Digital Image Water Marking Techniques:State of the Art

Mehak Saini[1], Dr. Priyanka[2]
[1,2] *Department of Electronics & Communication Engineering*
Deenbandhu Chhotu Ram University of Sci. & Tech., Murthal, Sonipat, Haryana, India

***Abstract*—**To provide security to data in a digital communication system; such as internet, a number of techniques such as, cryptography, steganography, digital watermarking etc. are used. Digital watermarking hides some crucial information in the original data to avoid illegal duplication and distribution of the multimedia data. Thus, it ensures the security, authenticity and copyright protection of the data and has become an important area of study for information hiding. The images distributed over the internet can be easily copied and may put the copyrights of their owners at a risk. This paper presents a detailed survey of various digital image watermarking techniques along with their relative merits and demerits. In addition, the applications, challenges and limitations of this emerging technology have also been explored.

Keywords*—Watermarking techniques; copyright protection; information security; digital image.*

I. INTRODUCTION

Nowadays, the internet has become ubiquitous and individuals can easily share their resources with others, on the web. Besides a number of advantages, this widespread transmission of information poses a threat to the copyright protection of digital media. To discourage the illegal duplication of images on the internet, a collection of some items of information, called a watermark, is inserted in images [1]. These watermarks can be of visible or invisible type. Visible watermarking is typically performed in the spatial domain. Invisible watermarks are inserted as visually redundant information and are imperceptible. However, they can be recovered by using some appropriate decoding algorithm. Invisible watermarks are called fragile if they can not survive image modification, otherwise, they are called robust. In 1993, the concept of digital watermarking was first introduced by Tirkel [2]. Digital watermarking is the embedding of watermark into the digital media, i.e., audio, text video or image. Embedded information can be extracted later to identify the real owner of the digital media. Broadly classifying, the watermarking methods can be of two types, i.e., spatial domain and transform domain methods. In first type, the intensity level values of the pixels of the host image are manipulated and the information is directly inserted into them. These methods have high capacity and can be easily implemented, but, they are subjected to noise and attacks. In transform domain methods, a predefined transformation is used to convert the host image [3].The watermark is embedded in the transformation coefficients. Finally, inverse transform is used to obtain watermarked image. This method is more robust as the watermark is not distributed locally, rather, it is distributed over the whole range of pixels of the image. Embedded information can be extracted later to identify the real owner of the digital media. Digital watermarking has a number of applications and has become a prime area in information hiding. This paper analyses the basic schemes, applications and shortcomings of this upcoming technology. Rest of the paper is organized as follows: Basic scheme of image water marking system is given in section II. Classification of watermarking techniques is presented in section III. In section IV, areas of application of various watermarking techniques are discussed. Conclusions and future scope are given in the last section.

II. BASIC COMPONENTS OF AN IMAGE WATERMARKING SYSTEM

A watermark (w_i) is inserted into image (f_i) by using an encoder as shown in Fig. 1 (a).The watermarked image thus produced is denoted by f_{wi}.

Fig. 1 (b) depicts a decoder which extracts and confirms the watermark present in marked image f_{wi} or f_j i.e., unmarked image. One doesn't require decoder for visible watermark w_i.

If watermark is invisible, a copy of f_i and/or w_i may or mayn't be required by the decoder. If they are used(f_i and/or w_i) then it is called a private or restricted key watermarking system. Otherwise, it is called a public or unrestricted key system [2].

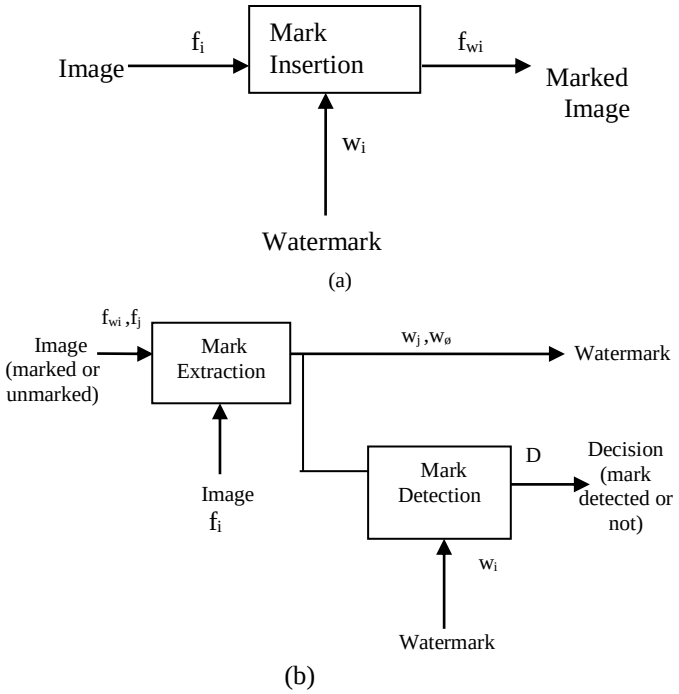

Fig. 1: (a-b). Basic watermarking scheme [1]

III. CLASSIFICATION OF WATERMARKING TECHNIQUES:

In this section, various types of digital watermarking techniques have been discussed in details. Image watermarking techniques are classified on the basis of characteristic, type, purpose, host signal, visibility, detection process, domain etc which are discussed as follows:

A. On the basis of characteristics of watermark

There are mainly three types of watermarking techniques on the basis of characterisics of watermark, i.e., robust, fragile and semi fragile [4]. Robust watermarking is used to secure copyright information of the digital works. This type of embedded watermark is able to withstand the image processing and lossy compression. It can resist different types of attacks. Fragile watermarking used for integrity protection and semi fragile watermark can tolerate changes to the watermarked image.

B. On the basis of type of the water mark

Another classification may be made with respect to the type of watermark.Watermark can be of noise type, e.g., gaussian, random, etc. or it can be of image type, i.e., stamp, logo, label etc.

C. On the basis of purpose of watermark

Watermarking scheme using a visible and robust watermark may be used for copyright protection. Tampering tip watermarking helps to protect the integrity of digital data [4]. Anti-counterfeiting watermarking is added during building process of paper notes & becomes detectable after the processes of scanning, printing etc. Another type of water marking can be used for hiding the important annotation of important data and thus restricting its illegal use.

D. On the basis of host signal

Watermarking scheme can be classified as image, audio, video, text or graphic types depending upon the type of the data to which the watermark is embedded.

E. On the basis of visibility

Watermarking scheme can be of visible or invisible type depending upon whether the watermark is visible or invisible to the human eye.

F. On the basis of detection process

Watermarking scheme can be visual or blind depending upon whether there is any/no need for the original data for detection process. In asymmetric water marking, different keys are utilized for the processes of embedding and detecting a water mark. If same keys are used for these two processes, the water marking scheme is symmetric

G. On the basis of domain

H. Different digital watermarking techniques are represented in Fig. 2.

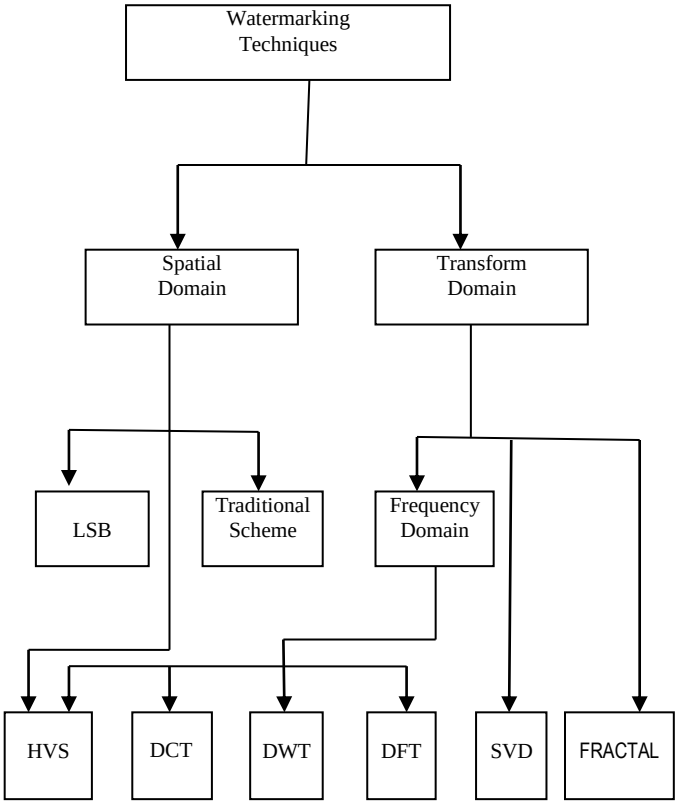

Fig. 2: Digital watermarking schemes

In spatial domain, raw data is directly loaded into the image pixels using various modulation techniques.
In frequency or transform domain, certain frequency values are altered by using transform techniques such as:

1. *DCT:* A Discrete Cosine Transform (DCT) is used to convert a finite sequence of data points into sum of cosine function. DCT based watermarking techniques provide more robustness against various simple image processing operations such as blurring, low pass filtering etc.
The disadvantage of using this technique is that it is not easy to implement, is comparitively expensive and gets affected by geometric attacks like rotation, scaling and translation (RST) [5].
2.*DWT:* A dicrete wavelet transform (DWT) is a computationally efficient technique used for watermarking. It decomposes the image into three spatial directions i.e., horizontal, vertical and diagonal.[6]
3. *DFT:* A discrete fourier transform (DFT) converts a finite data sequence into frequency components. DFT is RST (Rotation, Scaling and Translation) invariant i.e., it is resistant to geometric attacks.So, it is a better watermarking technique as compared to spatial domain techniques, DCT and DWT [5].
4. *SVD:* Singular value decomposition(SVD) is another transform domain technique . The disadvantages of SVD-based image watermarking are false positive, robust and transparency. However, it provides robustness and security [7]-[8].

5. *Fractal:* Fractal based watermarking method is used widely for watermarking in the transform domain[9].

Although water mark in spatial domain is f ragile yet this technique has low computational cost, computational time and computational complexity. Also, it has higher capacity and perpetual quality as compared to frequency domain technique. Spatial domain technique is generally used for authentication and frequency based techniques are used for copy right protection. Also, transform domain techniques are implemented by taking into consideration the Human Visual System (HVS) but it is not so in spatial domain watermarking techniques [4].

IV. APPLICATIONS OF WATERMARKING SCHEMES

The various fields of application [10] of digital image processing are discussed below :

A. Confirmation of ownership

For the validation and confirmation of ownership of creator of a media (i.e., image, audio, video, etc) watermarks are employed. An unambiguos watermark identifying the owner is embedded in the media to prove that he is the sole and legitimate creator of a media. It is important to use a watermarking algorithm that assures inevitability or non-quasi inevitability of the watermark. Also, some Trusted Third Party (TTP) may be employed that legaly assigns a unique registration code to the owner of the work in order to proof the ownership of the registered asset without ambiguity.

B. Fingerprinting

Unauthorized distribution and piracy of a multimedia content that is electronically available on a network can be stopped by embedding a unique watermark or a fingerprint in each copy of the data. Even if unauthorized copies of the data are found, then the origin of the copy can be found out by decoding the watermark or fingerprint. Here, the watermark should be invisible and must also be unaffected by various kinds of attacks targeted to remove or forge it and should be resistant to collusion. To avoid collusion, a group of 'n' users with same image but containing different finger prints should not invalidate a fingerprint or create a copy without any fingerprint.

C. Controlling copying of media

Watermarks can also be used for copy prevention and control. For instance, in a closed system in which the multimedia work requires special hardware for copying and/or viewing, a digital watermark can be inserted which indicates the allowed number of copies. Each and every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. A Digital Versatile Disc (DVD) is an example of such a system.

D. Authentication by fraud and tamper detection

In areas such as legal purposes, medical applications, commercial transactions and news reporting, it is important to ensure that the multimedia content has originated from a particular source and that it has not been changed or manipulated. All of this is done by embedding a watermark in the data. So, when the photo is checked, the watermark is retrieved by using a unique key associated with the source and the security or integrity of the data is verified through the integrity of the extracted watermark. Also, information from the original image can be added to watermark in order to make the recovery process easier. However, the watermark used for purpose of authentication should not have any affect on the quality of an image and should be invulnerable to forgery attacks. In this case, robustness is not an important factor as removal of the watermark makes the content inauthentic and hence is of no value.

E. ID Card Security

The photograph of a person on a passport or ID (e.g., passport number, person's name, etc.) can be embedded with some information such as written text. So, an additional level of security is provided to the passport which can be checked when watermark is extracted. For instance, if the ID card gets stolen and the picture is forged by the attacker then failure in extracting the watermark will invalidate the ID card. Also, such watermarks can be employed in many applications such as in rights management and protection like tracking use of content, binding content to specific players, automatic billing , broadcast monitoring etc.

F. Invisible Marking on Paper

Watermarks can be used to mark white paper for authenticating the creator or the originating source, checking the authenticity of the document, or adding date to the document. Such applications are used for protecting official documents such as contracts. For instance, watermarking techniques can be used to embed the name of the lawyer or important data such as key monetary amounts. In the case of a dispute, the digital watermark is then read allowing authentication of key information in the contract. Alp Vision has developed a genuine method to invisibly mark blank white paper with normal and visible ink. This technology has been patented and is called Cryptoglyph.

G. Intellectual Property Right (IPR) Protection

The protection of Intellectual Property Right (IPR) is a very important area which requires watermarking for security purposes as it is a good target. This term includes the protection of the rights of the creator, the rights of the legitimate owner, copyright protection, moral rights protection (e.g. the integrity of the work in the respect of the moral beliefs of the creator). There are major tasks in IPR protection area such as:

demonstration of the ownership in legal disputes
fingerprinting
controlling copying of media.
It is quite difficult to protect digital contents from piracy.

V. IMAGE WATERMARKING SCHEMES USING SOFT COMPUTING TECHNIQUES

For several applications of image processing, e.g., digital watermarking of video and images, execution of code has to take place within specified constraints of time. At the same time, embedding and extraction of data has to fulfill two mutually exclusive objectives, i.e., robustness and visual imperceptibility. Moreover, the capacity of watermark is assumed to be constant as the size of embedded content is quite small as compared to the size of host signal. Hence, the embedding and extraction processes have to be optimized in such a way that time complexity is minimum and there is not much loss of visual quality after water-marking and execution of attacks on signed images.

In literature, a number of soft computing techniques have been used to optimize these processes [11-16]. For this purpose, a gradient descent based artificial neural network using back propagation learning (slow on account of inherent mathematics involved) is used in [11] and a radial basis function neural network (comparatively faster) is used in [12]. These techniques are adaptive and give good results in terms of visual imperceptibility as well as robustness. Several researchers have developed fuzzy inference system based image watermarking schemes [13-14]. These schemes, although not adaptive and fast enough (to be implemented on real time scale) , yet produce good results with respect to the above said issues of image watermarking are concerned.

Many machine learning based algorithms have also been used for this purpose [15-16]. Recently, least square support vector regression has been utilized to embed and extract a binary image as watermark in three different images [15]. However, finite newton support vector regression algorithm has been proven to be comparatively faster watermark embedding and extraction scheme [16] as it completes training with in a few iterations. Although, in these papers, issue with respect to time complexity has not been taken into consideration.

Huang et al. developed a fast algorithm for training of ANN, popularly known as the extreme learning machine (ELM). In this approach, they used only one tunable parameter, i.e., the number of hidden neurons. Using this training process, training time up is reported to be reduced to a large extent (to a few milliseconds).The training of this machine is found to be extremely fast and on regular image databases used by authors, it is reported to have been finished within milliseconds with a reasonably good accuracy [17-19].

Mishra et. al [20] have recently proposed a novel digital image watermarking algorithm based on Extreme Learning Machine (ELM) for two gray scale images. As mentioned, the ELM algorithm is very fast and completes its training in milliseconds unlike its other counterparts such as BPN or FIS based systems They used the ELM output as the watermark to be embedded within the host image using Cox's formula [21] to obtain the signed image. The authors report high PSNR values which indicate that the quality of signed images is good.

Hans-Arno Jacobsen [22] discussed a generic architecture for hybrid intelligent systems in his paper. He has emphasized over integration of intelligent systems that aims at overcoming the limitations of individual techniques through hybridization or fusion of various techniques. According to author, it is difficult to identify merits and demerits of different individual approaches. He argues that neural networks are suited for learning and adaptation but it is like a black box and hence it is not interpretable. On the other hand, the fuzzy knowledge based systems have complementary characteristics. In this case, the incorporation and interpretation of knowledge is straight forward whereas learning and adaptation constitute major drawbacks in case of fuzzy systems. Due to these reasons ANNs and Fuzzy system are complementary to each other and suffer from their inherent drawbacks. The integration of these intelligent systems has helped in overcoming limitations of individual techniques.

VI. CONCLUSIONS AND FUTURE SCOPE

In this paper, we have presented an overview of various digital image watermarking techniques and application areas.

The future plan of work is to implement a robust and efficient digital watermarking scheme using hybrid scheme which incorporates the benefits of two or more intelligent techniques.

REFERENCES

[1]. Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", edition 3, Pearson.

[2]. Tirkel, Anatol Z., et al. "Electronic watermark." *Digital Image Computing, Technology and Applications (DICTA'93)* , 1993, pp. 666-673.

[3]. Fatemeh Daraee and Saeed Mozaffari, " Watermarking in binary documents images using fractal codes", Pattern recognition letters, Vol. 35, January 2014, pp. 120-129, doi: http://dx.doi.org/10.1016/j.patrec.2013.04.022.

[4]. Prabhishek Singh, R S Chadha A Survey of Digital Watermarking Techniques, Applications and Attacks ISO 9001:2008 Certified International Journal of Engineering and Innovative echnology (IJEIT), Volume 2, Issue 9, March 2013

[5]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A survey of digital image watermarking techniques", in Proc. of IEEE international conference on industrial informatics (INDIN), 2005, pp. 709-716.

[6]. I.J. Cox, M.L.Miller, J.A.Bloom, J.Fridrich, and T.Kalker,"Digital Watermarking and Steganography" Elsevier, 2008.

[7]. A.Mansouri, A.Mahmoudi Aznaveh and F. Torkamani Azar," SVD-based Digital Image Watermarking using Complex Wavelet Transform", Sadhana (Vol. 34, Part 3), pp. 393–406, 2009.

[8]. "Y.Fisher, Fractal Image Compression: Theory and Application", Springer, 1994.

[9]. M.Hong Pi, and C.Hung Li,"A Novel Fractal Image Watermarking" in Proc. International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.369-372, 2004.

[10]. Sunesh and Harish Kumar. Article: Watermark Attacks And Applications in Watermarking. IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011 RTMC(10):-, May 2012.

[11]. Huang, S., Zhang, W., Feng, W., Yang, H.: Blind watermarking scheme based on neural network. In: 7th World Congress on Intelligent Control and Automation (WCICA 2008), pp. 5985–5989 (2008)
[12]. C.-R., Beack, S.-H., Woo, D.-M., Han, S.-S.: A Blind Watermarking Algorithm Based on HVS and RBF Neural Network for Digital Image. In: Jiao, L., Wang, L., Gao, X.-B., Liu, J., Wu, F. (eds.) ICNC 2006. LNCS, vol. 4221, pp. 93–496. Springer, Heidelberg (2006)
[13]. Motwani, M.C., Harris Jr., F.C.: Fuzzy Perceptual Watermarking for Ownership Verification. In: Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV 2009), Las Vegas, Nevada, July 13-16 (2009)
[14]. Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.: A Dual Watermarking Technique for Images. In: ACM Multimedia, Part 2, pp. 49–51 (1999)
[15]. Mehta, R., Mishra, A., Singh, R., Rajpal, N.: Digital Image Watermarking in DCT Domain Using Finite Newton Support Vector Regression. In: Proceedings of 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 123–126 (2010)
[16]. Chaudhary, V., Mishra, A., Mehta, R., Verma, M., Singh, R., Rajpal, N.: Watemarking ofGrayscale Images in DCT Domain Using Least-Squares Support Vector Regression. International Journal of Machine Learning and Computing 2(6), 725–728 (2012)
[17]. Huang, G.-B., Zhu, Q.-Y., Siew, C.K.: Extreme Learning Machine: Theory and Applications. Neurcomputing (70), 489–501 (2006)
[18]. Huang, G.-B., Zhu, Q.-Y., Siew, C.K.: Real-Time Learning Capability of Neural Networks. IEEE Transactions on Neural Networks 17(4), 863–878 (2006)
[19]. Huang, G.-B.: The Matlab code for ELM (2004), http://www.ntu.edu.sg/home/egbhuang
[20]. Mishra, A., Goel, A., Singh, R., Singh, L., Chetty, G.: A Novel Image Watermarking Scheme Using Extreme Learning Machine. In: Conference Proceedings of International Joint Conference on Neural Networks (IJCNN), pp. 1–6 (June 2012)
[21]. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing 6(12), 1673–1687 (1997)
[22]. Jacobsen, H.A.: A Generic Architecture for Hybrid Intelligent Systems. In: Proceedings of The IEEE World Congress on Computational Intelligence (FUZZ IEEE), USA, vol. 1, pp. 709–714 (1998).
[23]. Lamri Laouamer, Muath AlShaikh, Laurent Nana, Anca Christine Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity," Journal of innovation in digital ecosystems 2, ScienceDirect, 2015, pp.

Mehak Saini (DOB: 4 April 1994) is B.Tech (ECE) and pursuing M.Tech from Deenbandhu Chhoturam University of Science and Technology Murthal, Sonepat (Haryana), India. She is a young Technocrat and Researcher. Her area of Interest is Signal and Image processing.

Priyanka is working at Associate Professor at D.C.R. University of Science and Technology, Murthal, Sonipat, India. Her current areas of interest are signal processing, image processing and SAW filter design. Her highest qualification is Ph. D. in Electronics Engineering from Indian Institute of Technology, Delhi, India. She is IEEE member & has published several papers in refereed journals including IEEE Transactions & Conferences.