Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

Digital Video Watermarking: Features, Techniques, and Challenges

Lakshay Sharma,Abhineet Anand, Naresh Kumar Trivedi, Mohit Sharma, Jaskaran Singh.
Chitkara University Institute of Engineering Technology,
Chitkara University, Punjab.
Email – abhineet.anand@chitkara.edu.in

Abstract—The advent of digital technology can createseveralidentical copies of the original multimedia assets comprise of image, audio and video objects. Yet, these capabilities introduce several uncover issues includes illegitimate redistribution, ownership protection, content authentication, fingerprinting, copyright and many more. Digital video watermarking is a potential emerging solution to protect the digital multimedia from such threads. The technique suggested to hiding the authenticated information intothemultimedia assets like image, audio or video in such manner that it doesn't affect the quality of video objects and can be easily be extracted by certified user whenever required. On contrary, difficult to manipulate or remove by illicit person. The paperelaborates the features, applications, existing techniques, major categories of security attacks and related work done by previous researchers on digital video watermarking. Finally, the paper reviewed suchconcernwhich, still, requiredbeingdeterminedin digital video watermarking.

***Keyword*—**Copyright Protection, Digital Video Watermarking, DCT, DWT, SVD, Multimedia Security,

1. INTRODUCTION:

The availability of high internet technology exchange heavy multimedia items, irrespective of geographical location, between two or more computer system momentarily. Moreover, the advent of digital technology can easily reproduce the exact multiple copies because original and copied version of digital data cannot be distinguished. Due to these two rapidly change technologies, unauthorized user can redistribute it in an unauthentic way to other group of user via internet. Undoubtedly, the transfer of such pirated information causes the huge financial loses for film produces. Other serious problems associated with digital video watermarking is to protect the copyright [1], content [2], ownership [3], fingerprinting [4] and broadcast monitoring [5]. There are number of different techniques are existing in order to solve these concerns. They are categorized into three major techniques comprise steganography [6], cryptography [6] and watermarking [7].

Cryptography is an encryption technique in which the video is scrambled, by using symmetric or asymmetric key, into unintelligent form which transferred through internet so that the unauthorized user would not be able to read the same in transit phase. The file is remains protected during the transmission of multimedia content. After reaching to the destination the receiver can decrypt it by using the same or different cryptography key. Once decrypted, it becomes the original copy. Now, the concern is that the receiver can make the illegal copies and redistribute in an illegal manner. Hence, this technique fails to protect the copyright and other issues when receiver is not trustworthy.

Steganography is the other technique used to protect the data. In this technique the innocent object is used to carry the meaningful information. In this technique, secret information data is

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

firstly embedded into the meaningless object such as any image, audio or video file. And send to the destination over the internet. After reaching to the destination, the receiver will collect the useful information from the host via the method synchronized with the sender. Yet, the drawback is that there is no relationship exists between the host object and the secret data. This technique also fails to protect the host data.

Thanks to watermark technology. This technique suggested to embed the meaningful information into the digital multimedia object in such a manner that it can be extracted any time by only and only authorized person but difficult for illegal user to extract or even to destroy the same in order to resolve the security, piracy and other issues of Multimedia objects[30].

A lot of research has been done in the field of image watermarking for last two decades. The field of Image watermarking is exhausted. Video watermarking is totally different from the image watermarking. There are many problems related to video watermarking which are faced as it is totally related to problems like file insertion, deletion, swapping etc which are totally different from the Image watermarking.

Video watermarking is a visible embedded overlay on a video consisting of text, logo or a video copyrights. In today's time people are illegally using other people's video on their names which makes a big problem for the copyright protection issues. So it is necessary to use some method to prevent the video from being copied and for this Video watermarking is the best method. But the problems faced in this field are much like one of the major problem faced is there is always a tradeoff among robustness, imperceptibility and payload capacity that is all the three cannot be calculated simultaneously with proper values. So, the Video watermarking techniques are elaborated in this research paper. Watermarking process is classified into various types which are according to document type, applications, human perception and working Domain. All the types are further classified into various sub-categories as shown in figure 1.1.

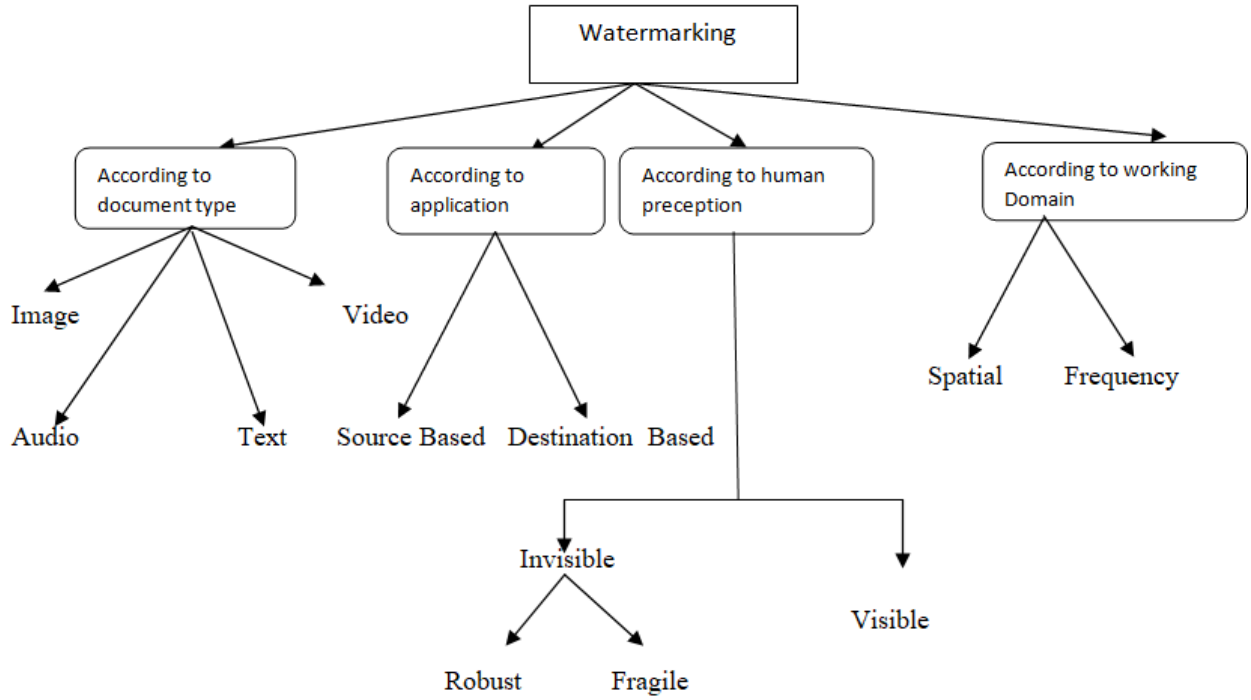

Fig.1: Types of Watermarking

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

The rest of the paper is organized as follows. The Application of watermarking are classified based on various categories are defined in Section 2. The features of digital video watermarking are described in Section 3. Section 4 illustrates the security issues against the techniques adopted by researchers. Section 5 explained the work done by previous researchers.

2. APPLICATIONS

Watermark processes are used in those areas where security and owner identification is needed in multimedia securities. The potential applications are described below [8].

2.1. **Broadcast Monitoring-**Embedding a digital watermark in audio or video at the time of broadcast allows the content owner from unauthorized broadcast.Digital watermark affects the visual quality of the work but still it is used by many companies to protect their broadcasts.The insertion of the watermark into the video is such that the precise identity of a particular video clip can be established.

2.2. Ownership Assertion-Watermark embedding in the digital content and then extracting it proves the ownership of the content.A watermarking system designed to serve ownership claims and proprietary claims have three major components: watermark and key generation, embedding and detection. Extracting the watermark not only prove the copyright ownership but also the ownership of the document.

2.3. Transaction Tracking-The copies of the digital content are identified uniquely.The owner of the content embeds watermark in every copy of the content.If the copy is misused than the owner can easily find the owner of the copy.

2.4. Content Authentication-To make sure that the data is not being tampered the watermark is extracted and the authentication is checked. Mostly the watermark embedded in digital content and the content is on internet to check authentication when watermark extracted have differences compared to the original watermark which shows the unauthorized use of the content.

2.5. Copy Control and Fingerprinting-It is similar to transaction tracking.It is used to prevent the use of the content without authorization by embedding watermark in the content.The person authorized for the use of copy of digital content can be traced by extracting the embedded watermark.

3. FEATURES OF DIGITAL VIDEO WATERMARKING

3.1. Robustness:

The general idea of robustness of a system is to deal with the errors during execution and then cope with the flawed inputs. Robustness of a digital video watermarking algorithm is the resistance of the watermark from certain transformations and attacks that affect the quality of the digital watermark in the video[9]. The measure of robustness of a digital video watermark tells us the immunity of the watermark against the hacking issues.

A similarity measurement between original and extracted watermark is attained to evaluate for extraction fidelity defined as

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

$$NC= \frac{\sum i \sum j . W_{ij} * W'_{ij}}{\sqrt{\sum i \sum j \left(W_{ij}\right)^2} \sqrt{\sum i \sum j \left(W'_{ij}\right)^2}}$$

$W_{ij}$is the pixel value of the i_{th} row and j_{th} column of reference watermark and W'_{ij} is the pixel value of the i_{th} row and j_{th} column of extracted watermark.

3.2. Perceptibility:

A video watermark which does not distort the quality of the video clip is called an imperceptible watermarked video which is a vigorous approach in digital video watermarking. Although if the presence of the watermark embedded in the video clip is noticeable, the watermark is perceptible[10] .To identify the imperceptibility of a video we come up with the distinctive exercise of peak signal to noise ratio (PSNR) which is often used for the same .Hence, the watermark used should be imperceptible which can also be understood by the synchronization of the original cover signal and the watermark signal.

3.3. Payload capacity:

The payload capacity is an integral part of digital video watermarking. It tells us the amount of information that can be embedded in the host video without spoiling the visual quality.Watermark granularity implies the harmonization level of detail between the video and the watermark which is a vital characteristic to be maintained in the video during the insertion of data in the video.

3.4. Security:

Digital video watermarking is more secure than any other technique as the address of the watermark embedded in the video is secret unless someone knows the secret key to it. There is always a need of authentication for the user as well as the provider before the beginning of the transaction which makes this protected[11]. Although sometimes the privacy of client also matterssoit may be desirable that no one, not even the content provider, be able to figure out the identity of the client.

4. CHALLENGES IN DIGITAL VIDEO WATERMARKING :

Digital video watermarking is a solid technique to protect the copyrights of the users but sometimes the watermarked digital data is attacked is in order to extract the information and then to gain benefits from the hacked data. The attacks are as follows:

4.1. Removal attacks:

This kind of attack aims to extract all the information in a video without hacking the security key of the watermark algorithm. This category include denoising, quantization, compression, multiple watermark and collusion attacks[12]. This attack may not achieve to remove the embedded watermark from the multimedia data but can potentially hinder watermark information.

4.2. Geometric attacks:

These type of attacks include either rotating, scaling, cropping and deletion of certain lines from the column or altering processing techniques. In this attack the watermark can only be completed extracted

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

if the applied technique reaches to a perfect synchronization with the digital data information,otherwise the technique is quite capable of atleast distorting the embedded watermark.

4.3. Cryptographic attacks:

The main aim of a cryptographic attack is to hack the security key of the watermarked information and remove the watermark. Moreover if achieved this may even aid the hacker to produce anew deceptive watermark[13].

4.4. Protocol attacks:

This type of attack aims to attack the whole concept of the multimedia watermark. The attack is directly programmed to hinder the watermark directly which may however produce either distortions or spoil the watermark potentially.

4.5. Deletion attacks:

The deletion attacks can be classified into two types of attacks that are quantization and noise removal attacks[14]. The main aim of the deletion attack is to eliminate the watermark effectively without any security key. These attacks can potentially affect the watermark that too with minimal encounters.

4.6. Frame manipulation attacks:

These particular attacks are applicable only on the video information data. These attacks for videos can be of two different types i.e.*Friendly* and *Non-friendly attacks*. Friendly attacks include the attacks which have no deliberate motive to destroy the watermark information in the video data, like frame insertion and frame deletion attacks used in commercial and censorship purposes. On the other side, Non-friendly attacks have an intention to alter the embedded watermark in the video by the use of frame averaging and frame swapping attacks [15].

5. TECHNIQUES:

Techniques are classified into two types which can be further divided into sub types and described as follows:

5.1.SPATIAL DOMAIN

Spatial domain technique is used to attach watermark to any type of data. It works directly on pixel of randomly chosen data by modifying the pixels of the data.The most frequently used spatial domain technique is least significant bit(LSB) and some other algorithms are there like additive watermarking and patchwork algorithm[16,17].

5.1.1. Least significant bit : In this, watermark is embedded to the lowest order bit of all the pixel of image therefore extraction is also switch in same way by detection of lowest bit of the pixel of image and then watermark is extracted[17,18].

5.1.2. Additive watermarking : In this, watermark embedding is done by adding pseudo random noise pattern to intensity of image pixels. it is a straightforward method of embedding the watermark[19].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

5.1.3. Patchwork algorithm : It establish on statistical model. In this, watermark is embedded in the data with a isolated statics by using Gaussian distribution. Extraction is switch out by the combining the received signals with anticipate form[17,20].

5.2. TRANSFORM DOMAIN

It is also known as frequency domain. In this watermark is embedded by altering the transform domain coefficients. Most commonly used transform domain techniques are DCT, DWT and DFT.In comparison of spatial and transform domain,transform domains is more effectual in finding robustness and imperceptibility[21].

5.2.1. Discrete Cosine Transformation: In this image is given in the form of frequencies of cosines and watermark is embedded in the still images[17,22].

5.2.2. Discrete Wavelet Transform: It usually produce a time frequency of distinct signals at a given time. the transformations are establish on the wavelets.it transforms the image into three dimensions Horizontal, vertical, diagonal individually[17] .

5.2.3. Discrete Fourier Transform: It transforms the isolated function into frequency component.it has a robustness against geometric attacks and it also shows the translation invariance[17].

6. RELATED WORK:

Analysis of some previous research paper on digital video watermarking has been combined in table:

Paper no.	Techniques Adopted	Evaluation parameters	Weakness/ Cons
[23] (2013)	1. Wavelet Based Contourlet Transform Decomposition 2.Non-Negative Matrix Factorizationwith Sparseness Constraints 3.)Video Watermarking Algorithm	1. PSNR obtained for different video format.	1.) Added mark may beconvenientlychanged 2.) Because of reputation of the Laplacian pyramid, the same cannot be the best option.
[24] (2013)	1. QR Code a) Pattern Finder b) Error Correction c) Separators d) Pattern Timing e)PatternAlignment	1. MAE 2. MSE 3. RMSE 4. PSNR 5. NCC	The QR code images are tolerable up to 30% noise.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

	f) Data g)Remainder Bits h)Format Information 2. MPEG-2 Video Compression 3.Singular Value Decomposition (SVD)		
[25] (2014)	1. Wavelet transform in two bands. 2. Singular Value Decomposition for Algebraic transform.	1. Robustness 2. Imperceptibility 3. Payload	Not Suitable for general per pose.
[26] (2016)	1. LSB 2. DCT 3. DWT	1. MSE, RMSE, PSNR, NC using LSB. 2. MSE, RMSE, PSNR, NC using DCT.	Watermarking techniques have failed to store large volume of data.
[27] (2017)	1. DFT 2. DCT 3. FFT	PSNR obtained for different video format	H.265 increases complexity.
[28] (2017)	1. SWEA (Split watermark embedding algorithm) 2. DWT	1. Gamma correction 2. Frame Swapping	Perceptibility not experimented after applying attacks.
[29] (2018)	1. DWT 2. FFT 3. SVD 4. GMSAT	1. SSIM algorithm is used to improve the quality of extracted watermark.	the quality of theextracted watermark from the channelchrominanceismeasured by anSSIM index slightly lowerquality than thatextracted from theluminance channel.
[31]	1. DWT 2. FFT 3. DCT	1. Robustness 2. Imperceptibility	Watermarking techniques to improve robustness of the signal
[32]	1. DWT 2.DCT	1. Security 2.Payload	Not applicable to general purpose

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 3376 - 3385
Received 20 January 2021; Accepted 08 February 2021.

CONCLUSION:

This review paper concludes the importance of digital video watermarking in the field of digital communication to protect the copyrights of users in their respective multimedia assets. In this paper, the applications and features of digital video watermarking are discussedwhich outweigh other encryption techniques in many aspects. Although the embedded watermarks can be attacked but there are certain techniques discussed which counter the attacks for better data protection. In this review paper, recent research papers have been reviewed which incorporated the transformation and spatial techniques in order to implement robust digital video watermarking. Yet, none of the techniques resist for video watermarking for all type of intentional and unintentional attack. Therefore, more robust and imperceptible compressed domain based digital video watermarking still require implementing which must cover joint attacks in the compressed domain.

Conflict-of-interest statement

The authors have no conflicts of interest to declare.

REFERENCES:

[1]S. Samuel, W.T.Penzhorn,"Digital watermarking for copyright protection",7thAfricon Conference in AfricaVol 2,2004,pp. 953 - 957
[2]Weilin Huang, Anthony T.S. Ho, Vinod Pankajakshan,"Watermarking-based content authentication of motion-JPEG sequences",5th International Conference on Visual Information Engineering Vol 4,2008
[3]Husrev T. Sencar,NasirMemon,"Watermarking and Ownership Problem: A Revisit",Conference: Proceedings of the Fifth ACM Workshop on Digital Rights Management 2005, pp.93-101
[4]Li Liu,Daiyuan Peng,XiaojuLi, "A Security Video Watermarking Scheme forBroadcastMonitoring",IEEE 2015
[5] Li Liu,Xiaoju Li," Watermarking Protocol for Broadcast Monitoring",International Conference on E-Business and E-Government 2010
[6]ArtiBhardwaj,AjayKhuteta, "Digital Video Watermarking Techniques: A Review",International Journal of Engineering and Computer Science,Vol6,Issue 5,2017,pp.21328-2133
[7]Simranjeet Kaur, Er.Rana Gill, Rajneetkaur(2015)," Comparative Analyses of YCbCr Color Space and CIELab Color Space Based On DWT and SVD",page 1,para 1&2.
[8]Aaqib Rashid," Digital Watermarking Applications and Techniques: A Brief Review", International Journal of Computer Applications Technology and Research Volume 5–Issue 3,pp. 147-150, 2016

[9]Y.Raghavender Rao, Dr.E.Nagabhooshanam, Nikhil Prathapani, "Robust Video Watermarking Algorithms Based OnSvdTransform",ICICES- S.A.Engineering College, Chennai, Tamil Nadu, India.page 4,para 3,2014
[10]Brijesh B. Mehta, Hardika D. Aswar, "Watermarking for Security in Database: A Review",Conference on IT in Business, Industry and Government (CSIBIG) page 4,para 7,2014
[11]JantanaPanyavaraporn, "Multiple Video Watermarking Algorithm based on Wavelet Transform",13th International Symposium on Communications and Information Technologies (ISCIT) page 1,para 6,2013
[12]ChanPik Wah, Supervised by Prof. Michael R. Lyu, "Multimedia Security Digital Video Watermarking" Term Paper,Department of Computer Science and Engineering, CUHK, page 17, para 3,2002
[13]Arti Bhardwaj, Ajay Khuteta, "Digital Video Watermarking: A Review", International Journal Of Engineering And Computer ScienceVol.6,Issue 5 ,pp. 21328-21332,2017
[14]Mohammad-Reza Keyvanpour, MahsaBoreiry,"Classification and Evaluation of WatermarkingAttacks in the Field of Video Watermarking",5th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS),7-9 March, Qazvin Islamic Azad University, Tehran,pp.25,para 3,2017.
[15] Abhineet Anand, Vikas Kumar Sihag, and S. N. Gupta. 2012. Wavelength conversion and deflection routing in all-optical packet-switched networks through contention resolution: a survey. In Proceedings of the CUBE International Information Technology Conference (CUBE '12). Association for Computing Machinery, New York, NY, USA, 155–159. DOI:https://doi.org/10.1145/2381716.2381747.
[16]N.Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, Vol 2,pp. 126-130,2013
[17]MonikaPatel,Priti Srinivas Sajja," Analysis and Survey of Digital Watermarking Techniques", ijarcsse, Vol 3,pp. 203-210, 2013
[18] D. Mistry," Comparison of Digital Watermarking Methods" (IJCSE) International Journal on Computer Science and Engineering, Vol 2 pp. 2805-2909,2013
[20]http://ippr-practical.blogspot.inacessed on 24 April 2019.
[21] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Vol2, Issue-2, 2012.
[22]Vidyasagar M. Potdar, Song Han, Elizabeth Chang, ―A Survey of Digital Image Watermarking Techniques‖, 3rd IEEE International conference on Industrial Informatics (INDIN),2005
[23]Gopika V. Mane, G. G. Chiddarwar,"An Imperceptible Video Watermarking Algorithm using Fusion of Wavelet Based Contourlet Transform & Sparse Non Negative Matrix Factorization",IEEE International Conference on Computational Intelligence and Computing Research,2013

[24]G.Prabakaran,R.Bhavani,M.Ramesh,"A Robust QR- Code Video Watermarking Scheme Based On SVD and DWT Composite Domain", Proceedings of the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME),2013
[25]Y.Raghavender Rao, Dr.E.Nagabhooshanam, Nikhil Prathapani,"Robust Video Watermarking Algorithms Based OnSvd Transform ",ICICES - S.A.Engineering College, Chennai, Tamil Nadu, India,2014
[26]Harpreet Kaur,Veerdeepkaur,"Invisible Video Multiple Watermarking Using Optimized Techniques",Online International Conference on Green Engineering and Technologies (IC-GET),2016
[27] Shaik HedayathBasha, B. Jaison,"Survey on Patended and Unpatented Video Watermarking Techniques",2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017),Coimbatore, INDIA,2017
[28]JabirAli,Prof. S.P.Ghrera,"A secure method of copyright protection for digital videos using Split Watermark Embedding Algorithm",Fourth International Conference on Image Information Processing (ICIIP),2017
[29] Z. S. Veličković, Z. Milivojević and M. Z. Veličković, "A secured digital video watermarking in chrominance channel," 2018 23rd International Scientific-Professional Conference on Information Technology (IT), Zabljak,Montenegro, 018, pp. 1-4, doi: 10.1109/SPIT.2018.8350858.
[30]R. Tomar, H. K. Sharma, A. Dumka, J. C. Patni and A. Anand, "Blind watermarking technique for greyscale image using DCT and 1-D Walsh coding," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015, pp. 365-369, doi: 10.1109/NGCT.2015.7375142.
[31] Trivedi Naresh, Trivedi C. Munesh, "An algorithimic Digital Audio Watermarking in Perceptual Domain Using Direct Sequence Spectrum" IEEE Explore Conference CSNT 2014, NITTR, Bhopal at Apr 7-9, 2014.
[32] Trivedi Naresh, Trivedi C. Munesh, "Audio Masking for watermarking embedding under time domain audio signals" IEEE conference ICIN 2014, Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed) University, Udaipur at Nov 14-16, 2014.