or symbol that clearly seen on watermarked image. This type of watermark used for show the ownership of content like TV channel.

Invisible Watermark: This type of watermark is used to find the ownership as well as prevention from authorized application of image or content. Here, a watermark can insert information into an image which cannot be seen, but can be interrogated with the watermark extraction algorithm.

Robust Watermark: Robustness watermarking scheme is used for sign copyright information of the digital works, the embedded watermark can resist the common edit processing and various attacks.

Fragile Watermark: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. It can be determined whether the data has been tampered according to the state of fragile watermarking.

Semi fragile Watermark: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise compression attacks.

Invisible-Robust Watermark: The invisible-robust watermark is embedding in such a way that processes made to the pixel level; which are perceptually not determine and it can be recovered only with appropriate decoding process.

Invisible-Fragile Watermark: The invisible-fragile watermark is embedded in such a way that any attacks of the image would alter or destroy the watermark.

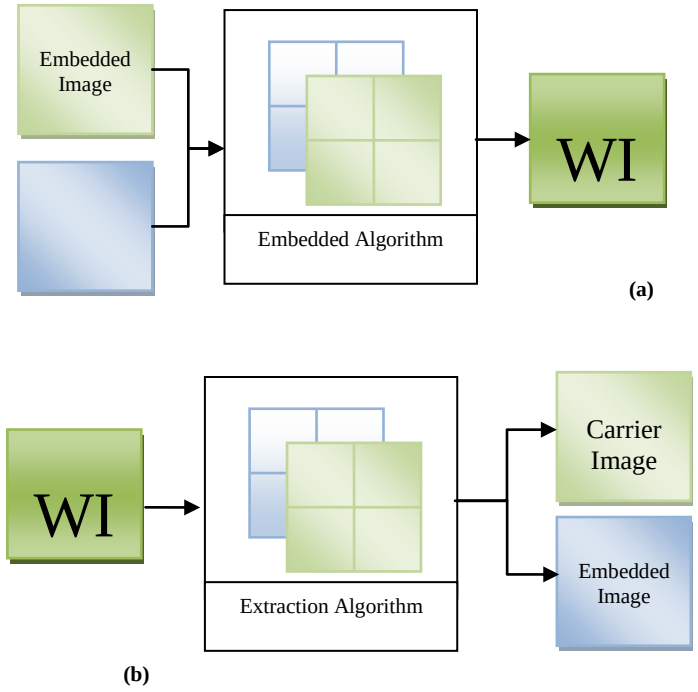

Fig. 1 Watermarking Algorithm: (a) embedded process, (b) extraction process

B. *Application of Image Watermarking*

Digital image watermarking is a very active research field with a lot of applications. Although it is a relatively new field, it has produced important algorithms for hiding messages into digital signals. The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. There are several different application area also exploited for watermarking benefits such as copyright protection, digital right management, tamper proofing, broadcasting monitoring, fingerprinting, access control, medical application, image and content authentication. These are discussed below [1, 4-5].

Copyright protection: Digital image watermarking can be used to identify and protect copyright ownership as well as illegally replicated.

Digital right management: watermarking scheme can protect the digital rights such as identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets.

Tamper proofing: Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content such as image, audio, video can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

Broadcast monitoring: Watermarking can protect the content ownership during the broadcasting of information over the telephone line, TV or internet etc.

Fingerprinting: In the applications of copyright protection, the watermark for finger printing is used to trace authorized

users who violate the license agreement and distribute the copyrighted material illegally.

Access control: It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose to allow access with control capacity.

Image and content authentication: A watermark can proof the image or content are authentic or not based on embedded watermark.

Therefore, various application and advantages are present of image watermarking. In this context, several methods are developed over the past decade based different techniques particular transform based watermarking schemes are shown their robustness in terms of properties in different applications.

III. OVERVIEW OF TRANSFORM BASED WATERMARKING

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

The transform domain watermarking is achieving very much attention and success as compared other contemporary watermarking schemes. Transform-domain watermarking techniques are typically much more robust to image manipulation compared to the spatial domain techniques. This is because the transform domain does not use the original image for embedding the watermark data. There are most commonly used transform domain methods is Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [6-24]. This technique discussed in brief in listed literature references.

In this context, transform-domain watermarking techniques are typically much more robust to image manipulation compared to the spatial domain techniques. This is because the transform domain does not use the original image for embedding the watermark data. In addition, a transform domain algorithm spreads the watermark data over all part of the image. Additionally, frequency domain-based techniques can embed more bits for watermark and are more robust to attack.

A. Process of Image Watermarking

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

Recommended font sizes are shown in Table 1.

The watermark embedding/insertion process dissipated in fig. 2 as a block diagram for transform domain. First, the input image is transformed using a transform such as the DWT or DCT. In general, any frequency domain transform can be used. The watermark data is embedded to a transformed image. In other words, the watermark data is inserted into transformed coefficients. Finally, inverse transform is performed on the transformed watermarked image.

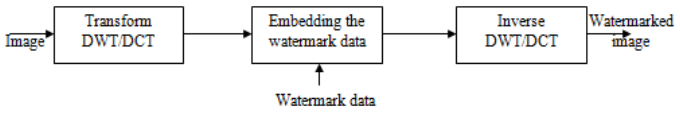

Fig. 2 Block diagram of embedded process based on the transform domain watermark

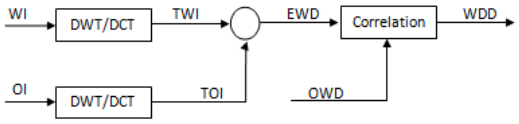

Fig. 3 Block diagram of extraction/detection process based on the transform domain watermark

The watermark detection process is the inverse procedure of the watermark insertion process as is depicted in fig. 3. As this figure shows, to extract the watermark data from the watermarked image, first, the watermarked and the original image are transformed using the DCT or DWT. Second, the transformed image is subtracted from the transformed watermarked image. This is because the watermark data is the difference between the original image and the watermarked image. Finally, the similarity of the original watermark data and the extracted watermark data is computed. The similarity is depends on the amount of the inserted watermark data and the watermark attacks. Since the DCT and DWT are usually used for watermarking in the frequency domain. Fig. 3 represents the extraction process of watermark image where, WI is watermarked image, OI is original image, and TWI is transform WI and TOI is Transform OI, EWD is extracted watermark data and OWD is original watermark data similarly, WDD is watermarked data. In this process, EWD obtained from extraction process between TWI and TOI.

In this context, a comparative analysis has been presented in Table. 1 that shows the efficiency and contribution of recent developed techniques of image watermark based on transforms.

TABLE I
PERFORMANCE COMPARISON OF DIFFERENT TECHNIQUES

Methods	**Transform**	**PSNR (in *db*)**	**Remark**
Y. Zhou [20]	DCT/JPEG	34.58	Good quality
Ibrahim [21]	DWT	47.54	robust with attacks
Chang [22]	DWT	40.80	robust with attacks
Nagarjuna [23]	SWT-SVD	58.87	robust with attacks
Samira [24]	RDWT-SVD	38.52	Good quality

Digital image watermarking is still very challenging research problem towards to robustness nature. It's provides various kind of solution from unauthorized information access, copyright protection, privacy, information protection, illegal claim of ownership. Therefore, a robust

watermarking technique has been needed that resist with different kind of attacks.

IV. CONCLUSIONS

An overview of image watermarking scheme based on transform technique is presented, which is applicable for various applications such as information security as well as secure communication of multimedia data. These techniques are work as hidden watermark mostly. In literature, several techniques are presented based on the different transform especially, DWT and DCT. These techniques have good efficiency of robust watermarking as well as watermark extraction as presented analysis in reported literature.

Digital watermarking scheme is widely utilized for authentication of data, copyright protection and communication process. It provides a consistent robust performance on different original image and watermarked image in various analyses.

REFERENCES

[1] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images," accepted by IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, Sept. 2003.

[2] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "Capacity for JPEG2000-To-JPEG2000 Images Watermarking," in *Proc. of IEEE Int. Conf. on Multimedia and Expo*, July 2003.

[3] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Son. Inc., 1991.

[4] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn. "Attacks on copyright marking systems", *in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH'98*, Portland, Oregon, U.S.A., April 14-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 218-238.

[5] Fabien A. P. Petitcolas. "Watermarking schemes evaluation". *IEEE Signal Processing*, vol. 17, no. 5, pp. 58–64, Sept. 2000

[6] H. Liu, H. Fu, J. Huang, 'A watermarking algorithm for JPEG files', Lecture Notes in Computer Science, vol. 4261, pp. 319-328, 2006.

[7] F. Gu, Zhe-M. Lu, J.-Sh. Pan, 'Multipurpose image watermarking in DCT domain using sub-sampling', IEEE Int. Sym. On Circuits and Systems (ISCAS 2005), vol. 5, pp. 4417-4420, 2005.

[8] P. Artameeyanant, 'Salient image for watermarking robust against compression and cropping', SICE Annual Conference 2005, pp. 1111-1113, 2005.

[9] Y.-G. Fu, L.-P. Shen, R.-M. Shen, H.-T. Lu, 'Robust watermarking scheme based on sub-sampling', Shanghai Jiaotong Daxue Xuebao/Journal of Shanghai Jiaotong University, vol. 39, Issue. 12, pp. 1929-1932+1937, 2005.

[10] K.-S. Kim, M.-J. Lee, H.-K. Lee, 'Blind image watermarking scheme in DWT-SVD domain', IIHMSP 2007, pp. 477-480, 2007.

[11] Ch.-Ch. Chen, De-Sh. Kao, 'DCT-Based reversible image watermarking approach', IIHMSP 2007, pp. 489-492, 2007.

[12] V. Saxena, J.P. Gupta, 'Towards increasing the robustness of image watermarking scheme against JPEG compression', IMECS 207, vol. 2, pp. 1903-1906, 2007.

[13] Ch.-Ch. Wang, YU-Ch. Hsu, 'New watermarking algorithm with data authentication and reduction for JPEG image', J. Electronic Imaging, vol. 17(3), 033009 (August 27, 2008), http://dx.doi.org/10.1117/1.2954128

[14] M.A. El-Iskandarani, S. M. Saad, A.M Abubahia, 'An efficient digital image watermarking scheme',42nd Annual IEEE ICCST 2008, pp. 37-42, 2008.

[15] Z. Rui-mei, L. Hua, P. Hue-wei, H. Bo-ning, 'A Blind watermarking algorithm based on DCT', IITA'08, pp. 821-824, 2008.

[16] Sh.-m. Zhu, J.-m. Liu, 'Adaptive Watermarking Scheme in Hybrid DWT-DCT Transform Based on Human Visual System', Int. Sym. KAM'08, pp. 668-671, 2008.

[17] G. Bhatnagar, B. Raman, K. Swaminathan, 'DWT-SVD based dual watermarking scheme', ICADIWT 2008, pp. 526-531, 2008.

[18] N. Jie, W. Zhiqiang, L. Zhen, 'A new JPEG resist color image watermarking algorithm based on quantization index modulation', 5th Int. Conf. IAS'09, pp. 669-672, 2009.

[19] L. Hu, F. Wan, 'Analysis on wavelet coefficient for image watermarking', Int. Conf. MINES'10, pp. 630-634, 2010.

[20] Y. Zhou, 'Joint robust watermarking and image compression', 2010 IEEE WIFS, pp. 1-6, 2010.

[21] N. Ibrahim, F. Khelifi, J. Jiang, I. Stanley, 'A robust image watermarking scheme based on normalized circular image in DWT domain', 10th ISSPA'10, pp. 33-36, 2010.

[22] CH.-Ch. Chang, K.-N. Chen, M.-H. Hsieh, 'A robust public watermarking scheme based on dwt', 6th IIH-MSP'10, pp. 21-26, 2010.

[23] P V Nagarjuna and K. Ranjeet, 'Robust Blind Digital Image Watermarking Scheme Based on Stationary Wavelet Transform", IEEE IC3, 8-10 Aug. 2013.

[24] Samira Lagzian, Mohsen Soryani, Mahmood Fathy, 'A New Robust Watermarking Scheme Based on RDWT-SVD' International Journal of Intelligent Information Processing, Vol. 2, Number 1, 2011, Doi:10.4156/ijiip.vol2. issue1.3.