Grenze International Journal of Computer Theory and Engineering , Oct 2016

Digital Image Watermarking using Machine Learning Techniques: A Technical Review

Swati Sharma[1], Amit Kumar Singh[2] and Pardeep Kumar[3]
[1-3]Department of Computer Science & Engineering, Jaypee University of Information Technology Waknaghat, Solan,
Himachal Pradesh-India
swatisbond@gmail.com, amit_245singh@yahoo.com, pardeepkumarkhokhar@gmail.com

Abstract—**Recently, digital information can be easily manipulated, copied, distributed and stored, which has resulted in the demand for safe ownership of the information. The watermarking provides a very good solution to the problem of copyright protection and content authentication. This paper discusses basic concepts of digital watermarking and its characteristics, important attacks on watermark system, general watermark embedding and extraction process, important transform and machine learning techniques and some reported transform and spatial domain based watermarking method using machine learning. Finally, the current state-of-the-art in the field is also discussed. This paper will be more important for researchers to implement effective watermarking method using machine learning technique.**

Index Terms— **Image Watermarking, Discrete wavelet transform (DWT), Discrete Cosine Transform (DCT), Support Vector Machine (SVM), Singular Value Decomposition (SVD), Fuzzy Support Vector Machine (FSVM), Neural Network (NN).**

I. INTRODUCTION

The digital media such as image, audio and video is an important way of communication in the world and being increasingly used for delivery of multimedia content, thus it is easy to manipulate, store, distribute or reproduce the data using different networking sites. This shows no difference in the quality between an original image and its copy image. However, unrestricted copying and malicious tampering cause huge financial losses and problems for intellectual property rights [1-2]. Therefore, information hiding has become an important research area and watermarking is used as a data hiding technique for the protection of digital images. Digital watermarking systems have been proposed to provide content protection, authentication and copyright protection, protection against unauthorized copying and distribution [3-4]. In this technique, it consists of protecting the illegal insertion of robust and imperceptible brand in a host image. The watermarking algorithms must be imperceptible to the naked eye, robust against attacks, blind which means the original image is not necessary for the detection and extraction of the brand. Important characteristics of digital watermarks are robustness, imperceptibility, capacity, security and computational cost [5-7]. However, robustness, imperceptibility and capacity are tradeoff between each other. So, there is a strong requirement to balance these characteristics. The image watermarking techniques is divided into two domain methods: 1) Spatial domain methods (least significant bit substitution, spread spectrum etc.) are more simple high capacity but are not robust against common signal processing attacks. 2) Transform domain methods

Grenze ID: 01.GIJCTE.2.3.517

(DWT, DCT and SVD etc.) are more robust against common signal processing attacks but the computational complexity is higher than spatial domain methods [8-10].

Machine learning is a technique to determine predict from desired observations or past behavior. It is a method that improves the detection rate of watermarks after being attacked and contains numerous methods for different classification and patterns for recognition of problem. It also provides increasing level of automation in the knowledge engineering process by replacing time consuming activity with automatic techniques used for improvement of accuracy and efficiency [9-11].

Generally, four types of attacks on digital watermarking systems as discussed below [5]:

a. Active attacks: In active attacks hacker tries to remove watermark. They are aimed at distortion of watermark before recognition. This shows the problem in copyright protection, copy control etc.

b. Passive attacks: In passive attacks, hackers just tried to figure out that there is watermark and identify it. In this attack no damage or removal is done.

c. Forgery attacks: In forgery attacks hackers embed new valid watermark rather than removing one. In this hackers can easily manipulates the data and makes corrupted image genuine.

d. Collusion attacks: In collusion attacks hackers has the same intension as for the active ones but used slightly different approach. The hacker uses instances of same data to construct the new copy without watermark.

II. General Watermarking System: Embedding and Extraction Process

In general, watermarking system consists of two processes, embedding and extraction. The embedding process is consisting of encoding [8]. It is used to produce the watermarked image. The watermark embedding process takes a cover image (C), watermark image (W_I) and secret key (K) then it goes to embedded function gives watermarked image (W_E). The extraction process is consisting of recovery process. It is used to recover the corrupted image, which may or may not be the watermarked image. The extraction process takes cover image and watermarked with secret key to recover the watermark from the possibly distorted image [9-10]. The watermark embedding and extraction process is given in Figure 1(a) and Figure 1(b) respectively. The watermark embedding process can be written as:

$W_E = F(C, W_{I,} K)$

Also, the watermark extraction process can be written as:

Watermark (W) = F (W or C, W_E, K)

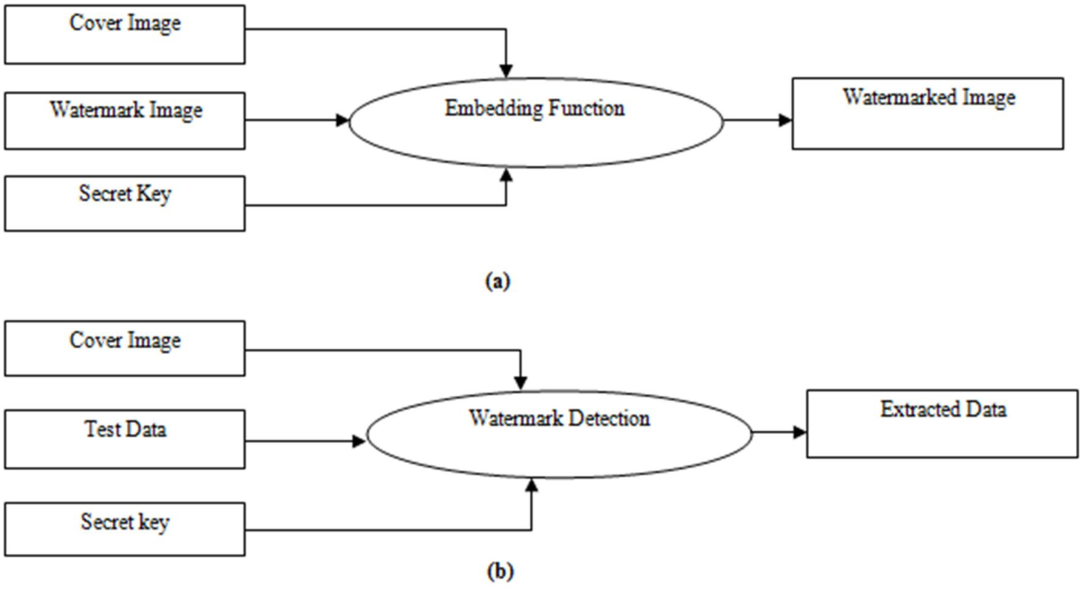

Figure 1: Watermark (a) Embedding process and (b) Extraction process [9]

Depending on the application requirements, the watermarking system can be blind, semi-blind or non- blind [9]. The robustness of the semi-blind watermarking system is poor than the other two system.

III. Existing Transform based Watermarking Techniques Using Machine Learning method

Review of image watermarking using noticeable machine learning techniques is carried out and presented below.

Vatsa et al. [12] proposed biometric based image watermarking algorithm where face image is embedded in the fingerprint. The embedding watermarking method based on Discrete Wavelet Transform (DWT) and Support Vector Machine (SVM). The experimental result is shown that the method is robust and the face image is resilient to geometric and frequency attacks. The integration of SVM improved the face recognition by 10%. Yen et al. [13] proposed a digital watermarking technique using spatial domain based on support vector machine. The watermarking technique uses only 128bits in training SVMs. To embed the watermark bits, the proposed scheme modifies blue channels of the central and surrounding pixels at same time. Watermarks are embedded in spatial domain and extracted directly from a watermarked image without the requirement of original image. The experimental result shows that the proposed scheme provides high PSNR of a watermarked images and low extraction error rate.

Jianzhen et al.[14] proposed a RST(Rotation, Scaling and translation) invariant watermarking technique utilizing SVM and image moments for synchronization. In watermarking technique to estimate RST transform parameters SVM is utilized to learn the image geometric pattern represented by six combined low order image moments. The experimental result shows that scheme can resist JPEG compression, noise and geometric attacks. Lei Li et al.[15], proposed a image watermarking scheme using spatial domain based on Fussy Support Vector Machine (FSVM). In the embedding process, the 8 * 8 block of the cover image is divided into sub-block of the texture features as input vectors using support vector machine. The image sub-block is divided into a weak texture and a strong texture. The strong texture information is embedded into the cover image. The method has been shown that the robustness of the FSVM based method is better than SVM based method against important attacks. Jain et al.[16], proposed a watermarking algorithm based on support vector machine using color image. In the embedding process, the watermark is embedded into the discrete wavelet domain of the original image and extracted by training support vector machine. In addition, the method is using momentum coefficient to reduce the error and increase the rate of the learning. The experimental results have been shown that the method is imperceptible against signal processing attacks. However, the value of PSNR is below than 27 dB for most of the attacks.

Ramamurthy et al.[17] proposed a robust digital image watermarking scheme using neural network and fuzzy logic approach. The approach shows comparison to embed watermark into host image using quantization in DWT domain based on BPNN (Back Propagation Neural Network) and DFIS (Dynamic Fuzzy Inference System). The experimental result shows the watermarking technique is robust and imperceptible to the attacks. B.Jagadeesh et al.[18], proposed a robust and blind Image watermarking algorithm for copyright protection of images. The embedding watermarking method is used by DWT based on the support vector machine. The experimental result shows that method is secured and robust for various attacks. However, the value of NC and PSNR is less than 0.9711 and 35dB for most of the attacks. Vafaei et al. [19] proposed a robust blind watermarking method. The watermarking method uses the Neural Networks in Discrete Wavelet Transform domain. The neural networking technique is used to maximize the strength of watermark image. The experimental result shows that method is robust and imperceptible to various attacks. B.Jagadeesh et al.[20] proposed a novel image watermarking method in discrete wavelet transform domain using support vector machine. The embedding watermarking method is used to extract the watermark from the watermarked image even after different image processing attacks. The experimental result shows that the given algorithm is secure and robust to different image attacks. Yahya et al. [21] proposed a model for information security using stego SVM classification. The embedding technique uses LSB in image steganography that hides data behind a cover-image in a spatial and discrete cosine transform (DCT) domain. The technique proposed a new model that utilizes Human Visual System (HVS) and embedding technique through shifted LSB called Stego SVM- Shifted LSB in DCT domain to preserve the imperceptibility and increase the robustness of stego-images.

Zhang et al.[22] proposed a technique of image watermarking capacity using neural network. The watermarking technique is used for hiding the information in the form of images and watermarking is used as a form of communication. The experimental result shows that the attraction basin of associative memory decided watermarking capacity. Shi et al.[23] proposed a new color watermark embedding technique with circulation, based on non-overlapping SVD for hiding important information in images. In the watermarking method cover image is decomposed into small watermarks and then watermark is embedded into one single block with circulation. The experimental result shows that scheme is robust against different image attacks. Thai et al.[24] proposed a technique for image classification using support vector machine and artificial neural network. In the technique, image is divided into sub images and each sub image is classified into the responsive class by ANN then SVM compiled all the classified result of ANN. The Experimental result shows the feasibility of the technique.

From the above, it is clear that image watermarking techniques in transform domain have been found to give high robustness, imperceptibility, capacity and security. The digital watermarks are potentially useful in various applications including ownership assertion, fingerprinting, copy prevention or control, telemedicine, e-commerce, e-governance, media forensics, and artificial intelligence and healthcare etc. Digital cinema is also considered as a practical application, where the information can be embedded as a watermark in every frame. Digital image watermarking is the most effective solution in these areas and its use to protect the information is increasingly exponentially day by day.

The transform based watermarking schemes can be further explored for video and audio watermarking.The state of art in transform domain based image watermarking using machine learning language as available in the literature is given below.

1. The method proposed in [12, 14, 16, 18, 20] based on the combination of DWT and SVM to achieve high robustness, imperceptibility and good quality of watermarked image. In [12] biometric is used to embed the face image with the fingerprint in order to achieve security also.
2. The method proposed in [13, 15] based on the combination of spatial domain with machine learning techniques (FSVM and SVM) to lower the attacks on digital data. In the technique [15] shown that the robustness of the FSVM based method is better than SVM based method against important attacks.
3. The method proposed in [17, 19] based on the combination of DWT with Neural Network uses to increase the strength of watermark image. In the technique [19] host image was decomposed into wavelet bits embedded in the sub-band coefficients.
4. The method proposed in [21] based on the combination of DCT and SVM uses LSB in image steganography that hides data behind a cover-image. The technique is robust to various attacks.

TABLE I: WAVELET BASED WATERMARKING USING MACHINE LEARNING MODEL

Sn.	Authors, Year	Technique used	Watermark Type, Size	Results (Maximum value) dB
1	Vatsa et al. [12], 2005	DWT, SVM	Fingerprint,FaceImage (512*512) / Extracted Face Image	Value of verification of face and fingerprint ranges from 0-1 and shows accuracy is improved by 10%.
2.	Yen et al.[13], 2006	Spatial domain method , SVM	Color image of Lena, Baboon , Monkey , House (512*512)/ Binary image of Rose (64*64)	PSNR= 45.536
3.	Jianzhen et al.[14], 2009	DWT, SVM	Grey scale image of lena (512*512)/ logo image	PSNR= 39.12
4.	Li et al.[15], 2010	Spatial Domain, SVM, FSVM	Grey scale image of Cameraman (256*256)/ logo image	PSNR=20.866,NC=0.986
5.	Jain et al.[16],2011	DWT, SVM	Lena, Baboon (256*256)/ logo color image (32*32)	PSNR=43.499
6.	Ramamurthy et al. [17], 2012	DWT , Neural Network, Fuzzy logic	Office_4 cover image (512*512)/ Barbara grey scale image (64*64)	PSNR=51.3593,NC=0.9965
7.	B.Jagadeesh et al.[18], 2013	DWT, SVM	Lena , Goldhill and pepper (512*512)/ logo(64*64)	PSNR=45.15,NC=1
8.	Vafaei et al.[19], 2013	DWT, Neural Network	Grey scale image of Lena , Baboon, Airplane, Barbara(512*512)/logo watermark Binary image (8*8)	PSNR=48.25, NC=0.99
9.	B.Jagadeesh et al.[20],2014	DWT ,SVM	Grey scale images of Goldhill, Mandrill and Peppers (512*512) /logo image (64*64)	PSNR=45.94,NC=0.961
10.	Yahya et al.[21], 2015	DCT, SVM	Lena, Baboon of size 1024 bits/ logo image	PSNR=49.86, NC=1.0

IV. Conclusion

Digital watermarking can be used in any area where there is need to protect multimedia data for the purpose of identification, annotation and copyright with guaranteed security and authenticity. This paper has presented detailed review of watermarking techniques based on spatial and frequency domain using machine learning techniques. The different watermarking techniques are use to learn about the parameters based on the performance along with the state of art. The use of machine learning method with watermarking is the blooming area that can further be explored.

Acknowledgement

The Author's are sincerely thankful to the potential/ anonymous reviewer's for their critical comments and suggestions to improve the quality of the paper.

References

[1] Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital Image Steganography : Survey and Analyses of Current Methods", Signal Processing, vol.90, no.3, 2010.

[2] Babak Mahdian and Stanislav Saic, "A bibliography on blind methods for identifying image forgery", Signal Processing: Image Communication 25, 2010.

[3] Huang-Chi Chen, Yu-Wen Chang and Rey-Chue Hwang, "A Watermarking Technique based on the Frequency Domain ", Journal of Multimedia,vol.7, no.1, 2012.

[4] Vaishali S. Jabade and Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications, vol.31, no.1, 2011.

[5] Prabhishek Singh and R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology, vol.2, no.9, 2013.

[6] Kaiser J.Giri, Mushtaq Ahmad Peer and P. Nagabhushan, "A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transform", International Journal of Image Graphics,2015.

[7] Henri Bruno Razafindradina and Attoumani Mohamed Karim, "Blind and Robust Image Watermarking based on Wavelet and Edge Insertion", International Journal on Cryptography and Information Security, Vol.3, no.3, 2013

[8] Harshita rawat, Ashwani kumar and Satendra kumar, "Robust Digital Image Watermarking Scheme for Copyright Protection", International Journal of Computer Applications, vol.75, no.18, 2013.

[9] Amit Kumar Singh, Mayank Dave and Anand Mohan, "Wavelet Based Image Watermarking: Futuristic Concepts in Information Security", Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, vol. 84, Issue 3, pp. 345-359, 2014.

[10] Simon Tong and Edward Chang, "support Vector Machine Active Learning for Image Retrieval", ACM, 2001

[11] Erkan Yavuz and Ziya Telatar, "Improved SVD-DWT Based Digital Image Watermarking Against Watermark Ambiguity", 2007.

[12] Mayank Vatsa, Richa Singh and Afzal Noore, "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking", IEICE Electronics Express, vol.2, no.12, pp.362-367, 2005.

[13] Shwu-Huey Yen and Chia-Jen Wang, "SVM Based watermarking technique", Tamkang Journal of Science and Engineering, vol. 9, no.2, 2006.

[14] Wu Jianzhen, "A RST Invariant Watermarking Scheme Utilizing Support Vector Machine and Image Moments for Synchronization", IEEE International Conference on Information Assurance and Security, 2009.

[15] Lei Li, Wen-Yan Ding and Jin-Yan Li, "A Novel Robustness Image Watermarking Scheme Based on Fuzzy Support Vector Machine", IEEE Pattern Recognition and Intelligence System, 2010.

[16] Yogendra Kumar Jain and Saurabh Tiwari, "An Enhanced Digital Watermarking for Color Image using SVM", International Journal of Computer Science and Information Technology, vol.2, no.5, 2011.

[17] Nallagarla Ramamurthy and Dr.S.Varadarajan, "Robust Digital image watermarking scheme with Neural Network and fuzzy logic approach", International Journal of Emerging Technology and Advanced Engineering, vol.2, no.9, 2012.

[18] B.Jagadeesh, P.Rajesh Kumar and P.Chenna Reddy, "Robust Digital Image Watermarking Scheme in Discrete Wavelet Transform Domain using Support Vector Machine", International Journal of Computer Applications, vol.73, no.14, 2013.

[19] M. Vafaei, H. Mahdavi Nasab and H. Pourghassem, "A new blind Robust Watermarking method based on Neural Networks in Wavelet Transform Domain", World Applied Science Journal, vol.22, no.11, 2013.

[20] B.Jagadeesh, P.Rajesh Kumar and P.Chenna Reddy, "Digital Image Watermark Extraction in Discrete Wavelet Transform Domain using Support Vector Machine", ACEEE International Journal of Recent Trends in Engineering and Technology , vol.11, 2014.

[21] Saadiah Yahya, Hanizan Shaker Hussain and Fakariah Hani M. Ali, “DCT Domain Stega SVM- shifted LSB Model for highly Imperceptible and robust cover image”, International Conference on Computing and Informatics, vol. 43, 2015.

[22] Fan Zhang and Hongbin Zhang, “Image watermarking capacity using Neural Network”, IEEE International Conference of Web Intelligence, 2004.

[23] Zhenghao Shi and Lifeng He, “Application of neural network in medical Image Processing”, International Symposium on Networking and Network Security, 2010.

[24] Le Hoang Thai, Tran Son Hai and Nguyen Thanh Thuy, “Image Classification using Support vector machine and Artificial neural networks”, International Journal of Information Technology and Computer Science, vol..32, no.38, 2012.